

# FortiOS - CLI Reference

Version 6.4.9

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



April 26, 2022

FortiOS 6.4.9 CLI Reference

01-649-684766-20220426

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>17</b>
<b>FortiOS CLI reference</b> .....	<b>18</b>
Creation of the CLI reference .....	18
Availability of commands and options .....	18
Command tree .....	19
<b>CLI configuration commands</b> .....	<b>20</b>
alertemail .....	21
config alertemail setting .....	21
antivirus .....	28
config antivirus settings .....	28
config antivirus heuristic .....	29
config antivirus quarantine .....	29
config antivirus profile .....	34
application .....	58
config application name .....	58
config application custom .....	60
config application rule-settings .....	61
config application list .....	61
config application group .....	69
authentication .....	70
config authentication scheme .....	70
config authentication rule .....	71
config authentication setting .....	73
certificate .....	75
config certificate ca .....	75
config certificate remote .....	76
config certificate local .....	77
config certificate crl .....	80
credential-store .....	82
config credential-store domain-controller .....	82
dlp .....	84
config dlp filepattern .....	84
config dlp sensitivity .....	87
config dlp sensor .....	87
dnsfilter .....	93
config dnsfilter domain-filter .....	93
config dnsfilter profile .....	94
emailfilter .....	99
config emailfilter bword .....	99
config emailfilter bwl .....	101
config emailfilter mheader .....	103
config emailfilter dnsbl .....	104
config emailfilter iptrust .....	105
config emailfilter profile .....	106

config emailfilter fortishield .....	113
config emailfilter options .....	114
endpoint-control .....	115
config endpoint-control fctems .....	115
extender .....	118
config extender sys-info .....	118
config extender extender-info .....	118
config extender modem-status .....	119
config extender lte-carrier-list .....	119
config extender lte-carrier-by-mcc-mnc .....	119
extender-controller .....	120
config extender-controller dataplan .....	120
config extender-controller extender .....	122
file-filter .....	130
config file-filter profile .....	130
firewall .....	133
config firewall address .....	135
config firewall multicast-address .....	139
config firewall address6-template .....	141
config firewall address6 .....	142
config firewall multicast-address6 .....	145
config firewall addrgrp .....	146
config firewall addrgrp6 .....	148
config firewall wildcard-fqdn custom .....	149
config firewall wildcard-fqdn group .....	149
config firewall service category .....	150
config firewall service custom .....	151
config firewall service group .....	155
config firewall city .....	156
config firewall region .....	156
config firewall country .....	156
config firewall internet-service .....	157
config firewall internet-service-name .....	158
config firewall internet-service-group .....	159
config firewall internet-service-extension .....	160
config firewall internet-service-reputation .....	162
config firewall internet-service-custom .....	163
config firewall internet-service-addition .....	164
config firewall internet-service-append .....	165
config firewall internet-service-custom-group .....	166
config firewall internet-service-sld .....	166
config firewall internet-service-ipbl-vendor .....	167
config firewall internet-service-ipbl-reason .....	167
config firewall internet-service-owner .....	167
config firewall internet-service-list .....	168
config firewall internet-service-definition .....	168
config firewall internet-service-botnet .....	169
config firewall vendor-mac .....	170
config firewall vendor-mac-summary .....	170

config firewall shaper traffic-shaper .....	170
config firewall shaper per-ip-shaper .....	173
config firewall shaper traffic .....	174
config firewall shaper per-ip .....	174
config firewall proxy-address .....	174
config firewall proxy-addrgrp .....	177
config firewall schedule onetime .....	179
config firewall schedule recurring .....	179
config firewall schedule group .....	180
config firewall ippool .....	181
config firewall ippool6 .....	183
config firewall ldb-monitor .....	184
config firewall vip .....	185
config firewall vip46 .....	214
config firewall vip6 .....	218
config firewall vip64 .....	245
config firewall vipgrp .....	249
config firewall vipgrp46 .....	250
config firewall vipgrp6 .....	250
config firewall vipgrp64 .....	251
config firewall ipmacbinding setting .....	252
config firewall ipmacbinding table .....	253
config firewall profile-protocol-options .....	253
config firewall ssl-ssh-profile .....	275
config firewall profile-group .....	297
config firewall ssl-server .....	298
config firewall decrypted-traffic-mirror .....	301
config firewall identity-based-route .....	302
config firewall auth-portal .....	302
config firewall security-policy .....	303
config firewall policy .....	309
config firewall traffic-class .....	326
config firewall shaping-policy .....	326
config firewall shaping-profile .....	331
config firewall local-in-policy .....	333
config firewall local-in-policy6 .....	334
config firewall ttl-policy .....	336
config firewall policy64 .....	337
config firewall policy46 .....	339
config firewall proxy-policy .....	342
config firewall dnstranslation .....	349
config firewall multicast-policy .....	350
config firewall multicast-policy6 .....	352
config firewall interface-policy .....	354
config firewall interface-policy6 .....	357
config firewall DoS-policy .....	360
config firewall DoS-policy6 .....	362
config firewall sniffer .....	364
config firewall central-snat-map .....	369

config firewall ssl setting .....	371
config firewall ssh local-key .....	373
config firewall ssh local-ca .....	374
config firewall ssh setting .....	374
config firewall ssh host-key .....	375
config firewall ip-translation .....	377
config firewall ipv6-eh-filter .....	378
config firewall iprope list .....	379
config firewall iprope appctrl list .....	380
config firewall iprope appctrl status .....	380
config firewall proute .....	380
config firewall proute6 .....	380
ftp-proxy .....	381
config ftp-proxy explicit .....	381
hardware .....	383
config hardware status .....	383
config hardware cpu .....	383
config hardware memory .....	383
config hardware nic .....	383
icap .....	385
config icap server .....	385
config icap profile .....	386
ips .....	391
config ips sensor .....	391
config ips view-map .....	395
config ips decoder .....	396
config ips rule .....	397
config ips rule-settings .....	399
config ips custom .....	399
config ips global .....	401
config ips settings .....	405
config ips session .....	405
ipsec .....	406
config ipsec tunnel .....	406
log .....	407
config log threat-weight .....	408
config log custom-field .....	417
config log syslogd setting .....	418
config log syslogd override-setting .....	421
config log syslogd filter .....	425
config log syslogd override-filter .....	427
config log syslogd2 setting .....	429
config log syslogd2 override-setting .....	433
config log syslogd2 filter .....	436
config log syslogd2 override-filter .....	438
config log syslogd3 setting .....	440
config log syslogd3 override-setting .....	444
config log syslogd3 filter .....	447

config log syslogd3 override-filter .....	449
config log syslogd4 setting .....	451
config log syslogd4 override-setting .....	455
config log syslogd4 filter .....	458
config log syslogd4 override-filter .....	460
config log webtrends setting .....	462
config log webtrends filter .....	463
config log memory global-setting .....	464
config log memory setting .....	465
config log memory filter .....	466
config log disk setting .....	467
config log disk filter .....	473
config log eventfilter .....	475
config log fortiguard setting .....	477
config log fortiguard override-setting .....	480
config log fortiguard filter .....	481
config log fortiguard override-filter .....	483
config log null-device setting .....	485
config log null-device filter .....	486
config log setting .....	487
config log gui-display .....	491
config log fortianalyzer setting .....	492
config log fortianalyzer override-setting .....	496
config log fortianalyzer filter .....	500
config log fortianalyzer override-filter .....	502
config log fortianalyzer2 setting .....	504
config log fortianalyzer2 override-setting .....	508
config log fortianalyzer2 filter .....	512
config log fortianalyzer2 override-filter .....	514
config log fortianalyzer3 setting .....	516
config log fortianalyzer3 override-setting .....	520
config log fortianalyzer3 filter .....	524
config log fortianalyzer3 override-filter .....	526
config log fortianalyzer-cloud setting .....	528
config log fortianalyzer-cloud override-setting .....	531
config log fortianalyzer-cloud filter .....	532
config log fortianalyzer-cloud override-filter .....	534
mgmt-data .....	537
config mgmt-data status .....	537
router .....	538
config router access-list .....	538
config router access-list6 .....	539
config router aspath-list .....	540
config router prefix-list .....	541
config router prefix-list6 .....	542
config router key-chain .....	543
config router community-list .....	544
config router route-map .....	545
config router rip .....	551

config router ripng .....	557
config router static .....	562
config router policy .....	565
config router policy6 .....	568
config router static6 .....	569
config router ospf .....	571
config router ospf6 .....	586
config router bgp .....	599
config router isis .....	638
config router multicast-flow .....	650
config router multicast .....	651
config router multicast6 .....	660
config router info .....	661
config router info6 .....	662
config router auth-path .....	662
config router setting .....	662
config router bfd .....	663
config router bfd6 .....	663
ssh-filter .....	664
config ssh-filter profile .....	664
switch-controller .....	667
config switch-controller traffic-policy .....	668
config switch-controller nac-settings .....	669
config switch-controller switch-interface-tag .....	670
config switch-controller 802-1X-settings .....	671
config switch-controller security-policy 802-1X .....	671
config switch-controller security-policy local-access .....	674
config switch-controller location .....	675
config switch-controller lldp-settings .....	679
config switch-controller lldp-profile .....	680
config switch-controller qos dot1p-map .....	684
config switch-controller qos ip-dscp-map .....	687
config switch-controller qos queue-policy .....	689
config switch-controller qos qos-policy .....	691
config switch-controller storm-control-policy .....	692
config switch-controller auto-config policy .....	693
config switch-controller auto-config default .....	694
config switch-controller auto-config custom .....	695
config switch-controller initial-config template .....	695
config switch-controller initial-config vlans .....	697
config switch-controller switch-profile .....	697
config switch-controller custom-command .....	698
config switch-controller virtual-port-pool .....	698
config switch-controller ptp settings .....	699
config switch-controller ptp policy .....	699
config switch-controller managed-switch .....	700
config switch-controller switch-group .....	731
config switch-controller stp-settings .....	731
config switch-controller stp-instance .....	732



config switch-controller storm-control .....	733
config switch-controller global .....	733
config switch-controller system .....	736
config switch-controller switch-log .....	738
config switch-controller igmp-snooping .....	739
config switch-controller sflow .....	739
config switch-controller quarantine .....	740
config switch-controller network-monitor-settings .....	740
config switch-controller flow-tracking .....	741
config switch-controller snmp-sysinfo .....	743
config switch-controller snmp-trap-threshold .....	744
config switch-controller snmp-community .....	745
config switch-controller snmp-user .....	747
config switch-controller traffic-sniffer .....	749
config switch-controller remote-log .....	750
config switch-controller vlan-policy .....	752
config switch-controller port-policy .....	753
config switch-controller mac-policy .....	754
config switch-controller nac-device .....	755
system .....	757
config system vdom .....	760
config system global .....	761
config system accprofile .....	796
config system vdom-link .....	805
config system switch-interface .....	806
config system object-tagging .....	808
config system lte-modem .....	809
config system interface .....	811
config system physical-switch .....	856
config system virtual-switch .....	857
config system stp .....	858
config system password-policy .....	860
config system password-policy-guest-admin .....	862
config system sms-server .....	864
config system custom-language .....	864
config system admin .....	865
config system api-user .....	871
config system sso-admin .....	873
config system settings .....	873
config system sit-tunnel .....	892
config system npu .....	893
config system fsso-polling .....	898
config system ha .....	899
config system ha-monitor .....	909
config system storage .....	910
config system dedicated-mgmt .....	911
config system arp-table .....	912
config system ipv6-neighbor-cache .....	913
config system dns .....	913

config system ddns .....	915
config system sflow .....	918
config system vdom-sflow .....	919
config system netflow .....	920
config system vdom-netflow .....	921
config system vdom-dns .....	922
config system replacemsg-image .....	924
config system replacemsg mail .....	924
config system replacemsg http .....	925
config system replacemsg webproxy .....	926
config system replacemsg ftp .....	927
config system replacemsg fortiguard-wf .....	928
config system replacemsg spam .....	929
config system replacemsg alertmail .....	929
config system replacemsg admin .....	930
config system replacemsg auth .....	931
config system replacemsg sslvpn .....	932
config system replacemsg nac-quar .....	933
config system replacemsg traffic-quota .....	933
config system replacemsg utm .....	934
config system replacemsg icap .....	935
config system replacemsg-group .....	936
config system snmp sysinfo .....	946
config system snmp community .....	947
config system snmp user .....	954
config system autoupdate push-update .....	960
config system autoupdate schedule .....	961
config system autoupdate tunneling .....	962
config system session-ttl .....	963
config system dhcp server .....	964
config system dhcp6 server .....	975
config system modem .....	978
config system 3g-modem custom .....	985
config system status .....	986
config system performance status .....	986
config system performance top .....	987
config system performance firewall packet-distribution .....	987
config system performance firewall statistics .....	987
config system session .....	987
config system session6 .....	987
config system cmdb .....	988
config system fortiguard-service .....	988
config system fortianalyzer-connectivity .....	988
config system checksum status .....	988
config system mgmt-csum .....	988
config system ha-nonsync-csum .....	988
config system fortiguard-log-service .....	989
config system central-mgmt .....	989
config system alias .....	989

config system auto-script .....	989
config system info admin status .....	990
config system info admin ssh .....	990
config system management-tunnel .....	991
config system fortimanager .....	992
config system fm .....	993
config system central-management .....	994
config system zone .....	999
config system geoip-country .....	1000
config system sdn-connector .....	1000
config system ipv6-tunnel .....	1006
config system external-resource .....	1007
config system ips-urlfilter-dns .....	1009
config system ips-urlfilter-dns6 .....	1009
config system network-visibility .....	1010
config system gre-tunnel .....	1011
config system ipsec-aggregate .....	1014
config system ipip-tunnel .....	1014
config system mobile-tunnel .....	1015
config system pppoe-interface .....	1017
config system vxlan .....	1019
config system geneve .....	1021
config system virtual-wire-pair .....	1022
config system dns-database .....	1022
config system dns-server .....	1025
config system resource-limits .....	1026
config system vdom-property .....	1028
config system sdwan .....	1030
config system speed-test-server .....	1049
config system lldp network-policy .....	1050
config system standalone-cluster .....	1057
config system cluster-sync .....	1058
config system fortiguard .....	1061
config system ips .....	1067
config system arp .....	1068
config system email-server .....	1068
config system alarm .....	1070
config system mac-address-table .....	1073
config system session-helper .....	1073
config system proxy-arp .....	1074
config system fips-cc .....	1075
config system tos-based-priority .....	1076
config system dscp-based-priority .....	1077
config system probe-response .....	1077
config system link-monitor .....	1078
config system auto-install .....	1082
config system console .....	1083
config system ntp .....	1084
config system ptp .....	1087

config system wccp .....	1088
config system nat64 .....	1091
config system vdom-radius-server .....	1093
config system startup-error-log .....	1094
config system source-ip status .....	1094
config system auto-update status .....	1094
config system auto-update versions .....	1094
config system session-info list .....	1094
config system session-info expectation .....	1094
config system session-info full-stat .....	1095
config system session-info statistics .....	1095
config system session-info ttl .....	1095
config system session-helper-info list .....	1095
config system ip-conflict status .....	1095
config system ftm-push .....	1095
config system geoip-override .....	1096
config system fortisandbox .....	1097
config system vdom-exception .....	1099
config system csf .....	1100
config system automation-trigger .....	1104
config system automation-action .....	1107
config system automation-destination .....	1113
config system automation-stitch .....	1113
config system nd-proxy .....	1114
config system saml .....	1115
config system vne-tunnel .....	1118
test .....	1120
config test smtp .....	1121
config test ftpd .....	1121
config test pop3 .....	1122
config test imap .....	1122
config test nntp .....	1122
config test harelay .....	1123
config test hasync .....	1123
config test hataik .....	1123
config test sessionsync .....	1124
config test forticldd .....	1124
config test miglogd .....	1124
config test urlfilter .....	1125
config test wf_monitor .....	1125
config test ovrd .....	1125
config test iotd .....	1126
config test ipsmonitor .....	1126
config test ipseengine .....	1126
config test ipldb .....	1127
config test ddnsd .....	1127
config test snmpd .....	1127
config test acd .....	1128
config test dnsproxy .....	1128

config test sflowd .....	1128
config test init .....	1129
config test l2tpcd .....	1129
config test dhcprelay .....	1129
config test pptpcd .....	1130
config test wccpd .....	1130
config test wad .....	1130
config test radiusd .....	1131
config test fsd .....	1131
config test ipsufd .....	1131
config test lted .....	1132
config test forticron .....	1132
config test uploadd .....	1133
config test quarantined .....	1133
config test dhcp6c .....	1133
config test dsd .....	1134
config test ipmc_sensord .....	1134
config test lnkmt .....	1134
config test dhcp6r .....	1135
config test updated .....	1135
config test awsd .....	1135
config test netxd .....	1136
config test fnbamd .....	1136
config test mrd .....	1136
config test zebos_launcher .....	1137
config test radius-das .....	1137
config test csfd .....	1137
config test fsvrd .....	1138
config test radvd .....	1138
config test fcnacd .....	1138
config test sdncd .....	1139
config test azd .....	1139
config test gcpcd .....	1139
config test ocid .....	1140
config test kubed .....	1140
config test autod .....	1140
config test bfd .....	1141
config test openstackd .....	1141
config test fas .....	1141
config test sepmd .....	1142
config test ipamd .....	1142
config test sdnd .....	1142
config test vned .....	1143
user .....	1144
config user radius .....	1144
config user tacacs+ .....	1155
config user exchange .....	1157
config user ldap .....	1159
config user krb-keytab .....	1165

config user domain-controller .....	1165
config user pop3 .....	1166
config user saml .....	1167
config user fsso .....	1168
config user adgrp .....	1172
config user fsso-polling .....	1172
config user fortitoken .....	1174
config user password-policy .....	1175
config user local .....	1176
config user setting .....	1179
config user peer .....	1183
config user peergrp .....	1185
config user quarantine .....	1185
config user group .....	1186
config user security-exempt-list .....	1191
config user nac-policy .....	1192
voip .....	1195
config voip profile .....	1195
vpn .....	1215
config vpn certificate ca .....	1215
config vpn certificate remote .....	1217
config vpn certificate local .....	1218
config vpn certificate crl .....	1220
config vpn certificate ocsdp-server .....	1222
config vpn certificate setting .....	1223
config vpn ssl web realm .....	1226
config vpn ssl web host-check-software .....	1227
config vpn ssl web portal .....	1229
config vpn ssl web user-group-bookmark .....	1246
config vpn ssl web user-bookmark .....	1251
config vpn ssl settings .....	1257
config vpn ssl monitor .....	1270
config vpn ipsec phase1 .....	1270
config vpn ipsec phase2 .....	1289
config vpn ipsec manualkey .....	1298
config vpn ipsec concentrator .....	1300
config vpn ipsec phase1-interface .....	1300
config vpn ipsec phase2-interface .....	1324
config vpn ipsec manualkey-interface .....	1333
config vpn ipsec forticlient .....	1335
config vpn ipsec stats crypto .....	1336
config vpn ipsec stats tunnel .....	1336
config vpn ipsec tunnel details .....	1336
config vpn ipsec tunnel summary .....	1336
config vpn ipsec tunnel name .....	1337
config vpn pptp .....	1337
config vpn l2tp .....	1338
config vpn ocvpn .....	1339
config vpn ike gateway .....	1343

config vpn status l2tp .....	1343
config vpn status pptp .....	1343
config vpn status ssl list .....	1343
config vpn status ssl hw-acceleration-status .....	1343
waf .....	1344
config waf main-class .....	1344
config waf sub-class .....	1344
config waf signature .....	1345
config waf profile .....	1345
web-proxy .....	1370
config web-proxy profile .....	1370
config web-proxy global .....	1374
config web-proxy explicit .....	1376
config web-proxy forward-server .....	1381
config web-proxy forward-server-group .....	1382
config web-proxy debug-url .....	1384
config web-proxy wisp .....	1384
config web-proxy url-match .....	1385
webfilter .....	1387
config webfilter ftgd-local-cat .....	1387
config webfilter content .....	1388
config webfilter content-header .....	1389
config webfilter urlfilter .....	1390
config webfilter ips-urlfilter-setting .....	1393
config webfilter ips-urlfilter-setting6 .....	1394
config webfilter ips-urlfilter-cache-setting .....	1394
config webfilter profile .....	1395
config webfilter fortiguard .....	1411
config webfilter categories .....	1413
config webfilter override .....	1413
config webfilter ftgd-local-rating .....	1414
config webfilter search-engine .....	1415
config webfilter ftgd-statistics .....	1416
config webfilter status .....	1416
config webfilter override-usr .....	1417
wireless-controller .....	1418
config wireless-controller inter-controller .....	1419
config wireless-controller global .....	1420
config wireless-controller hotspot20 anqp-venue-name .....	1423
config wireless-controller hotspot20 anqp-network-auth-type .....	1424
config wireless-controller hotspot20 anqp-roaming-consortium .....	1424
config wireless-controller hotspot20 anqp-nai-realm .....	1425
config wireless-controller hotspot20 anqp-3gpp-cellular .....	1428
config wireless-controller hotspot20 anqp-ip-address-type .....	1429
config wireless-controller hotspot20 h2qp-operator-name .....	1430
config wireless-controller hotspot20 h2qp-wan-metric .....	1430
config wireless-controller hotspot20 h2qp-conn-capability .....	1432
config wireless-controller hotspot20 icon .....	1434
config wireless-controller hotspot20 h2qp-osu-provider .....	1435

---

config wireless-controller hotspot20 qos-map .....	1437
config wireless-controller hotspot20 hs-profile .....	1438
config wireless-controller vap .....	1445
config wireless-controller timers .....	1469
config wireless-controller setting .....	1471
config wireless-controller log .....	1480
config wireless-controller apcfg-profile .....	1484
config wireless-controller bonjour-profile .....	1486
config wireless-controller arp-profile .....	1487
config wireless-controller region .....	1490
config wireless-controller vap-group .....	1491
config wireless-controller wids-profile .....	1491
config wireless-controller ble-profile .....	1498
config wireless-controller wtp-profile .....	1500
config wireless-controller wtp .....	1556
config wireless-controller wtp-group .....	1577
config wireless-controller qos-profile .....	1580
config wireless-controller wag-profile .....	1583
config wireless-controller utm-profile .....	1585
config wireless-controller address .....	1586
config wireless-controller addrgrp .....	1586
config wireless-controller snmp .....	1587
config wireless-controller mpsk-profile .....	1590
config wireless-controller access-control-list .....	1592
config wireless-controller scan .....	1594
config wireless-controller ap-status .....	1594
config wireless-controller wlchanlistlic .....	1595
config wireless-controller status .....	1595
config wireless-controller wtp-status .....	1596
config wireless-controller client-info .....	1596
config wireless-controller vap-status .....	1596
config wireless-controller rf-analysis .....	1597
config wireless-controller spectral-info .....	1597



## Change Log

Date	Change Description
2022-04-26	First automated release of the FortiOS 6.4.9 CLI Reference.

# FortiOS CLI reference

This document describes FortiOS 6.4.9 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI). For information on using the CLI, see the [FortiOS 6.4.9 Administration Guide](#), which contains information such as:

- [Connecting to the CLI](#)
- [CLI basics](#)
- [Command syntax](#)
- [Subcommands](#)
- [Permissions](#)

## Creation of the CLI reference

The CLI syntax is created by processing the schema from FortiGate models running FortiOS 6.4.9 and reformatting the resultant CLI output. The following reference models were used to create this CLI reference:

- *FGT\_80E\_POE*: a POE model with 12x PoE ports and 16x GE RJ45 ports. No log disk.
- *FWF\_61E*: a WiFi/desktop model with SSD storage, FortiSoC3, Wireless (802.11a/b/g/n/ac) and 10x GE RJ45 ports.
- *FGT\_501E*: a mid-range model with 2x 240GB SSD storage, NP6 and CP9 acceleration, 2x 10GE SFP+ slots, 8x GE SFP slots and 10x GE RJ45 ports.
- *FGT\_3000D*: a high-end model with 480GB SSD storage, NP6 and CP8 acceleration, dyak AC power supplies, 16x 10GE SFP+ slots and 2x GE RJ45 management ports.
- *FGT\_VM64*: a Virtual Machine model running on VMware ESXi.

If you have comments on this content, its format, or requests for commands that are not included, contact us at [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## Availability of commands and options

Some FortiOS CLI commands and options are not available on all FortiGate units. The CLI displays an error message if you attempt to enter a command or option that is not available. You can use the question mark '?' to verify the commands and options that are available.

Commands and options may not be available for the following reasons:

### FortiGate model

All commands are not available on all FortiGate models. For example, a hardware switch can be configured only on models which have the corresponding hardware switch chipset.

## Hardware configuration

For example, settings like `mediatype` would only be available on units with SFPs.

## FortiOS Carrier, FortiGate 5K/6K/7K, FortiGate with LTE, etc.

Commands for extended functionality are not available on all FortiGate models. The CLI Reference may not include all commands.

## Command tree

Enter `tree` to display the entire FortiOS CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file.

- To view all available commands, enter `tree`.
- To view a specific configuration branch of a tree, enter `tree <branch>`, for example: `tree system`.
- To view all available diagnose commands, enter `tree diagnose`.
- To view all available execute commands, enter `tree execute`.

# CLI configuration commands

Use configuration commands to configure and manage a FortiGate unit from the command line interface (CLI).

The CLI syntax is created by processing the schema from FortiGate models running FortiOS 6.4.9 and reformatting the resultant CLI output. The following reference models were used to create this CLI reference:

- *FGT\_80E\_POE*: a POE model with 12x PoE ports and 16x GE RJ45 ports. No log disk.
- *FWF\_61E*: a WiFi/desktop model with SSD storage, FortiSoC3, Wireless (802.11a/b/g/n/ac) and 10x GE RJ45 ports.
- *FGT\_501E*: a mid-range model with 2x 240GB SSD storage, NP6 and CP9 acceleration, 2x 10GE SFP+ slots, 8x GE SFP slots and 10x GE RJ45 ports.
- *FGT\_3000D*: a high-end model with 480GB SSD storage, NP6 and CP8 acceleration, dyak AC power supplies, 16x 10GE SFP+ slots and 2x GE RJ45 management ports.
- *FGT\_VM64*: a Virtual Machine model running on VMware ESXi.



The command branches are in alphabetical order. The commands beneath each branch are *not* in alphabetical order.

---

If you have comments on this content, its format, or requests for commands that are not included, contact us at [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## alertemail

This section includes syntax for the following commands:

- [config alertemail setting on page 21](#)

### config alertemail setting

Configure alert email settings.

```
config alertemail setting
  Description: Configure alert email settings.
  set username {string}
  set mailto1 {string}
  set mailto2 {string}
  set mailto3 {string}
  set filter-mode [category|threshold]
  set email-interval {integer}
  set IPS-logs [enable|disable]
  set firewall-authentication-failure-logs [enable|disable]
  set HA-logs [enable|disable]
  set IPsec-errors-logs [enable|disable]
  set FDS-update-logs [enable|disable]
  set PPP-errors-logs [enable|disable]
  set sslvpn-authentication-errors-logs [enable|disable]
  set antivirus-logs [enable|disable]
  set webfilter-logs [enable|disable]
  set configuration-changes-logs [enable|disable]
  set violation-traffic-logs [enable|disable]
  set admin-login-logs [enable|disable]
  set FDS-license-expiring-warning [enable|disable]
  set log-disk-usage-warning [enable|disable]
  set fortiguard-log-quota-warning [enable|disable]
  set amc-interface-bypass-mode [enable|disable]
  set FIPS-CC-errors [enable|disable]
  set FSSO-disconnect-logs [enable|disable]
  set ssh-logs [enable|disable]
  set FDS-license-expiring-days {integer}
  set local-disk-usage {integer}
  set emergency-interval {integer}
  set alert-interval {integer}
  set critical-interval {integer}
  set error-interval {integer}
  set warning-interval {integer}
  set notification-interval {integer}
  set information-interval {integer}
  set debug-interval {integer}
  set severity [emergency|alert|...]
end
```

## config alertemail setting

Parameter	Description	Type	Size	Default
username	Name that appears in the From: field of alert emails (max. 63 characters).	string	Maximum length: 63	
mailto1	Email address to send alert email to (usually a system administrator) (max. 63 characters).	string	Maximum length: 63	
mailto2	Optional second email address to send alert email to (max. 63 characters).	string	Maximum length: 63	
mailto3	Optional third email address to send alert email to (max. 63 characters).	string	Maximum length: 63	
filter-mode	How to filter log messages that are sent to alert emails.	option	-	category
email-interval	Interval between sending alert emails .	integer	Minimum value: 1 Maximum value: 99999	5
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-	disable
HA-logs	Enable/disable HA logs in alert email.	option	-	disable

Parameter	Description	Type	Size	Default						
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec error logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec error logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec error logs in alert email.	<i>disable</i>	Disable IPsec error logs in alert email.			
Option	Description									
<i>enable</i>	Enable IPsec error logs in alert email.									
<i>disable</i>	Disable IPsec error logs in alert email.									
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard update logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard update logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard update logs in alert email.	<i>disable</i>	Disable FortiGuard update logs in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard update logs in alert email.									
<i>disable</i>	Disable FortiGuard update logs in alert email.									
PPP-errors-logs	Enable/disable PPP error logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PPP error logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PPP error logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PPP error logs in alert email.	<i>disable</i>	Disable PPP error logs in alert email.			
Option	Description									
<i>enable</i>	Enable PPP error logs in alert email.									
<i>disable</i>	Disable PPP error logs in alert email.									
sslvpn-authentication-errors-logs	Enable/disable SSL-VPN authentication error logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSL-VPN authentication error logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL-VPN authentication error logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.	<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.			
Option	Description									
<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.									
<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.									
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable antivirus logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable antivirus logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable antivirus logs in alert email.	<i>disable</i>	Disable antivirus logs in alert email.			
Option	Description									
<i>enable</i>	Enable antivirus logs in alert email.									
<i>disable</i>	Disable antivirus logs in alert email.									
webfilter-logs	Enable/disable web filter logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable web filter logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable web filter logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable web filter logs in alert email.	<i>disable</i>	Disable web filter logs in alert email.			
Option	Description									
<i>enable</i>	Enable web filter logs in alert email.									
<i>disable</i>	Disable web filter logs in alert email.									
configuration-changes-logs	Enable/disable configuration change logs in alert email.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable configuration change logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable configuration change logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable configuration change logs in alert email.	<i>disable</i>	Disable configuration change logs in alert email.			
Option	Description									
<i>enable</i>	Enable configuration change logs in alert email.									
<i>disable</i>	Disable configuration change logs in alert email.									
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable violation traffic logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable violation traffic logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable violation traffic logs in alert email.	<i>disable</i>	Disable violation traffic logs in alert email.			
Option	Description									
<i>enable</i>	Enable violation traffic logs in alert email.									
<i>disable</i>	Disable violation traffic logs in alert email.									
admin-login-logs	Enable/disable administrator login/logout logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable administrator login/logout logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable administrator login/logout logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable administrator login/logout logs in alert email.	<i>disable</i>	Disable administrator login/logout logs in alert email.			
Option	Description									
<i>enable</i>	Enable administrator login/logout logs in alert email.									
<i>disable</i>	Disable administrator login/logout logs in alert email.									
FDS-license-expiring-warning	Enable/disable FortiGuard license expiration warnings in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard license expiration warnings in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard license expiration warnings in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.	<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.									
<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.									
log-disk-usage-warning	Enable/disable disk usage warnings in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable disk usage warnings in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable disk usage warnings in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable disk usage warnings in alert email.	<i>disable</i>	Disable disk usage warnings in alert email.			
Option	Description									
<i>enable</i>	Enable disk usage warnings in alert email.									
<i>disable</i>	Disable disk usage warnings in alert email.									
fortiguard-log-quota-warning	Enable/disable FortiCloud log quota warnings in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiCloud log quota warnings in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiCloud log quota warnings in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.	<i>disable</i>	Disable FortiCloud log quota warnings in alert email.			
Option	Description									
<i>enable</i>	Enable FortiCloud log quota warnings in alert email.									
<i>disable</i>	Disable FortiCloud log quota warnings in alert email.									
amc-interface-bypass-mode	Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	<i>disable</i>	Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.			
Option	Description									
<i>enable</i>	Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.									
<i>disable</i>	Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.									
FIPS-CC-errors	Enable/disable FIPS and Common Criteria error logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FIPS and Common Criteria error logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FIPS and Common Criteria error logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.	<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.			
Option	Description									
<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.									
<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.									
FSSO-disconnect-logs	Enable/disable logging of FSSO collector agent disconnect.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging of FSSO collector agent disconnect.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging of FSSO collector agent disconnect.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging of FSSO collector agent disconnect.	<i>disable</i>	Disable logging of FSSO collector agent disconnect.			
Option	Description									
<i>enable</i>	Enable logging of FSSO collector agent disconnect.									
<i>disable</i>	Disable logging of FSSO collector agent disconnect.									
ssh-logs	Enable/disable SSH logs in alert email.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSH logs in alert email.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSH logs in alert email.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSH logs in alert email.	<i>disable</i>	Disable SSH logs in alert email.			
Option	Description									
<i>enable</i>	Enable SSH logs in alert email.									
<i>disable</i>	Disable SSH logs in alert email.									
FDS-license-expiring-days	Number of days to send alert email prior to FortiGuard license expiration .	integer	Minimum value: 1 Maximum value: 100	15						
local-disk-usage	Disk usage percentage at which to send alert email .	integer	Minimum value: 1 Maximum value: 99	75						
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	1						

Parameter	Description	Type	Size	Default						
alert-interval	Alert alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	2						
critical-interval	Critical alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	3						
error-interval	Error alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	5						
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	10						
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	20						
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	30						
debug-interval	Debug alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	60						
severity	Lowest severity level to log.	option	-	alert						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> </tbody> </table>		Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.		
Option	Description									
<i>emergency</i>	Emergency level.									
<i>alert</i>	Alert level.									

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																	
<i>critical</i>	Critical level.																	
<i>error</i>	Error level.																	
<i>warning</i>	Warning level.																	
<i>notification</i>	Notification level.																	
<i>information</i>	Information level.																	
<i>debug</i>	Debug level.																	

# antivirus

This section includes syntax for the following commands:

- [config antivirus heuristic on page 29](#)
- [config antivirus profile on page 34](#)
- [config antivirus quarantine on page 29](#)
- [config antivirus settings on page 28](#)

## config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
  Description: Configure AntiVirus settings.
  set use-extreme-db [enable|disable]
  set grayware [enable|disable]
  set override-timeout {integer}
end
```

## config antivirus settings

Parameter	Description	Type	Size	Default						
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable extreme AVDB.</td></tr><tr><td><i>disable</i></td><td>Disable extreme AVDB.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable extreme AVDB.	<i>disable</i>	Disable extreme AVDB.			
Option	Description									
<i>enable</i>	Enable extreme AVDB.									
<i>disable</i>	Disable extreme AVDB.									
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable grayware detection.</td></tr><tr><td><i>disable</i></td><td>Disable grayware detection.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable grayware detection.	<i>disable</i>	Disable grayware detection.			
Option	Description									
<i>enable</i>	Enable grayware detection.									
<i>disable</i>	Disable grayware detection.									
override-timeout	Override the large file scan timeout value in seconds . Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600	0						

## config antivirus heuristic

Configure global heuristic options.

```
config antivirus heuristic
  Description: Configure global heuristic options.
  set mode [pass|block|...]
end
```

## config antivirus heuristic

Parameter	Description	Type	Size	Default								
mode	Enable/disable heuristics and determine how the system behaves if heuristics detects a problem.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>pass</i></td><td>Enable heuristics but detected files are passed. If enabled, the system will record a log message.</td></tr><tr><td><i>block</i></td><td>Enable heuristics and detected files are blocked. If enabled, the system will record a log message.</td></tr><tr><td><i>disable</i></td><td>Turn off heuristics.</td></tr></tbody></table>	Option	Description	<i>pass</i>	Enable heuristics but detected files are passed. If enabled, the system will record a log message.	<i>block</i>	Enable heuristics and detected files are blocked. If enabled, the system will record a log message.	<i>disable</i>	Turn off heuristics.			
Option	Description											
<i>pass</i>	Enable heuristics but detected files are passed. If enabled, the system will record a log message.											
<i>block</i>	Enable heuristics and detected files are blocked. If enabled, the system will record a log message.											
<i>disable</i>	Turn off heuristics.											

## config antivirus quarantine

Configure quarantine options.

```
config antivirus quarantine
  Description: Configure quarantine options.
  set agelimit {integer}
  set maxfilesize {integer}
  set quarantine-quota {integer}
  set drop-infected {option1}, {option2}, ...
  set store-infected {option1}, {option2}, ...
  set drop-blocked {option1}, {option2}, ...
  set store-blocked {option1}, {option2}, ...
  set drop-heuristic {option1}, {option2}, ...
  set store-heuristic {option1}, {option2}, ...
  set lowspace [drop-new|ovrw-old]
  set destination [NULL|disk|...]
end
```

## config antivirus quarantine

Parameter	Description	Type	Size	Default
agelimit	Age limit for quarantined files .	integer	Minimum value: 0 Maximum value: 479	0
maxfilesize	Maximum file size to quarantine .	integer	Minimum value: 0 Maximum value: 500	0
quarantine-quota	The amount of disk space to reserve for quarantining files .	integer	Minimum value: 0 Maximum value: 4294967295	0
drop-infected	Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-	

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>https</i>	HTTPS.
<i>ftps</i>	FTPS.
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

Parameter	Description	Type	Size	Default
store-infected	Quarantine infected files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>https</i>	HTTPS.
<i>ftps</i>	FTPS.
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

drop-blocked	Do not quarantine dropped files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-
--------------	---	--------	---

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.

Parameter	Description	Type	Size	Default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>imaps</i></td> <td>IMAPS.</td> </tr> <tr> <td><i>smtps</i></td> <td>SMTPS.</td> </tr> <tr> <td><i>pop3s</i></td> <td>POP3S.</td> </tr> <tr> <td><i>ftps</i></td> <td>FTPS.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> </tbody> </table>	Option	Description	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.													
Option	Description																															
<i>nntp</i>	NNTP.																															
<i>imaps</i>	IMAPS.																															
<i>smtps</i>	SMTPS.																															
<i>pop3s</i>	POP3S.																															
<i>ftps</i>	FTPS.																															
<i>mapi</i>	MAPI.																															
<i>cifs</i>	CIFS.																															
<i>ssh</i>	SSH.																															
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s ftps mapi cifs ssh																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>imaps</i></td> <td>IMAPS.</td> </tr> <tr> <td><i>smtps</i></td> <td>SMTPS.</td> </tr> <tr> <td><i>pop3s</i></td> <td>POP3S.</td> </tr> <tr> <td><i>ftps</i></td> <td>FTPS.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> </tbody> </table>	Option	Description	<i>imap</i>	IMAP.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
Option	Description																															
<i>imap</i>	IMAP.																															
<i>smtp</i>	SMTP.																															
<i>pop3</i>	POP3.																															
<i>http</i>	HTTP.																															
<i>ftp</i>	FTP.																															
<i>nntp</i>	NNTP.																															
<i>imaps</i>	IMAPS.																															
<i>smtps</i>	SMTPS.																															
<i>pop3s</i>	POP3S.																															
<i>ftps</i>	FTPS.																															
<i>mapi</i>	MAPI.																															
<i>cifs</i>	CIFS.																															
<i>ssh</i>	SSH.																															



Parameter	Description	Type	Size	Default																														
drop-heuristic	Do not quarantine files detected by heuristics found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>imaps</i></td> <td>IMAPS.</td> </tr> <tr> <td><i>smtps</i></td> <td>SMTPS.</td> </tr> <tr> <td><i>pop3s</i></td> <td>POP3S.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS.</td> </tr> <tr> <td><i>ftps</i></td> <td>FTPS.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> </tbody> </table>	Option	Description	<i>imap</i>	IMAP.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
Option	Description																																	
<i>imap</i>	IMAP.																																	
<i>smtp</i>	SMTP.																																	
<i>pop3</i>	POP3.																																	
<i>http</i>	HTTP.																																	
<i>ftp</i>	FTP.																																	
<i>nntp</i>	NNTP.																																	
<i>imaps</i>	IMAPS.																																	
<i>smtps</i>	SMTPS.																																	
<i>pop3s</i>	POP3S.																																	
<i>https</i>	HTTPS.																																	
<i>ftps</i>	FTPS.																																	
<i>mapi</i>	MAPI.																																	
<i>cifs</i>	CIFS.																																	
<i>ssh</i>	SSH.																																	
store-heuristic	Quarantine files detected by heuristics found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> </tbody> </table>	Option	Description	<i>imap</i>	IMAP.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.																					
Option	Description																																	
<i>imap</i>	IMAP.																																	
<i>smtp</i>	SMTP.																																	
<i>pop3</i>	POP3.																																	
<i>http</i>	HTTP.																																	
<i>ftp</i>	FTP.																																	

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>imaps</i></td> <td>IMAPS.</td> </tr> <tr> <td><i>smtps</i></td> <td>SMTPS.</td> </tr> <tr> <td><i>pop3s</i></td> <td>POP3S.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS.</td> </tr> <tr> <td><i>ftps</i></td> <td>FTPS.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> </tbody> </table>	Option	Description	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
Option	Description																							
<i>nntp</i>	NNTP.																							
<i>imaps</i>	IMAPS.																							
<i>smtps</i>	SMTPS.																							
<i>pop3s</i>	POP3S.																							
<i>https</i>	HTTPS.																							
<i>ftps</i>	FTPS.																							
<i>mapi</i>	MAPI.																							
<i>cifs</i>	CIFS.																							
<i>ssh</i>	SSH.																							
lowspace	Select the method for handling additional files when running low on disk space.	option	-	ovrw-old																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop-new</i></td> <td>Drop (delete) the most recently quarantined files.</td> </tr> <tr> <td><i>ovrw-old</i></td> <td>Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.</td> </tr> </tbody> </table>	Option	Description	<i>drop-new</i>	Drop (delete) the most recently quarantined files.	<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																	
Option	Description																							
<i>drop-new</i>	Drop (delete) the most recently quarantined files.																							
<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																							
destination	Choose whether to quarantine files to the FortiGate disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	NULL **																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>NULL</i></td> <td>Files that would be quarantined are deleted.</td> </tr> <tr> <td><i>disk</i></td> <td>Quarantine files to the FortiGate hard disk.</td> </tr> <tr> <td><i>FortiAnalyzer</i></td> <td>FortiAnalyzer</td> </tr> </tbody> </table>	Option	Description	<i>NULL</i>	Files that would be quarantined are deleted.	<i>disk</i>	Quarantine files to the FortiGate hard disk.	<i>FortiAnalyzer</i>	FortiAnalyzer															
Option	Description																							
<i>NULL</i>	Files that would be quarantined are deleted.																							
<i>disk</i>	Quarantine files to the FortiGate hard disk.																							
<i>FortiAnalyzer</i>	FortiAnalyzer																							

\*\* Values may differ between models.

## config antivirus profile

Configure AntiVirus profiles.

```
config antivirus profile
  Description: Configure AntiVirus profiles.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set feature-set [flow|proxy]
    set ftgd-analytics [disable|suspicious|...]
```

```

set analytics-max-upload {integer}
set analytics-wl-filetype {integer}
set analytics-bl-filetype {integer}
set analytics-db [disable|enable]
set mobile-malware-db [disable|enable]
config http
  Description: Configure HTTP AntiVirus options.
  set options {option1}, {option2}, ...
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set emulator [enable|disable]
  set outbreak-prevention [disabled|files|...]
  set content-disarm [disable|enable]
end
config ftp
  Description: Configure FTP AntiVirus options.
  set options {option1}, {option2}, ...
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set emulator [enable|disable]
  set outbreak-prevention [disabled|files|...]
end
config imap
  Description: Configure IMAP AntiVirus options.
  set options {option1}, {option2}, ...
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set emulator [enable|disable]
  set executables [default|virus]
  set outbreak-prevention [disabled|files|...]
  set content-disarm [disable|enable]
end
config pop3
  Description: Configure POP3 AntiVirus options.
  set options {option1}, {option2}, ...
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set emulator [enable|disable]
  set executables [default|virus]
  set outbreak-prevention [disabled|files|...]
  set content-disarm [disable|enable]
end
config smtp
  Description: Configure SMTP AntiVirus options.
  set options {option1}, {option2}, ...
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...
  set emulator [enable|disable]
  set executables [default|virus]
  set outbreak-prevention [disabled|files|...]
  set content-disarm [disable|enable]
end
config mapi
  Description: Configure MAPI AntiVirus options.
  set options {option1}, {option2}, ...
  set archive-block {option1}, {option2}, ...
  set archive-log {option1}, {option2}, ...

```

```

    set emulator [enable|disable]
    set executables [default|virus]
    set outbreak-prevention [disabled|files|...]
end
config nntp
    Description: Configure NNTP AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set outbreak-prevention [disabled|files|...]
end
config cifs
    Description: Configure CIFS AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set outbreak-prevention [disabled|files|...]
end
config ssh
    Description: Configure SFTP and SCP AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set outbreak-prevention [disabled|files|...]
end
config nac-quar
    Description: Configure AntiVirus quarantine settings.
    set infected [none|quar-src-ip]
    set expiry {user}
    set log [enable|disable]
end
config outbreak-prevention
    Description: Configure Virus Outbreak Prevention settings.
    set ftgd-service [disable|enable]
    set external-blocklist [disable|enable]
end
config content-disarm
    Description: AV Content Disarm and Reconstruction settings.
    set original-file-destination [fortisandbox|quarantine|...]
    set error-action [block|log-only|...]
    set office-macro [disable|enable]
    set office-hylink [disable|enable]
    set office-linked [disable|enable]
    set office-embed [disable|enable]
    set office-dde [disable|enable]
    set office-action [disable|enable]
    set pdf-javacode [disable|enable]
    set pdf-embedfile [disable|enable]
    set pdf-hyperlink [disable|enable]
    set pdf-act-gotor [disable|enable]
    set pdf-act-launch [disable|enable]
    set pdf-act-sound [disable|enable]
    set pdf-act-movie [disable|enable]
    set pdf-act-java [disable|enable]

```

```

    set pdf-act-form [disable|enable]
    set cover-page [disable|enable]
    set detect-only [disable|enable]
end
set av-virus-log [enable|disable]
set av-block-log [enable|disable]
set extended-log [enable|disable]
set scan-mode [default|legacy]
next
end

```

## config antivirus profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35	
feature-set	Flow/proxy feature set.	option	-	flow
	<b>Option</b>	<b>Description</b>		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not upload files to FortiSandbox.		
	<i>suspicious</i>	Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.		
	<i>everything</i>	Submit all files scanned by AntiVirus to FortiSandbox. AntiVirus may not scan all files.		
analytics-max-upload	Maximum size of files that can be uploaded to FortiSandbox .	integer	Minimum value: 1 Maximum value: 186 **	10
analytics-wl-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
analytics-bl-filetype	Only submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0						
analytics-db	Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Use only the standard AV signature databases.</td> </tr> <tr> <td><i>enable</i></td> <td>Also use the FortiSandbox signature database.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Use only the standard AV signature databases.	<i>enable</i>	Also use the FortiSandbox signature database.			
Option	Description									
<i>disable</i>	Use only the standard AV signature databases.									
<i>enable</i>	Also use the FortiSandbox signature database.									
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not use the mobile malware signature database.</td> </tr> <tr> <td><i>enable</i></td> <td>Also use the mobile malware signature database.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not use the mobile malware signature database.	<i>enable</i>	Also use the mobile malware signature database.			
Option	Description									
<i>disable</i>	Do not use the mobile malware signature database.									
<i>enable</i>	Also use the mobile malware signature database.									
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
extended-log	Enable/disable extended logging for antivirus.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
scan-mode	Choose between default scan mode and legacy scan mode.	option	-	default						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>On the fly decompression and scanning of certain archive files.</td> </tr> <tr> <td><i>legacy</i></td> <td>Scan archive files only after the entire file is received.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	On the fly decompression and scanning of certain archive files.	<i>legacy</i>	Scan archive files only after the entire file is received.			
Option	Description									
<i>default</i>	On the fly decompression and scanning of certain archive files.									
<i>legacy</i>	Scan archive files only after the entire file is received.									

\*\* Values may differ between models.

## config http

Parameter	Description	Type	Size	Default																				
options	Enable/disable HTTP AntiVirus scanning, monitoring, and quarantine.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable HTTP antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable HTTP antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable HTTP antivirus scanning.	<i>avmonitor</i>	Enable HTTP antivirus logging.	<i>quarantine</i>	Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.															
Option	Description																							
<i>scan</i>	Enable HTTP antivirus scanning.																							
<i>avmonitor</i>	Enable HTTP antivirus logging.																							
<i>quarantine</i>	Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.																							
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.																	
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																			
<i>partiallycorrupted</i>	Log partially corrupted archives.																			
<i>multipart</i>	Log multipart archives.																			
<i>nested</i>	Log nested archives.																			
<i>mailbomb</i>	Log mail bomb archives.																			
<i>fileslimit</i>	Log exceeded archive files limit.																			
<i>timeout</i>	Log scan timeout.																			
<i>unhandled</i>	Log archives that FortiOS cannot open.																			
emulator	Enable/disable the virus emulator.	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.													
Option	Description																			
<i>enable</i>	Enable the virus emulator.																			
<i>disable</i>	Disable the virus emulator.																			
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.											
Option	Description																			
<i>disabled</i>	Disabled.																			
<i>files</i>	Analyze files as sent, not the content of archives.																			
<i>full-archive</i>	Analyze files including the content of archives.																			
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Content Disarm and Reconstruction for this protocol.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Content Disarm and Reconstruction for this protocol.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.													
Option	Description																			
<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.																			
<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.																			

## config ftp

Parameter	Description	Type	Size	Default				
options	Enable/disable FTP AntiVirus scanning, monitoring, and quarantine.	option	-					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable FTP antivirus scanning.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable FTP antivirus scanning.			
Option	Description							
<i>scan</i>	Enable FTP antivirus scanning.							



Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>avmonitor</i></td> <td>Enable FTP antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable FTP antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>avmonitor</i>	Enable FTP antivirus logging.	<i>quarantine</i>	Enable FTP antivirus quarantine. Files are quarantined depending on quarantine settings.																	
Option	Description																							
<i>avmonitor</i>	Enable FTP antivirus logging.																							
<i>quarantine</i>	Enable FTP antivirus quarantine. Files are quarantined depending on quarantine settings.																							
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.																			
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable the virus emulator.							
Option	Description											
<i>disable</i>	Disable the virus emulator.											
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.			
Option	Description											
<i>disabled</i>	Disabled.											
<i>files</i>	Analyze files as sent, not the content of archives.											
<i>full-archive</i>	Analyze files including the content of archives.											

### config imap

Parameter	Description	Type	Size	Default																				
options	Enable/disable IMAP AntiVirus scanning, monitoring, and quarantine.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable IMAP antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable IMAP antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable IMAP antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable IMAP antivirus scanning.	<i>avmonitor</i>	Enable IMAP antivirus logging.	<i>quarantine</i>	Enable IMAP antivirus quarantine. Files are quarantined depending on quarantine settings.															
Option	Description																							
<i>scan</i>	Enable IMAP antivirus scanning.																							
<i>avmonitor</i>	Enable IMAP antivirus logging.																							
<i>quarantine</i>	Enable IMAP antivirus quarantine. Files are quarantined depending on quarantine settings.																							
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																	
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							
<i>disable</i>	Disable the virus emulator.																							
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.																	
Option	Description																							
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																							
<i>virus</i>	Treat Windows executables as viruses.																							
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.															
Option	Description																							
<i>disabled</i>	Disabled.																							
<i>files</i>	Analyze files as sent, not the content of archives.																							
<i>full-archive</i>	Analyze files including the content of archives.																							
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Content Disarm and Reconstruction for this protocol.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Content Disarm and Reconstruction for this protocol.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.																	
Option	Description																							
<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.																							
<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.																							

## config pop3

Parameter	Description	Type	Size	Default																				
options	Enable/disable POP3 AntiVirus scanning, monitoring, and quarantine.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable POP3 antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable POP3 antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable POP3 antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable POP3 antivirus scanning.	<i>avmonitor</i>	Enable POP3 antivirus logging.	<i>quarantine</i>	Enable POP3 antivirus quarantine. Files are quarantined depending on quarantine settings.															
Option	Description																							
<i>scan</i>	Enable POP3 antivirus scanning.																							
<i>avmonitor</i>	Enable POP3 antivirus logging.																							
<i>quarantine</i>	Enable POP3 antivirus quarantine. Files are quarantined depending on quarantine settings.																							
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							

Parameter	Description	Type	Size	Default								
emulator	Enable/disable the virus emulator.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.					
Option	Description											
<i>enable</i>	Enable the virus emulator.											
<i>disable</i>	Disable the virus emulator.											
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.					
Option	Description											
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.											
<i>virus</i>	Treat Windows executables as viruses.											
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.			
Option	Description											
<i>disabled</i>	Disabled.											
<i>files</i>	Analyze files as sent, not the content of archives.											
<i>full-archive</i>	Analyze files including the content of archives.											
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Content Disarm and Reconstruction for this protocol.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Content Disarm and Reconstruction for this protocol.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.					
Option	Description											
<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.											
<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.											

## config smtp

Parameter	Description	Type	Size	Default								
options	Enable/disable SMTP AntiVirus scanning, monitoring, and quarantine.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable SMTP antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable SMTP antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable SMTP antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable SMTP antivirus scanning.	<i>avmonitor</i>	Enable SMTP antivirus logging.	<i>quarantine</i>	Enable SMTP antivirus quarantine. Files are quarantined depending on quarantine settings.			
Option	Description											
<i>scan</i>	Enable SMTP antivirus scanning.											
<i>avmonitor</i>	Enable SMTP antivirus logging.											
<i>quarantine</i>	Enable SMTP antivirus quarantine. Files are quarantined depending on quarantine settings.											

Parameter	Description	Type	Size	Default																				
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																	
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							
<i>disable</i>	Disable the virus emulator.																							
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																				

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.					
Option	Description											
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.											
<i>virus</i>	Treat Windows executables as viruses.											
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.			
Option	Description											
<i>disabled</i>	Disabled.											
<i>files</i>	Analyze files as sent, not the content of archives.											
<i>full-archive</i>	Analyze files including the content of archives.											
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Content Disarm and Reconstruction for this protocol.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Content Disarm and Reconstruction for this protocol.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.					
Option	Description											
<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.											
<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.											

## config mapi

Parameter	Description	Type	Size	Default								
options	Enable/disable MAPI AntiVirus scanning, monitoring, and quarantine.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable MAPI antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable MAPI antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable MAPI antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable MAPI antivirus scanning.	<i>avmonitor</i>	Enable MAPI antivirus logging.	<i>quarantine</i>	Enable MAPI antivirus quarantine. Files are quarantined depending on quarantine settings.			
Option	Description											
<i>scan</i>	Enable MAPI antivirus scanning.											
<i>avmonitor</i>	Enable MAPI antivirus logging.											
<i>quarantine</i>	Enable MAPI antivirus quarantine. Files are quarantined depending on quarantine settings.											
archive-block	Select the archive types to block.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.			
Option	Description											
<i>encrypted</i>	Block encrypted archives.											
<i>corrupted</i>	Block corrupted archives.											
<i>partiallycorrupted</i>	Block partially corrupted archives.											

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.									
Option	Description																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																	
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							
<i>disable</i>	Disable the virus emulator.																							
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Perform standard AntiVirus scanning of Windows executable files.</td> </tr> <tr> <td><i>virus</i></td> <td>Treat Windows executables as viruses.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.																	
Option	Description																							
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																							
<i>virus</i>	Treat Windows executables as viruses.																							
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled																				



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.			
Option	Description											
<i>disabled</i>	Disabled.											
<i>files</i>	Analyze files as sent, not the content of archives.											
<i>full-archive</i>	Analyze files including the content of archives.											

## config nntp

Parameter	Description	Type	Size	Default																				
options	Enable/disable NNTP AntiVirus scanning, monitoring, and quarantine.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable NNTP antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable NNTP antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable NNTP antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable NNTP antivirus scanning.	<i>avmonitor</i>	Enable NNTP antivirus logging.	<i>quarantine</i>	Enable NNTP antivirus quarantine. Files are quarantined depending on quarantine settings.															
Option	Description																							
<i>scan</i>	Enable NNTP antivirus scanning.																							
<i>avmonitor</i>	Enable NNTP antivirus logging.																							
<i>quarantine</i>	Enable NNTP antivirus quarantine. Files are quarantined depending on quarantine settings.																							
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.																	
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																			
<i>partiallycorrupted</i>	Log partially corrupted archives.																			
<i>multipart</i>	Log multipart archives.																			
<i>nested</i>	Log nested archives.																			
<i>mailbomb</i>	Log mail bomb archives.																			
<i>fileslimit</i>	Log exceeded archive files limit.																			
<i>timeout</i>	Log scan timeout.																			
<i>unhandled</i>	Log archives that FortiOS cannot open.																			
emulator	Enable/disable the virus emulator.	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.													
Option	Description																			
<i>enable</i>	Enable the virus emulator.																			
<i>disable</i>	Disable the virus emulator.																			
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.											
Option	Description																			
<i>disabled</i>	Disabled.																			
<i>files</i>	Analyze files as sent, not the content of archives.																			
<i>full-archive</i>	Analyze files including the content of archives.																			

### config cifs

Parameter	Description	Type	Size	Default								
options	Enable/disable CIFS AntiVirus scanning, monitoring, and quarantine.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable CIFS antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable CIFS antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable CIFS antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable CIFS antivirus scanning.	<i>avmonitor</i>	Enable CIFS antivirus logging.	<i>quarantine</i>	Enable CIFS antivirus quarantine. Files are quarantined depending on quarantine settings.			
Option	Description											
<i>scan</i>	Enable CIFS antivirus scanning.											
<i>avmonitor</i>	Enable CIFS antivirus logging.											
<i>quarantine</i>	Enable CIFS antivirus quarantine. Files are quarantined depending on quarantine settings.											
archive-block	Select the archive types to block.	option	-									

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																	
Option	Description																							
<i>enable</i>	Enable the virus emulator.																							
<i>disable</i>	Disable the virus emulator.																							
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.																			
Option	Description																							
<i>disabled</i>	Disabled.																							

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.			
Option	Description									
<i>files</i>	Analyze files as sent, not the content of archives.									
<i>full-archive</i>	Analyze files including the content of archives.									

## config ssh

Parameter	Description	Type	Size	Default																				
options	Enable/disable SFTP and SCP AntiVirus scanning, monitoring, and quarantine.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scan</i></td> <td>Enable SSH antivirus scanning.</td> </tr> <tr> <td><i>avmonitor</i></td> <td>Enable SSH antivirus logging.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Enable SSH antivirus quarantine. Files are quarantined depending on quarantine settings.</td> </tr> </tbody> </table>	Option	Description	<i>scan</i>	Enable SSH antivirus scanning.	<i>avmonitor</i>	Enable SSH antivirus logging.	<i>quarantine</i>	Enable SSH antivirus quarantine. Files are quarantined depending on quarantine settings.															
Option	Description																							
<i>scan</i>	Enable SSH antivirus scanning.																							
<i>avmonitor</i>	Enable SSH antivirus logging.																							
<i>quarantine</i>	Enable SSH antivirus quarantine. Files are quarantined depending on quarantine settings.																							
archive-block	Select the archive types to block.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Block encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Block corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Block partially corrupted archives.</td> </tr> <tr> <td><i>multipart</i></td> <td>Block multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Block nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Block mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Block exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Block scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Block archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>encrypted</i></td> <td>Log encrypted archives.</td> </tr> <tr> <td><i>corrupted</i></td> <td>Log corrupted archives.</td> </tr> <tr> <td><i>partiallycorrupted</i></td> <td>Log partially corrupted archives.</td> </tr> </tbody> </table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.															
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>multipart</i></td> <td>Log multipart archives.</td> </tr> <tr> <td><i>nested</i></td> <td>Log nested archives.</td> </tr> <tr> <td><i>mailbomb</i></td> <td>Log mail bomb archives.</td> </tr> <tr> <td><i>fileslimit</i></td> <td>Log exceeded archive files limit.</td> </tr> <tr> <td><i>timeout</i></td> <td>Log scan timeout.</td> </tr> <tr> <td><i>unhandled</i></td> <td>Log archives that FortiOS cannot open.</td> </tr> </tbody> </table>	Option	Description	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																	
<i>multipart</i>	Log multipart archives.																	
<i>nested</i>	Log nested archives.																	
<i>mailbomb</i>	Log mail bomb archives.																	
<i>fileslimit</i>	Log exceeded archive files limit.																	
<i>timeout</i>	Log scan timeout.																	
<i>unhandled</i>	Log archives that FortiOS cannot open.																	
emulator	Enable/disable the virus emulator.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the virus emulator.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the virus emulator.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.											
Option	Description																	
<i>enable</i>	Enable the virus emulator.																	
<i>disable</i>	Disable the virus emulator.																	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-	disabled														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> <tr> <td><i>files</i></td> <td>Analyze files as sent, not the content of archives.</td> </tr> <tr> <td><i>full-archive</i></td> <td>Analyze files including the content of archives.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.									
Option	Description																	
<i>disabled</i>	Disabled.																	
<i>files</i>	Analyze files as sent, not the content of archives.																	
<i>full-archive</i>	Analyze files including the content of archives.																	

### config nac-quar

Parameter	Description	Type	Size	Default						
infected	Enable/Disable quarantining infected hosts to the banned user list.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Do not quarantine infected hosts.</td> </tr> <tr> <td><i>quar-src-ip</i></td> <td>Quarantine all traffic from the infected hosts source IP.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Do not quarantine infected hosts.	<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.			
Option	Description									
<i>none</i>	Do not quarantine infected hosts.									
<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.									
expiry	Duration of quarantine.	user	Not Specified	5m						
log	Enable/disable AntiVirus quarantine logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AntiVirus quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AntiVirus quarantine logging.					
Option	Description									
<i>enable</i>	Enable AntiVirus quarantine logging.									

Parameter	Description	Type	Size	Default				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable AntiVirus quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable AntiVirus quarantine logging.			
Option	Description							
<i>disable</i>	Disable AntiVirus quarantine logging.							

### config outbreak-prevention

Parameter	Description	Type	Size	Default						
ftgd-service	Enable/disable FortiGuard Virus outbreak prevention service.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable FortiGuard Virus Outbreak Prevention service.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable FortiGuard Virus Outbreak Prevention service.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable FortiGuard Virus Outbreak Prevention service.	<i>enable</i>	Enable FortiGuard Virus Outbreak Prevention service.			
Option	Description									
<i>disable</i>	Disable FortiGuard Virus Outbreak Prevention service.									
<i>enable</i>	Enable FortiGuard Virus Outbreak Prevention service.									
external-blocklist	Enable/disable external malware blocklist.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable external malware blocklist.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable external malware blocklist.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable external malware blocklist.	<i>enable</i>	Enable external malware blocklist.			
Option	Description									
<i>disable</i>	Disable external malware blocklist.									
<i>enable</i>	Enable external malware blocklist.									

### config content-disarm

Parameter	Description	Type	Size	Default								
original-file-destination	Destination to send original file if active content is removed.	option	-	discard								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortisandbox</i></td> <td>Send original file to configured FortiSandbox.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Send original file to quarantine.</td> </tr> <tr> <td><i>discard</i></td> <td>Original file will be discarded after content disarm.</td> </tr> </tbody> </table>	Option	Description	<i>fortisandbox</i>	Send original file to configured FortiSandbox.	<i>quarantine</i>	Send original file to quarantine.	<i>discard</i>	Original file will be discarded after content disarm.			
Option	Description											
<i>fortisandbox</i>	Send original file to configured FortiSandbox.											
<i>quarantine</i>	Send original file to quarantine.											
<i>discard</i>	Original file will be discarded after content disarm.											
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block file on CDR error.</td> </tr> <tr> <td><i>log-only</i></td> <td>Log CDR error, but allow file.</td> </tr> <tr> <td><i>ignore</i></td> <td>Do nothing on CDR error.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block file on CDR error.	<i>log-only</i>	Log CDR error, but allow file.	<i>ignore</i>	Do nothing on CDR error.			
Option	Description											
<i>block</i>	Block file on CDR error.											
<i>log-only</i>	Log CDR error, but allow file.											
<i>ignore</i>	Do nothing on CDR error.											

Parameter	Description	Type	Size	Default
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-dde	Enable/disable stripping of Dynamic Data Exchange events in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		

Parameter	Description	Type	Size	Default
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		



Parameter	Description	Type	Size	Default						
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this Content Disarm and Reconstruction feature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this Content Disarm and Reconstruction feature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this Content Disarm and Reconstruction feature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this Content Disarm and Reconstruction feature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this Content Disarm and Reconstruction feature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this Content Disarm and Reconstruction feature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this Content Disarm and Reconstruction feature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this Content Disarm and Reconstruction feature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this Content Disarm and Reconstruction feature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this Content Disarm and Reconstruction feature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									

## application

This section includes syntax for the following commands:

- [config application list on page 61](#)
- [config application name on page 58](#)
- [config application rule-settings on page 61](#)
- [config application custom on page 60](#)
- [config application group on page 69](#)

### config application name

Configure application signatures.

```
config application name
  Description: Configure application signatures.
  edit <name>
    set id {integer}
    set category {integer}
    set popularity {integer}
    set risk {integer}
    set weight {integer}
    set protocol {user}
    set technology {user}
    set behavior {user}
    set vendor {user}
  config parameters
    Description: Application parameters.
    edit <name>
      set default value {string}
    next
  end
  config metadata
    Description: Meta data.
    edit <id>
      set metaid {integer}
      set valueid {integer}
    next
  end
next
end
```

## config application name

Parameter	Description	Type	Size	Default
id	Application ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
popularity	Application popularity.	integer	Minimum value: 0 Maximum value: 255	0
risk	Application risk.	integer	Minimum value: 0 Maximum value: 255	0
weight	Application weight.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Application protocol.	user	Not Specified	
technology	Application technology.	user	Not Specified	
behavior	Application behavior.	user	Not Specified	
vendor	Application vendor.	user	Not Specified	

## config parameters

Parameter	Description	Type	Size	Default
default value	Parameter default value.	string	Maximum length: 199	

## config metadata

Parameter	Description	Type	Size	Default
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config application custom

Configure custom application signatures.

```
config application custom
  Description: Configure custom application signatures.
  edit <tag>
    set id {integer}
    set comment {string}
    set signature {var-string}
    set category {integer}
    set protocol {user}
    set technology {user}
    set behavior {user}
    set vendor {user}
  next
end
```

## config application custom

Parameter	Description	Type	Size	Default
id	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	string	Maximum length: 63	
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095	

Parameter	Description	Type	Size	Default
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Custom application signature protocol.	user	Not Specified	
technology	Custom application signature technology.	user	Not Specified	
behavior	Custom application signature behavior.	user	Not Specified	
vendor	Custom application signature vendor.	user	Not Specified	

## config application rule-settings

Configure application rule settings.

```
config application rule-settings
  Description: Configure application rule settings.
  edit <id>
    next
  end
```

## config application list

Configure application control lists.

```
config application list
  Description: Configure application control lists.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set extended-log [enable|disable]
    set other-application-action [pass|block]
    set app-replacemsg [disable|enable]
    set other-application-log [disable|enable]
    set enforce-default-app-port [disable|enable]
    set force-inclusion-ssl-di-sigs [disable|enable]
    set unknown-application-action [pass|block]
    set unknown-application-log [disable|enable]
    set p2p-black-list {option1}, {option2}, ...
    set deep-app-inspection [disable|enable]
    set options {option1}, {option2}, ...
  config entries
    Description: Application list entries.
    edit <id>
      set risk <level1>, <level2>, ...
      set category <id1>, <id2>, ...
      set application <id1>, <id2>, ...
      set protocols {user}
      set vendor {user}
      set technology {user}
```

```

set behavior {user}
set popularity {option1}, {option2}, ...
set exclusion <id1>, <id2>, ...
config parameters
  Description: Application parameters.
  edit <id>
    config members
      Description: Parameter tuple members.
      edit <id>
        set name {string}
        set value {string}
      next
    end
  next
end
set action [pass|block|...]
set log [disable|enable]
set log-packet [disable|enable]
set rate-count {integer}
set rate-duration {integer}
set rate-mode [periodical|continuous]
set rate-track [none|src-ip|...]
set session-ttl {integer}
set shaper {string}
set shaper-reverse {string}
set per-ip-shaper {string}
set quarantine [none|attacker]
set quarantine-expiry {user}
set quarantine-log [disable|enable]
next
end
set control-default-network-services [disable|enable]
config default-network-services
  Description: Default network service entries.
  edit <id>
    set port {integer}
    set services {option1}, {option2}, ...
    set violation-action [pass|monitor|...]
  next
end
next
end

```

## config application list

Parameter	Description	Type	Size	Default
comment	comments	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
extended-log	Enable/disable extended logging.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
other-application-action	Action for other applications.	option	-	pass						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow sessions matching an application in this application list.</td> </tr> <tr> <td><i>block</i></td> <td>Block sessions matching an application in this application list.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow sessions matching an application in this application list.	<i>block</i>	Block sessions matching an application in this application list.			
Option	Description									
<i>pass</i>	Allow sessions matching an application in this application list.									
<i>block</i>	Block sessions matching an application in this application list.									
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable replacement messages for blocked applications.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable replacement messages for blocked applications.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable replacement messages for blocked applications.	<i>enable</i>	Enable replacement messages for blocked applications.			
Option	Description									
<i>disable</i>	Disable replacement messages for blocked applications.									
<i>enable</i>	Enable replacement messages for blocked applications.									
other-application-log	Enable/disable logging for other applications.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for other applications.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for other applications.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for other applications.	<i>enable</i>	Enable logging for other applications.			
Option	Description									
<i>disable</i>	Disable logging for other applications.									
<i>enable</i>	Enable logging for other applications.									
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable default application port enforcement.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable default application port enforcement.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable default application port enforcement.	<i>enable</i>	Enable default application port enforcement.			
Option	Description									
<i>disable</i>	Disable default application port enforcement.									
<i>enable</i>	Enable default application port enforcement.									
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable forced inclusion of signatures which normally require SSL deep inspection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable forced inclusion of signatures which normally require SSL deep inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.	<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.					
Option	Description											
<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.											
<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.											
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow unknown applications.</td> </tr> <tr> <td><i>block</i></td> <td>Drop or block unknown applications.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow unknown applications.	<i>block</i>	Drop or block unknown applications.					
Option	Description											
<i>pass</i>	Pass or allow unknown applications.											
<i>block</i>	Drop or block unknown applications.											
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for unknown applications.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for unknown applications.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for unknown applications.	<i>enable</i>	Enable logging for unknown applications.					
Option	Description											
<i>disable</i>	Disable logging for unknown applications.											
<i>enable</i>	Enable logging for unknown applications.											
p2p-black-list	P2P applications to be black listed.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>skype</i></td> <td>Skype.</td> </tr> <tr> <td><i>edonkey</i></td> <td>Edonkey.</td> </tr> <tr> <td><i>bittorrent</i></td> <td>Bit torrent.</td> </tr> </tbody> </table>	Option	Description	<i>skype</i>	Skype.	<i>edonkey</i>	Edonkey.	<i>bittorrent</i>	Bit torrent.			
Option	Description											
<i>skype</i>	Skype.											
<i>edonkey</i>	Edonkey.											
<i>bittorrent</i>	Bit torrent.											
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable deep application inspection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable deep application inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable deep application inspection.	<i>enable</i>	Enable deep application inspection.					
Option	Description											
<i>disable</i>	Disable deep application inspection.											
<i>enable</i>	Enable deep application inspection.											
options	Basic application protocol signatures allowed by default.	option	-	allow-dns								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow-dns</i></td> <td>Allow DNS.</td> </tr> </tbody> </table>	Option	Description	<i>allow-dns</i>	Allow DNS.							
Option	Description											
<i>allow-dns</i>	Allow DNS.											



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow-icmp</i></td> <td>Allow ICMP.</td> </tr> <tr> <td><i>allow-http</i></td> <td>Allow generic HTTP web browsing.</td> </tr> <tr> <td><i>allow-ssl</i></td> <td>Allow generic SSL communication.</td> </tr> <tr> <td><i>allow-quit</i></td> <td>Allow QUIC.</td> </tr> </tbody> </table>	Option	Description	<i>allow-icmp</i>	Allow ICMP.	<i>allow-http</i>	Allow generic HTTP web browsing.	<i>allow-ssl</i>	Allow generic SSL communication.	<i>allow-quit</i>	Allow QUIC.			
Option	Description													
<i>allow-icmp</i>	Allow ICMP.													
<i>allow-http</i>	Allow generic HTTP web browsing.													
<i>allow-ssl</i>	Allow generic SSL communication.													
<i>allow-quit</i>	Allow QUIC.													
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable protocol enforcement over selected ports.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable protocol enforcement over selected ports.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable protocol enforcement over selected ports.	<i>enable</i>	Enable protocol enforcement over selected ports.							
Option	Description													
<i>disable</i>	Disable protocol enforcement over selected ports.													
<i>enable</i>	Enable protocol enforcement over selected ports.													

## config entries

Parameter	Description	Type	Size	Default
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295	
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
protocols	Application protocol filter.	user	Not Specified	all
vendor	Application vendor filter.	user	Not Specified	all
technology	Application technology filter.	user	Not Specified	all
behavior	Application behavior filter.	user	Not Specified	all

Parameter	Description	Type	Size	Default												
popularity	Application popularity filter .	option	-	1 2 3 4 5												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Popularity level 1.</td> </tr> <tr> <td>2</td> <td>Popularity level 2.</td> </tr> <tr> <td>3</td> <td>Popularity level 3.</td> </tr> <tr> <td>4</td> <td>Popularity level 4.</td> </tr> <tr> <td>5</td> <td>Popularity level 5.</td> </tr> </tbody> </table>	Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.			
Option	Description															
1	Popularity level 1.															
2	Popularity level 2.															
3	Popularity level 3.															
4	Popularity level 4.															
5	Popularity level 5.															
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
action	Pass or block traffic, or reset connection for traffic from this application.	option	-	block												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow matching traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block or drop matching traffic.</td> </tr> <tr> <td><i>reset</i></td> <td>Reset sessions for matching traffic.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.	<i>reset</i>	Reset sessions for matching traffic.							
Option	Description															
<i>pass</i>	Pass or allow matching traffic.															
<i>block</i>	Block or drop matching traffic.															
<i>reset</i>	Reset sessions for matching traffic.															
log	Enable/disable logging for this application list.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.									
Option	Description															
<i>disable</i>	Disable logging.															
<i>enable</i>	Enable logging.															
log-packet	Enable/disable packet logging.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable packet logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.									
Option	Description															
<i>disable</i>	Disable packet logging.															
<i>enable</i>	Enable packet logging.															
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0												

Parameter	Description	Type	Size	Default												
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60												
rate-mode	Rate limit mode.	option	-	continuous												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>periodical</i></td> <td>Allow configured number of packets every rate-duration.</td> </tr> <tr> <td><i>continuous</i></td> <td>Block packets once the rate is reached.</td> </tr> </tbody> </table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.									
Option	Description															
<i>periodical</i>	Allow configured number of packets every rate-duration.															
<i>continuous</i>	Block packets once the rate is reached.															
rate-track	Track the packet protocol field.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>none</td> </tr> <tr> <td><i>src-ip</i></td> <td>Source IP.</td> </tr> <tr> <td><i>dest-ip</i></td> <td>Destination IP.</td> </tr> <tr> <td><i>dhcp-client-mac</i></td> <td>DHCP client.</td> </tr> <tr> <td><i>dns-domain</i></td> <td>DNS domain.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
Option	Description															
<i>none</i>	none															
<i>src-ip</i>	Source IP.															
<i>dest-ip</i>	Destination IP.															
<i>dhcp-client-mac</i>	DHCP client.															
<i>dns-domain</i>	DNS domain.															
session-ttl	Session TTL .	integer	Minimum value: 0 Maximum value: 4294967295	0												
shaper	Traffic shaper.	string	Maximum length: 35													
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35													
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35													
quarantine	Quarantine method.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
Option	Description															
<i>none</i>	Quarantine is disabled.															
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.															
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m												

Parameter	Description	Type	Size	Default						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
Option	Description									
<i>disable</i>	Disable quarantine logging.									
<i>enable</i>	Enable quarantine logging.									

### config members

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

### config default-network-services

Parameter	Description	Type	Size	Default																								
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0																								
services	Network protocols.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>dns</i></td> <td>DNS.</td> </tr> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP.	<i>ssh</i>	SSH.	<i>telnet</i>	TELNET.	<i>ftp</i>	FTP.	<i>dns</i>	DNS.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>snmp</i>	SNMP.	<i>nntp</i>	NNTP.	<i>https</i>	HTTPS.			
Option	Description																											
<i>http</i>	HTTP.																											
<i>ssh</i>	SSH.																											
<i>telnet</i>	TELNET.																											
<i>ftp</i>	FTP.																											
<i>dns</i>	DNS.																											
<i>smtp</i>	SMTP.																											
<i>pop3</i>	POP3.																											
<i>imap</i>	IMAP.																											
<i>snmp</i>	SNMP.																											
<i>nntp</i>	NNTP.																											
<i>https</i>	HTTPS.																											

Parameter	Description	Type	Size	Default								
violation-action	Action for protocols not white listed under selected port.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow protocols not white listed under selected port.</td> </tr> <tr> <td><i>monitor</i></td> <td>Monitor protocols not white listed under selected port.</td> </tr> <tr> <td><i>block</i></td> <td>Block protocols not white listed under selected port.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow protocols not white listed under selected port.	<i>monitor</i>	Monitor protocols not white listed under selected port.	<i>block</i>	Block protocols not white listed under selected port.			
Option	Description											
<i>pass</i>	Allow protocols not white listed under selected port.											
<i>monitor</i>	Monitor protocols not white listed under selected port.											
<i>block</i>	Block protocols not white listed under selected port.											

## config application group

Configure firewall application groups.

```

config application group
  Description: Configure firewall application groups.
  edit <name>
    set comment {var-string}
    set type [application|category]
    set application <id1>, <id2>, ...
    set category <id1>, <id2>, ...
  next
end

```

## config application group

Parameter	Description	Type	Size	Default						
comment	Comment	var-string	Maximum length: 255							
type	Application group type.	option	-	application						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>application</i></td> <td>Application ID.</td> </tr> <tr> <td><i>category</i></td> <td>Application category ID.</td> </tr> </tbody> </table>	Option	Description	<i>application</i>	Application ID.	<i>category</i>	Application category ID.			
Option	Description									
<i>application</i>	Application ID.									
<i>category</i>	Application category ID.									
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295							

## authentication

This section includes syntax for the following commands:

- [config authentication setting on page 73](#)
- [config authentication rule on page 71](#)
- [config authentication scheme on page 70](#)

### config authentication scheme

Configure Authentication Schemes.

```
config authentication scheme
  Description: Configure Authentication Schemes.
  edit <name>
    set method {option1}, {option2}, ...
    set negotiate-ntlm [enable|disable]
    set kerberos-keytab {string}
    set domain-controller {string}
    set fssso-agent-for-ntlm {string}
    set require-tfa [enable|disable]
    set fssso-guest [enable|disable]
    set user-database <name1>, <name2>, ...
    set ssh-ca {string}
  next
end
```

### config authentication scheme

Parameter	Description	Type	Size	Default																		
method	Authentication methods .	option	-																			
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>digest</i></td><td>Digest HTTP authentication.</td></tr><tr><td><i>form</i></td><td>Form-based HTTP authentication.</td></tr><tr><td><i>negotiate</i></td><td>Negotiate authentication.</td></tr><tr><td><i>fssso</i></td><td>Fortinet Single Sign-On (FSSO) authentication.</td></tr><tr><td><i>rssso</i></td><td>RADIUS Single Sign-On (RSSO) authentication.</td></tr><tr><td><i>ssh-publickey</i></td><td>Public key based SSH authentication.</td></tr></tbody></table>	Option	Description	<i>ntlm</i>	NTLM authentication.	<i>basic</i>	Basic HTTP authentication.	<i>digest</i>	Digest HTTP authentication.	<i>form</i>	Form-based HTTP authentication.	<i>negotiate</i>	Negotiate authentication.	<i>fssso</i>	Fortinet Single Sign-On (FSSO) authentication.	<i>rssso</i>	RADIUS Single Sign-On (RSSO) authentication.	<i>ssh-publickey</i>	Public key based SSH authentication.			
Option	Description																					
<i>ntlm</i>	NTLM authentication.																					
<i>basic</i>	Basic HTTP authentication.																					
<i>digest</i>	Digest HTTP authentication.																					
<i>form</i>	Form-based HTTP authentication.																					
<i>negotiate</i>	Negotiate authentication.																					
<i>fssso</i>	Fortinet Single Sign-On (FSSO) authentication.																					
<i>rssso</i>	RADIUS Single Sign-On (RSSO) authentication.																					
<i>ssh-publickey</i>	Public key based SSH authentication.																					

Parameter	Description	Type	Size	Default						
negotiate-ntlm	Enable/disable negotiate authentication for NTLM .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negotiate authentication for NTLM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negotiate authentication for NTLM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negotiate authentication for NTLM.	<i>disable</i>	Disable negotiate authentication for NTLM.			
Option	Description									
<i>enable</i>	Enable negotiate authentication for NTLM.									
<i>disable</i>	Disable negotiate authentication for NTLM.									
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35							
domain-controller	Domain controller setting.	string	Maximum length: 35							
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35							
require-tfa	Enable/disable two-factor authentication .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable two-factor authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable two-factor authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable two-factor authentication.	<i>disable</i>	Disable two-factor authentication.			
Option	Description									
<i>enable</i>	Enable two-factor authentication.									
<i>disable</i>	Disable two-factor authentication.									
fsso-guest	Enable/disable user fsso-guest authentication .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable user fsso-guest authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable user fsso-guest authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable user fsso-guest authentication.	<i>disable</i>	Disable user fsso-guest authentication.			
Option	Description									
<i>enable</i>	Enable user fsso-guest authentication.									
<i>disable</i>	Disable user fsso-guest authentication.									
user-database <name>	Authentication server to contain user information; "local" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79							
ssh-ca	SSH CA name.	string	Maximum length: 35							

## config authentication rule

Configure Authentication Rules.

```

config authentication rule
  Description: Configure Authentication Rules.
  edit <name>
    set status [enable|disable]
    set protocol [http|ftp|...]
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set ip-based [enable|disable]
    set active-auth-method {string}
  
```

```

set sso-auth-method {string}
set web-auth-cookie [enable|disable]
set transaction-based [enable|disable]
set web-portal [enable|disable]
set comments {var-string}
next
end

```

## config authentication rule

Parameter	Description	Type	Size	Default										
status	Enable/disable this authentication rule.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this authentication rule.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this authentication rule.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this authentication rule.	<i>disable</i>	Disable this authentication rule.							
Option	Description													
<i>enable</i>	Enable this authentication rule.													
<i>disable</i>	Disable this authentication rule.													
protocol	Authentication is required for the selected protocol .	option	-	http										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP traffic is matched and authentication is required.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP traffic is matched and authentication is required.</td> </tr> <tr> <td><i>socks</i></td> <td>SOCKS traffic is matched and authentication is required.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH traffic is matched and authentication is required.</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP traffic is matched and authentication is required.	<i>ftp</i>	FTP traffic is matched and authentication is required.	<i>socks</i>	SOCKS traffic is matched and authentication is required.	<i>ssh</i>	SSH traffic is matched and authentication is required.			
Option	Description													
<i>http</i>	HTTP traffic is matched and authentication is required.													
<i>ftp</i>	FTP traffic is matched and authentication is required.													
<i>socks</i>	SOCKS traffic is matched and authentication is required.													
<i>ssh</i>	SSH traffic is matched and authentication is required.													
srcaddr <name>	Authentication is required for the selected IPv4 source address. Address name.	string	Maximum length: 79											
srcaddr6 <name>	Authentication is required for the selected IPv6 source address. Address name.	string	Maximum length: 79											
ip-based	Enable/disable IP-based authentication. When enabled, previously authenticated users from the same IP address will be exempted.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IP-based authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IP-based authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IP-based authentication.	<i>disable</i>	Disable IP-based authentication.							
Option	Description													
<i>enable</i>	Enable IP-based authentication.													
<i>disable</i>	Disable IP-based authentication.													
active-auth-method	Select an active authentication method.	string	Maximum length: 35											
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35											



Parameter	Description	Type	Size	Default						
web-auth-cookie	Enable/disable Web authentication cookies .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Web authentication cookie.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Web authentication cookie.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Web authentication cookie.	<i>disable</i>	Disable Web authentication cookie.			
Option	Description									
<i>enable</i>	Enable Web authentication cookie.									
<i>disable</i>	Disable Web authentication cookie.									
transaction-based	Enable/disable transaction based authentication .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable transaction based authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable transaction based authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable transaction based authentication.	<i>disable</i>	Disable transaction based authentication.			
Option	Description									
<i>enable</i>	Enable transaction based authentication.									
<i>disable</i>	Disable transaction based authentication.									
web-portal	Enable/disable web portal for proxy transparent policy .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable web-portal.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable web-portal.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable web-portal.	<i>disable</i>	Disable web-portal.			
Option	Description									
<i>enable</i>	Enable web-portal.									
<i>disable</i>	Disable web-portal.									
comments	Comment.	var-string	Maximum length: 1023							

## config authentication setting

Configure authentication setting.

```

config authentication setting
  Description: Configure authentication setting.
  set active-auth-scheme {string}
  set sso-auth-scheme {string}
  set captive-portal-type [fqdn|ip]
  set captive-portal-ip {ipv4-address-any}
  set captive-portal-ip6 {ipv6-address}
  set captive-portal {string}
  set captive-portal6 {string}
  set captive-portal-port {integer}
  set auth-https [enable|disable]
  set captive-portal-ssl-port {integer}
end

```

## config authentication setting

Parameter	Description	Type	Size	Default						
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35							
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35							
captive-portal-type	Captive portal type.	option	-	fqdn						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fqdn</i></td> <td>Use FQDN for captive portal.</td> </tr> <tr> <td><i>ip</i></td> <td>Use an IP address for captive portal.</td> </tr> </tbody> </table>	Option	Description	<i>fqdn</i>	Use FQDN for captive portal.	<i>ip</i>	Use an IP address for captive portal.			
Option	Description									
<i>fqdn</i>	Use FQDN for captive portal.									
<i>ip</i>	Use an IP address for captive portal.									
captive-portal-ip	Captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0						
captive-portal-ip6	Captive portal IPv6 address.	ipv6-address	Not Specified	::						
captive-portal	Captive portal host name.	string	Maximum length: 255							
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255							
captive-portal-port	Captive portal port number .	integer	Minimum value: 1 Maximum value: 65535	7830						
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
captive-portal-ssl-port	Captive portal SSL port number .	integer	Minimum value: 1 Maximum value: 65535	7831						

## certificate

This section includes syntax for the following commands:

- [config certificate remote on page 76](#)
- [config certificate local on page 77](#)
- [config certificate crl on page 80](#)
- [config certificate ca on page 75](#)

### config certificate ca

CA certificate.

```
config certificate ca
  Description: CA certificate.
  edit <name>
    set ca {user}
    set range [global|vdom]
    set source [factory|user|...]
    set ssl-inspection-trusted [enable|disable]
    set scep-url {string}
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set source-ip {ipv4-address}
  next
end
```

### config certificate ca

Parameter	Description	Type	Size	Default						
ca	CA certificate as a PEM file.	user	Not Specified							
range	Either global or VDOM IP address range for the CA certificate.	option	-	global						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></tbody></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.			
Option	Description									
<i>global</i>	Global range.									
<i>vdom</i>	VDOM IP address range.									
source	CA certificate source type.	option	-	user						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr></tbody></table>	Option	Description	<i>factory</i>	Factory installed certificate.					
Option	Description									
<i>factory</i>	Factory installed certificate.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>user</i></td> <td>User generated certificate.</td> </tr> <tr> <td><i>bundle</i></td> <td>Bundle file certificate.</td> </tr> </tbody> </table>	Option	Description	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description									
<i>user</i>	User generated certificate.									
<i>bundle</i>	Bundle file certificate.									
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Trusted CA for SSL inspection.</td> </tr> <tr> <td><i>disable</i></td> <td>Untrusted CA for SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Trusted CA for SSL inspection.	<i>disable</i>	Untrusted CA for SSL inspection.			
Option	Description									
<i>enable</i>	Trusted CA for SSL inspection.									
<i>disable</i>	Untrusted CA for SSL inspection.									
scep-url	URL of the SCEP server.	string	Maximum length: 255							
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295	0						
auto-update-days-warning	Number of days before an expiry-warning message is generated .	integer	Minimum value: 0 Maximum value: 4294967295	0						
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0						

## config certificate remote

Remote certificate as a PEM file.

```

config certificate remote
  Description: Remote certificate as a PEM file.
  edit <name>
    set remote {user}
    set range [global|vdom]
    set source [factory|user|...]
  next
end

```

## config certificate remote

Parameter	Description	Type	Size	Default								
remote	Remote certificate.	user	Not Specified									
range	Either the global or VDOM IP address range for the remote certificate.	option	-	global								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></tbody></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Remote certificate source type.	option	-	user								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></tbody></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

## config certificate local

Local keys and certificates.

```
config certificate local
  Description: Local keys and certificates.
  edit <name>
    set password {password}
    set comments {string}
    set private-key {user}
    set certificate {user}
    set csr {user}
    set state {user}
    set scep-url {string}
    set range [global|vdom]
    set source [factory|user|...]
    set auto-regenerate-days {integer}
    set auto-regenerate-days-warning {integer}
    set scep-password {password}
    set ca-identifier {string}
    set name-encoding [printable|utf8]
    set source-ip {ipv4-address}
    set ike-localid {string}
    set ike-localid-type [asn1dn|fqdn]
    set enroll-protocol [none|scep|...]
    set cmp-server {string}
    set cmp-path {string}
    set cmp-server-cert {string}
    set cmp-regeneration-method [keyupdate|renewal]
```

next  
end

## config certificate local

Parameter	Description	Type	Size	Default								
password	Password as a PEM file.	password	Not Specified									
comments	Comment.	string	Maximum length: 511									
private-key	PEM format key, encrypted with a password.	user	Not Specified									
certificate	PEM format certificate.	user	Not Specified									
csr	Certificate Signing Request.	user	Not Specified									
state	Certificate Signing Request State.	user	Not Specified									
scep-url	SCEP server URL.	string	Maximum length: 255									
range	Either a global or VDOM IP address range for the certificate.	option	-	global								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Global range.</td> </tr> <tr> <td><i>vdom</i></td> <td>VDOM IP address range.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>factory</i></td> <td>Factory installed certificate.</td> </tr> <tr> <td><i>user</i></td> <td>User generated certificate.</td> </tr> <tr> <td><i>bundle</i></td> <td>Bundle file certificate.</td> </tr> </tbody> </table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified									

Parameter	Description	Type	Size	Default								
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255									
name-encoding	Name encoding method for auto-regeneration.	option	-	printable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>printable</i></td> <td>Printable encoding (default).</td> </tr> <tr> <td><i>utf8</i></td> <td>UTF-8 encoding.</td> </tr> </tbody> </table>	Option	Description	<i>printable</i>	Printable encoding (default).	<i>utf8</i>	UTF-8 encoding.					
Option	Description											
<i>printable</i>	Printable encoding (default).											
<i>utf8</i>	UTF-8 encoding.											
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0								
ike-localid	Local ID the FortiGate uses for authentication as a VPN client.	string	Maximum length: 63									
ike-localid-type	IKE local ID type.	option	-	asn1dn								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>asn1dn</i></td> <td>ASN.1 distinguished name.</td> </tr> <tr> <td><i>fqdn</i></td> <td>Fully qualified domain name.</td> </tr> </tbody> </table>	Option	Description	<i>asn1dn</i>	ASN.1 distinguished name.	<i>fqdn</i>	Fully qualified domain name.					
Option	Description											
<i>asn1dn</i>	ASN.1 distinguished name.											
<i>fqdn</i>	Fully qualified domain name.											
enroll-protocol	Certificate enrollment protocol.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None (default).</td> </tr> <tr> <td><i>scep</i></td> <td>Simple Certificate Enrollment Protocol.</td> </tr> <tr> <td><i>cmpv2</i></td> <td>Certificate Management Protocol Version 2.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None (default).	<i>scep</i>	Simple Certificate Enrollment Protocol.	<i>cmpv2</i>	Certificate Management Protocol Version 2.			
Option	Description											
<i>none</i>	None (default).											
<i>scep</i>	Simple Certificate Enrollment Protocol.											
<i>cmpv2</i>	Certificate Management Protocol Version 2.											
cmp-server	'ADDRESS:PORT' for CMP server.	string	Maximum length: 63									
cmp-path	Path location inside CMP server.	string	Maximum length: 255									
cmp-server-cert	CMP server certificate.	string	Maximum length: 79									
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>keyupate</i></td> <td>Key Update.</td> </tr> <tr> <td><i>renewal</i></td> <td>Renewal.</td> </tr> </tbody> </table>	Option	Description	<i>keyupate</i>	Key Update.	<i>renewal</i>	Renewal.					
Option	Description											
<i>keyupate</i>	Key Update.											
<i>renewal</i>	Renewal.											

## config certificate crl

Certificate Revocation List as a PEM file.

```
config certificate crl
  Description: Certificate Revocation List as a PEM file.
  edit <name>
    set crl {user}
    set range [global|vdom]
    set source [factory|user|...]
    set update-vdom {string}
    set ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set http-url {string}
    set scep-url {string}
    set scep-cert {string}
    set update-interval {integer}
    set source-ip {ipv4-address}
  next
end
```

## config certificate crl

Parameter	Description	Type	Size	Default								
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
range	Either global or VDOM IP address range for the certificate.	option	-	global								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></tbody></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></tbody></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									



Parameter	Description	Type	Size	Default
ldap-password	LDAP server user password.	password	Not Specified	
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255	
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255	
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0

## credential-store

This section includes syntax for the following commands:

- [config credential-store domain-controller on page 82](#)

### config credential-store domain-controller

Define known domain controller servers.

```
config credential-store domain-controller
  Description: Define known domain controller servers.
  edit <server-name>
    set hostname {string}
    set domain-name {string}
    set username {string}
    set password {password}
    set port {integer}
    set ip {ipv4-address-any}
    set ip6 {ipv6-address}
  next
end
```

### config credential-store domain-controller

Parameter	Description	Type	Size	Default
hostname	Hostname of the server to connect to.	string	Maximum length: 255	
domain-name	Fully qualified domain name (FQDN).	string	Maximum length: 255	
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64	
password	Password for specified username.	password	Not Specified	
port	Port number of service. Port number 0 indicates automatic discovery.	integer	Minimum value: 0 Maximum value: 65535	0
ip	IPv4 server address.	ipv4-address-any	Not Specified	0.0.0.0

---

Parameter	Description	Type	Size	Default
ip6	IPv6 server address.	ipv6-address	Not Specified	::

## dlp

This section includes syntax for the following commands:

- [config dlp sensor on page 87](#)
- [config dlp sensitivity on page 87](#)
- [config dlp filepattern on page 84](#)

### config dlp filepattern

Configure file patterns used by DLP blocking.

```
config dlp filepattern
  Description: Configure file patterns used by DLP blocking.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Configure file patterns used by DLP blocking.
      edit <pattern>
        set filter-type [pattern|type]
        set file-type [7z|arj|...]
      next
    end
  next
end
```

### config dlp filepattern

Parameter	Description	Type	Size	Default
name	Name of table containing the file pattern list.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

### config entries

Parameter	Description	Type	Size	Default						
filter-type	Filter by file name pattern or by file type.	option	-	pattern						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>pattern</i></td><td>Filter by file name pattern.</td></tr><tr><td><i>type</i></td><td>Filter by file type.</td></tr></tbody></table>	Option	Description	<i>pattern</i>	Filter by file name pattern.	<i>type</i>	Filter by file type.			
Option	Description									
<i>pattern</i>	Filter by file name pattern.									
<i>type</i>	Filter by file type.									

Parameter	Description	Type	Size	Default																																																										
file-type	Select a file type.	option	-	unknown																																																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>7z</i></td> <td>Match 7-zip files.</td> </tr> <tr> <td><i>arj</i></td> <td>Match arj compressed files.</td> </tr> <tr> <td><i>cab</i></td> <td>Match Windows cab files.</td> </tr> <tr> <td><i>lzh</i></td> <td>Match lzh compressed files.</td> </tr> <tr> <td><i>rar</i></td> <td>Match rar archives.</td> </tr> <tr> <td><i>tar</i></td> <td>Match tar files.</td> </tr> <tr> <td><i>zip</i></td> <td>Match zip files.</td> </tr> <tr> <td><i>bzip</i></td> <td>Match bzip files.</td> </tr> <tr> <td><i>gzip</i></td> <td>Match gzip files.</td> </tr> <tr> <td><i>bzip2</i></td> <td>Match bzip2 files.</td> </tr> <tr> <td><i>xz</i></td> <td>Match xz files.</td> </tr> <tr> <td><i>bat</i></td> <td>Match Windows batch files.</td> </tr> <tr> <td><i>uue</i></td> <td>Match uue files.</td> </tr> <tr> <td><i>mime</i></td> <td>Match mime files.</td> </tr> <tr> <td><i>base64</i></td> <td>Match base64 files.</td> </tr> <tr> <td><i>binhex</i></td> <td>Match binhex files.</td> </tr> <tr> <td><i>elf</i></td> <td>Match elf files.</td> </tr> <tr> <td><i>exe</i></td> <td>Match Windows executable files.</td> </tr> <tr> <td><i>hta</i></td> <td>Match hta files.</td> </tr> <tr> <td><i>html</i></td> <td>Match html files.</td> </tr> <tr> <td><i>jad</i></td> <td>Match jad files.</td> </tr> <tr> <td><i>class</i></td> <td>Match class files.</td> </tr> <tr> <td><i>cod</i></td> <td>Match cod files.</td> </tr> <tr> <td><i>javascript</i></td> <td>Match javascript files.</td> </tr> <tr> <td><i>msoffice</i></td> <td>Match MS-Office files. For example, doc, xls, ppt, and so on.</td> </tr> <tr> <td><i>msofficex</i></td> <td>Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.</td> </tr> <tr> <td><i>fsg</i></td> <td>Match fsg files.</td> </tr> <tr> <td><i>upx</i></td> <td>Match upx files.</td> </tr> </tbody> </table>	Option	Description	<i>7z</i>	Match 7-zip files.	<i>arj</i>	Match arj compressed files.	<i>cab</i>	Match Windows cab files.	<i>lzh</i>	Match lzh compressed files.	<i>rar</i>	Match rar archives.	<i>tar</i>	Match tar files.	<i>zip</i>	Match zip files.	<i>bzip</i>	Match bzip files.	<i>gzip</i>	Match gzip files.	<i>bzip2</i>	Match bzip2 files.	<i>xz</i>	Match xz files.	<i>bat</i>	Match Windows batch files.	<i>uue</i>	Match uue files.	<i>mime</i>	Match mime files.	<i>base64</i>	Match base64 files.	<i>binhex</i>	Match binhex files.	<i>elf</i>	Match elf files.	<i>exe</i>	Match Windows executable files.	<i>hta</i>	Match hta files.	<i>html</i>	Match html files.	<i>jad</i>	Match jad files.	<i>class</i>	Match class files.	<i>cod</i>	Match cod files.	<i>javascript</i>	Match javascript files.	<i>msoffice</i>	Match MS-Office files. For example, doc, xls, ppt, and so on.	<i>msofficex</i>	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.	<i>fsg</i>	Match fsg files.	<i>upx</i>	Match upx files.			
Option	Description																																																													
<i>7z</i>	Match 7-zip files.																																																													
<i>arj</i>	Match arj compressed files.																																																													
<i>cab</i>	Match Windows cab files.																																																													
<i>lzh</i>	Match lzh compressed files.																																																													
<i>rar</i>	Match rar archives.																																																													
<i>tar</i>	Match tar files.																																																													
<i>zip</i>	Match zip files.																																																													
<i>bzip</i>	Match bzip files.																																																													
<i>gzip</i>	Match gzip files.																																																													
<i>bzip2</i>	Match bzip2 files.																																																													
<i>xz</i>	Match xz files.																																																													
<i>bat</i>	Match Windows batch files.																																																													
<i>uue</i>	Match uue files.																																																													
<i>mime</i>	Match mime files.																																																													
<i>base64</i>	Match base64 files.																																																													
<i>binhex</i>	Match binhex files.																																																													
<i>elf</i>	Match elf files.																																																													
<i>exe</i>	Match Windows executable files.																																																													
<i>hta</i>	Match hta files.																																																													
<i>html</i>	Match html files.																																																													
<i>jad</i>	Match jad files.																																																													
<i>class</i>	Match class files.																																																													
<i>cod</i>	Match cod files.																																																													
<i>javascript</i>	Match javascript files.																																																													
<i>msoffice</i>	Match MS-Office files. For example, doc, xls, ppt, and so on.																																																													
<i>msofficex</i>	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.																																																													
<i>fsg</i>	Match fsg files.																																																													
<i>upx</i>	Match upx files.																																																													

Parameter	Description	Type	Size	Default																																																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>petite</i></td> <td>Match petite files.</td> </tr> <tr> <td><i>aspack</i></td> <td>Match aspack files.</td> </tr> <tr> <td><i>sis</i></td> <td>Match sis files.</td> </tr> <tr> <td><i>hlp</i></td> <td>Match Windows help files.</td> </tr> <tr> <td><i>activemime</i></td> <td>Match activemime files.</td> </tr> <tr> <td><i>jpeg</i></td> <td>Match jpeg files.</td> </tr> <tr> <td><i>gif</i></td> <td>Match gif files.</td> </tr> <tr> <td><i>tiff</i></td> <td>Match tiff files.</td> </tr> <tr> <td><i>png</i></td> <td>Match png files.</td> </tr> <tr> <td><i>bmp</i></td> <td>Match bmp files.</td> </tr> <tr> <td><i>unknown</i></td> <td>Match unknown files.</td> </tr> <tr> <td><i>mpeg</i></td> <td>Match mpeg files.</td> </tr> <tr> <td><i>mov</i></td> <td>Match mov files.</td> </tr> <tr> <td><i>mp3</i></td> <td>Match mp3 files.</td> </tr> <tr> <td><i>wma</i></td> <td>Match wma files.</td> </tr> <tr> <td><i>wav</i></td> <td>Match wav files.</td> </tr> <tr> <td><i>pdf</i></td> <td>Match Acrobat PDF files.</td> </tr> <tr> <td><i>avi</i></td> <td>Match avi files.</td> </tr> <tr> <td><i>rm</i></td> <td>Match rm files.</td> </tr> <tr> <td><i>torrent</i></td> <td>Match torrent files.</td> </tr> <tr> <td><i>hibun</i></td> <td>Match special-file-23-support files.</td> </tr> <tr> <td><i>msi</i></td> <td>Match Windows Installer msi files.</td> </tr> <tr> <td><i>mach-o</i></td> <td>Match Mach object files.</td> </tr> <tr> <td><i>dmg</i></td> <td>Match Apple disk image files.</td> </tr> <tr> <td><i>.net</i></td> <td>Match .NET files.</td> </tr> <tr> <td><i>xar</i></td> <td>Match xar archive files.</td> </tr> <tr> <td><i>chm</i></td> <td>Match Windows compiled HTML help files.</td> </tr> <tr> <td><i>iso</i></td> <td>Match ISO archive files.</td> </tr> <tr> <td><i>crx</i></td> <td>Match Chrome extension files.</td> </tr> <tr> <td><i>flac</i></td> <td>Match flac files.</td> </tr> </tbody> </table>	Option	Description	<i>petite</i>	Match petite files.	<i>aspack</i>	Match aspack files.	<i>sis</i>	Match sis files.	<i>hlp</i>	Match Windows help files.	<i>activemime</i>	Match activemime files.	<i>jpeg</i>	Match jpeg files.	<i>gif</i>	Match gif files.	<i>tiff</i>	Match tiff files.	<i>png</i>	Match png files.	<i>bmp</i>	Match bmp files.	<i>unknown</i>	Match unknown files.	<i>mpeg</i>	Match mpeg files.	<i>mov</i>	Match mov files.	<i>mp3</i>	Match mp3 files.	<i>wma</i>	Match wma files.	<i>wav</i>	Match wav files.	<i>pdf</i>	Match Acrobat PDF files.	<i>avi</i>	Match avi files.	<i>rm</i>	Match rm files.	<i>torrent</i>	Match torrent files.	<i>hibun</i>	Match special-file-23-support files.	<i>msi</i>	Match Windows Installer msi files.	<i>mach-o</i>	Match Mach object files.	<i>dmg</i>	Match Apple disk image files.	<i>.net</i>	Match .NET files.	<i>xar</i>	Match xar archive files.	<i>chm</i>	Match Windows compiled HTML help files.	<i>iso</i>	Match ISO archive files.	<i>crx</i>	Match Chrome extension files.	<i>flac</i>	Match flac files.			
Option	Description																																																																	
<i>petite</i>	Match petite files.																																																																	
<i>aspack</i>	Match aspack files.																																																																	
<i>sis</i>	Match sis files.																																																																	
<i>hlp</i>	Match Windows help files.																																																																	
<i>activemime</i>	Match activemime files.																																																																	
<i>jpeg</i>	Match jpeg files.																																																																	
<i>gif</i>	Match gif files.																																																																	
<i>tiff</i>	Match tiff files.																																																																	
<i>png</i>	Match png files.																																																																	
<i>bmp</i>	Match bmp files.																																																																	
<i>unknown</i>	Match unknown files.																																																																	
<i>mpeg</i>	Match mpeg files.																																																																	
<i>mov</i>	Match mov files.																																																																	
<i>mp3</i>	Match mp3 files.																																																																	
<i>wma</i>	Match wma files.																																																																	
<i>wav</i>	Match wav files.																																																																	
<i>pdf</i>	Match Acrobat PDF files.																																																																	
<i>avi</i>	Match avi files.																																																																	
<i>rm</i>	Match rm files.																																																																	
<i>torrent</i>	Match torrent files.																																																																	
<i>hibun</i>	Match special-file-23-support files.																																																																	
<i>msi</i>	Match Windows Installer msi files.																																																																	
<i>mach-o</i>	Match Mach object files.																																																																	
<i>dmg</i>	Match Apple disk image files.																																																																	
<i>.net</i>	Match .NET files.																																																																	
<i>xar</i>	Match xar archive files.																																																																	
<i>chm</i>	Match Windows compiled HTML help files.																																																																	
<i>iso</i>	Match ISO archive files.																																																																	
<i>crx</i>	Match Chrome extension files.																																																																	
<i>flac</i>	Match flac files.																																																																	

---

## config dlp sensitivity

Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source.

```
config dlp sensitivity
  Description: Create self-explanatory DLP sensitivity levels to be used when setting
              sensitivity under config fp-doc-source.
  edit <name>
  next
end
```

## config dlp sensor

Configure DLP sensors.

```
config dlp sensor
  Description: Configure DLP sensors.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    config filter
      Description: Set up DLP filters for this sensor.
      edit <id>
        set name {string}
        set severity [info|low|...]
        set type [file|message]
        set proto {option1}, {option2}, ...
        set filter-by [credit-card|ssn|...]
        set file-size {integer}
        set company-identifier {string}
        set sensitivity <name1>, <name2>, ...
        set file-type {integer}
        set regexp {string}
        set archive [disable|enable]
        set action [allow|log-only|...]
        set expiry {user}
      next
    end
    set dlp-log [enable|disable]
    set extended-log [enable|disable]
    set nac-quar-log [enable|disable]
    set full-archive-proto {option1}, {option2}, ...
    set summary-proto {option1}, {option2}, ...
  next
end
```

## config dlp sensor

Parameter	Description	Type	Size	Default										
comment	Comment.	var-string	Maximum length: 255											
feature-set	Flow/proxy feature set.	option	-	flow										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>flow</i></td> <td>Flow feature set.</td> </tr> <tr> <td><i>proxy</i></td> <td>Proxy feature set.</td> </tr> </tbody> </table>	Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.							
Option	Description													
<i>flow</i>	Flow feature set.													
<i>proxy</i>	Proxy feature set.													
replacemsg-group	Replacement message group used by this DLP sensor.	string	Maximum length: 35											
dlp-log	Enable/disable DLP logging.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DLP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DLP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP logging.	<i>disable</i>	Disable DLP logging.							
Option	Description													
<i>enable</i>	Enable DLP logging.													
<i>disable</i>	Disable DLP logging.													
extended-log	Enable/disable extended logging for data leak prevention.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
nac-quar-log	Enable/disable NAC quarantine logging.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NAC quarantine logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NAC quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NAC quarantine logging.	<i>disable</i>	Disable NAC quarantine logging.							
Option	Description													
<i>enable</i>	Enable NAC quarantine logging.													
<i>disable</i>	Disable NAC quarantine logging.													
full-archive-proto	Protocols to always content archive.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>http-get</i></td> <td>HTTP GET.</td> </tr> </tbody> </table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.			
Option	Description													
<i>smtp</i>	SMTP.													
<i>pop3</i>	POP3.													
<i>imap</i>	IMAP.													
<i>http-get</i>	HTTP GET.													



Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http-post</i></td> <td>HTTP POST.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>ssh</i></td> <td>SFTP and SCP.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> </tbody> </table>	Option	Description	<i>http-post</i>	HTTP POST.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.											
Option	Description																									
<i>http-post</i>	HTTP POST.																									
<i>ftp</i>	FTP.																									
<i>nntp</i>	NNTP.																									
<i>mapi</i>	MAPI.																									
<i>ssh</i>	SFTP and SCP.																									
<i>cifs</i>	CIFS.																									
summary-proto	Protocols to always log summary.	option	-																							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>http-get</i></td> <td>HTTP GET.</td> </tr> <tr> <td><i>http-post</i></td> <td>HTTP POST.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>ssh</i></td> <td>SFTP and SCP.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> </tbody> </table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.	<i>http-post</i>	HTTP POST.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.			
Option	Description																									
<i>smtp</i>	SMTP.																									
<i>pop3</i>	POP3.																									
<i>imap</i>	IMAP.																									
<i>http-get</i>	HTTP GET.																									
<i>http-post</i>	HTTP POST.																									
<i>ftp</i>	FTP.																									
<i>nntp</i>	NNTP.																									
<i>mapi</i>	MAPI.																									
<i>ssh</i>	SFTP and SCP.																									
<i>cifs</i>	CIFS.																									

### config filter

Parameter	Description	Type	Size	Default						
name	Filter name.	string	Maximum length: 35							
severity	Select the severity or threat level that matches this filter.	option	-	medium						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>info</i></td> <td>Informational.</td> </tr> <tr> <td><i>low</i></td> <td>Low.</td> </tr> </tbody> </table>	Option	Description	<i>info</i>	Informational.	<i>low</i>	Low.			
Option	Description									
<i>info</i>	Informational.									
<i>low</i>	Low.									

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>medium</i></td> <td>Medium.</td> </tr> <tr> <td><i>high</i></td> <td>High.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical.</td> </tr> </tbody> </table>	Option	Description	<i>medium</i>	Medium.	<i>high</i>	High.	<i>critical</i>	Critical.																	
Option	Description																									
<i>medium</i>	Medium.																									
<i>high</i>	High.																									
<i>critical</i>	Critical.																									
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>file</i></td> <td>Check the contents of downloaded or attached files.</td> </tr> <tr> <td><i>message</i></td> <td>Check the contents of email messages, web pages, etc.</td> </tr> </tbody> </table>	Option	Description	<i>file</i>	Check the contents of downloaded or attached files.	<i>message</i>	Check the contents of email messages, web pages, etc.																			
Option	Description																									
<i>file</i>	Check the contents of downloaded or attached files.																									
<i>message</i>	Check the contents of email messages, web pages, etc.																									
proto	Check messages or files over one or more of these protocols.	option	-																							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>smtp</i></td> <td>SMTP.</td> </tr> <tr> <td><i>pop3</i></td> <td>POP3.</td> </tr> <tr> <td><i>imap</i></td> <td>IMAP.</td> </tr> <tr> <td><i>http-get</i></td> <td>HTTP GET.</td> </tr> <tr> <td><i>http-post</i></td> <td>HTTP POST.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>nntp</i></td> <td>NNTP.</td> </tr> <tr> <td><i>mapi</i></td> <td>MAPI.</td> </tr> <tr> <td><i>ssh</i></td> <td>SFTP and SCP.</td> </tr> <tr> <td><i>cifs</i></td> <td>CIFS.</td> </tr> </tbody> </table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.	<i>http-post</i>	HTTP POST.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.			
Option	Description																									
<i>smtp</i>	SMTP.																									
<i>pop3</i>	POP3.																									
<i>imap</i>	IMAP.																									
<i>http-get</i>	HTTP GET.																									
<i>http-post</i>	HTTP POST.																									
<i>ftp</i>	FTP.																									
<i>nntp</i>	NNTP.																									
<i>mapi</i>	MAPI.																									
<i>ssh</i>	SFTP and SCP.																									
<i>cifs</i>	CIFS.																									
filter-by	Select the type of content to match.	option	-	credit-card																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>credit-card</i></td> <td>Match credit cards.</td> </tr> <tr> <td><i>ssn</i></td> <td>Match social security numbers.</td> </tr> <tr> <td><i>regexp</i></td> <td>Use a regular expression to match content.</td> </tr> <tr> <td><i>file-type</i></td> <td>Match a DLP file pattern list.</td> </tr> </tbody> </table>	Option	Description	<i>credit-card</i>	Match credit cards.	<i>ssn</i>	Match social security numbers.	<i>regexp</i>	Use a regular expression to match content.	<i>file-type</i>	Match a DLP file pattern list.															
Option	Description																									
<i>credit-card</i>	Match credit cards.																									
<i>ssn</i>	Match social security numbers.																									
<i>regexp</i>	Use a regular expression to match content.																									
<i>file-type</i>	Match a DLP file pattern list.																									

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>file-size</i></td> <td>Match any file over with a size over the threshold.</td> </tr> <tr> <td><i>watermark</i></td> <td>Look for defined file watermarks.</td> </tr> <tr> <td><i>encrypted</i></td> <td>Look for encrypted files.</td> </tr> </tbody> </table>	Option	Description	<i>file-size</i>	Match any file over with a size over the threshold.	<i>watermark</i>	Look for defined file watermarks.	<i>encrypted</i>	Look for encrypted files.					
Option	Description													
<i>file-size</i>	Match any file over with a size over the threshold.													
<i>watermark</i>	Look for defined file watermarks.													
<i>encrypted</i>	Look for encrypted files.													
file-size	Match files this size or larger .	integer	Minimum value: 0 Maximum value: 4294967295	0 **										
company-identifier	Enter a company identifier watermark to match. Only watermarks that your company has placed on the files are matched.	string	Maximum length: 35											
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35											
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0										
regexp	Enter a regular expression to match (max. 255 characters).	string	Maximum length: 255											
archive	Enable/disable DLP archiving.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>No DLP archiving.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable full DLP archiving.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	No DLP archiving.	<i>enable</i>	Enable full DLP archiving.							
Option	Description													
<i>disable</i>	No DLP archiving.													
<i>enable</i>	Enable full DLP archiving.													
action	Action to take with content that this DLP sensor matches.	option	-	allow										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the content to pass through the FortiGate and do not create a log message.</td> </tr> <tr> <td><i>log-only</i></td> <td>Allow the content to pass through the FortiGate, but write a log message.</td> </tr> <tr> <td><i>block</i></td> <td>Block the content and write a log message.</td> </tr> <tr> <td><i>quarantine-ip</i></td> <td>Quarantine all traffic from the IP address and write a log message.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the content to pass through the FortiGate and do not create a log message.	<i>log-only</i>	Allow the content to pass through the FortiGate, but write a log message.	<i>block</i>	Block the content and write a log message.	<i>quarantine-ip</i>	Quarantine all traffic from the IP address and write a log message.			
Option	Description													
<i>allow</i>	Allow the content to pass through the FortiGate and do not create a log message.													
<i>log-only</i>	Allow the content to pass through the FortiGate, but write a log message.													
<i>block</i>	Block the content and write a log message.													
<i>quarantine-ip</i>	Quarantine all traffic from the IP address and write a log message.													
expiry	Quarantine duration in days, hours, minutes format (dddhhmm).	user	Not Specified	5m										

---

\*\* Values may differ between models.

## dnsfilter

This section includes syntax for the following commands:

- [config dnsfilter domain-filter](#) on page 93
- [config dnsfilter profile](#) on page 94

### config dnsfilter domain-filter

Configure DNS domain filters.

```
config dnsfilter domain-filter
  Description: Configure DNS domain filters.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: DNS domain filter entries.
      edit <id>
        set domain {string}
        set type [simple|regex|...]
        set action [block|allow|...]
        set status [enable|disable]
      next
    end
  next
end
```

### config dnsfilter domain-filter

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

### config entries

Parameter	Description	Type	Size	Default
domain	Domain entries to be filtered.	string	Maximum length: 511	
type	DNS domain filter type.	option	-	simple

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>simple</i></td> <td>Simple domain string.</td> </tr> <tr> <td><i>regex</i></td> <td>Regular expression domain string.</td> </tr> <tr> <td><i>wildcard</i></td> <td>Wildcard domain string.</td> </tr> </tbody> </table>	Option	Description	<i>simple</i>	Simple domain string.	<i>regex</i>	Regular expression domain string.	<i>wildcard</i>	Wildcard domain string.			
Option	Description											
<i>simple</i>	Simple domain string.											
<i>regex</i>	Regular expression domain string.											
<i>wildcard</i>	Wildcard domain string.											
action	Action to take for domain filter matches.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block DNS requests matching the domain filter.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow DNS requests matching the domain filter without logging.</td> </tr> <tr> <td><i>monitor</i></td> <td>Allow DNS requests matching the domain filter with logging.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block DNS requests matching the domain filter.	<i>allow</i>	Allow DNS requests matching the domain filter without logging.	<i>monitor</i>	Allow DNS requests matching the domain filter with logging.			
Option	Description											
<i>block</i>	Block DNS requests matching the domain filter.											
<i>allow</i>	Allow DNS requests matching the domain filter without logging.											
<i>monitor</i>	Allow DNS requests matching the domain filter with logging.											
status	Enable/disable this domain filter.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this domain filter.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this domain filter.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this domain filter.	<i>disable</i>	Disable this domain filter.					
Option	Description											
<i>enable</i>	Enable this domain filter.											
<i>disable</i>	Disable this domain filter.											

## config dnsfilter profile

Configure DNS domain filter profiles.

```

config dnsfilter profile
  Description: Configure DNS domain filter profiles.
  edit <name>
    set comment {var-string}
    config domain-filter
      Description: Domain filter settings.
      set domain-filter-table {integer}
    end
    config ftgd-dns
      Description: FortiGuard DNS Filter settings.
      set options {option1}, {option2}, ...
      config filters
        Description: FortiGuard DNS domain filters.
        edit <id>
          set category {integer}
          set action [block|monitor]
          set log [enable|disable]
        next
      end
    end
    set log-all-domain [enable|disable]
    set sdns-ftgd-err-log [enable|disable]
    set sdns-domain-log [enable|disable]
    set block-action [block|redirect]
  
```

```

set redirect-portal {ipv4-address}
set redirect-portal6 {ipv6-address}
set block-botnet [disable|enable]
set safe-search [disable|enable]
set youtube-restrict [strict|moderate]
set external-ip-blocklist <name1>, <name2>, ...
config dns-translation
  Description: DNS translation settings.
  edit <id>
    set addr-type [ipv4|ipv6]
    set src {ipv4-address}
    set dst {ipv4-address}
    set netmask {ipv4-netmask}
    set status [enable|disable]
    set src6 {ipv6-address}
    set dst6 {ipv6-address}
    set prefix {integer}
  next
end
next
end

```

## config dnsfilter profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging of all domains visited.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging of all domains visited.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging of all domains visited.	<i>disable</i>	Disable logging of all domains visited.			
Option	Description									
<i>enable</i>	Enable logging of all domains visited.									
<i>disable</i>	Disable logging of all domains visited.									
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard SDNS rating error logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard SDNS rating error logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard SDNS rating error logging.	<i>disable</i>	Disable FortiGuard SDNS rating error logging.			
Option	Description									
<i>enable</i>	Enable FortiGuard SDNS rating error logging.									
<i>disable</i>	Disable FortiGuard SDNS rating error logging.									
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable domain filtering and botnet domain logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable domain filtering and botnet domain logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable domain filtering and botnet domain logging.	<i>disable</i>	Disable domain filtering and botnet domain logging.			
Option	Description									
<i>enable</i>	Enable domain filtering and botnet domain logging.									
<i>disable</i>	Disable domain filtering and botnet domain logging.									

Parameter	Description	Type	Size	Default						
block-action	Action to take for blocked domains.	option	-	redirect						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Return NXDOMAIN for blocked domains.</td> </tr> <tr> <td><i>redirect</i></td> <td>Redirect blocked domains to SDNS portal.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Return NXDOMAIN for blocked domains.	<i>redirect</i>	Redirect blocked domains to SDNS portal.			
Option	Description									
<i>block</i>	Return NXDOMAIN for blocked domains.									
<i>redirect</i>	Redirect blocked domains to SDNS portal.									
redirect-portal	IPv4 address of the SDNS redirect portal.	ipv4-address	Not Specified	0.0.0.0						
redirect-portal6	IPv6 address of the SDNS redirect portal.	ipv6-address	Not Specified	::						
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable blocking botnet C&amp;C DNS lookups.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable blocking botnet C&amp;C DNS lookups.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable blocking botnet C&C DNS lookups.	<i>enable</i>	Enable blocking botnet C&C DNS lookups.			
Option	Description									
<i>disable</i>	Disable blocking botnet C&C DNS lookups.									
<i>enable</i>	Enable blocking botnet C&C DNS lookups.									
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.			
Option	Description									
<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.									
<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.									
youtube-restrict	Set safe search for YouTube restriction level.	option	-	strict						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>strict</i></td> <td>Enable strict safe search for YouTube.</td> </tr> <tr> <td><i>moderate</i></td> <td>Enable moderate safe search for YouTube.</td> </tr> </tbody> </table>	Option	Description	<i>strict</i>	Enable strict safe search for YouTube.	<i>moderate</i>	Enable moderate safe search for YouTube.			
Option	Description									
<i>strict</i>	Enable strict safe search for YouTube.									
<i>moderate</i>	Enable moderate safe search for YouTube.									
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79							

### config domain-filter

Parameter	Description	Type	Size	Default
domain-filter-table	DNS domain filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0



## config ftgd-dns

Parameter	Description	Type	Size	Default						
options	FortiGuard DNS filter options.	option	-							
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>error-allow</i></td><td>Allow all domains when FortiGuard DNS servers fail.</td></tr><tr><td><i>ftgd-disable</i></td><td>Disable FortiGuard DNS domain rating.</td></tr></tbody></table>	Option	Description	<i>error-allow</i>	Allow all domains when FortiGuard DNS servers fail.	<i>ftgd-disable</i>	Disable FortiGuard DNS domain rating.			
Option	Description									
<i>error-allow</i>	Allow all domains when FortiGuard DNS servers fail.									
<i>ftgd-disable</i>	Disable FortiGuard DNS domain rating.									

## config filters

Parameter	Description	Type	Size	Default						
category	Category number.	integer	Minimum value: 0 Maximum value: 255	0						
action	Action to take for DNS requests matching the category.	option	-	monitor						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>block</i></td><td>Block DNS requests matching the category.</td></tr><tr><td><i>monitor</i></td><td>Allow DNS requests matching the category and log the result.</td></tr></tbody></table>	Option	Description	<i>block</i>	Block DNS requests matching the category.	<i>monitor</i>	Allow DNS requests matching the category and log the result.			
Option	Description									
<i>block</i>	Block DNS requests matching the category.									
<i>monitor</i>	Allow DNS requests matching the category and log the result.									
log	Enable/disable DNS filter logging for this DNS profile.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable DNS filter logging.</td></tr><tr><td><i>disable</i></td><td>Disable DNS filter logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable DNS filter logging.	<i>disable</i>	Disable DNS filter logging.			
Option	Description									
<i>enable</i>	Enable DNS filter logging.									
<i>disable</i>	Disable DNS filter logging.									

## config dns-translation

Parameter	Description	Type	Size	Default						
addr-type	DNS translation type (IPv4 or IPv6).	option	-	ipv4						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ipv4</i></td><td>IPv4 address type.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 address type.</td></tr></tbody></table>	Option	Description	<i>ipv4</i>	IPv4 address type.	<i>ipv6</i>	IPv6 address type.			
Option	Description									
<i>ipv4</i>	IPv4 address type.									
<i>ipv6</i>	IPv6 address type.									
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0						
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255						
status	Enable/disable this DNS translation entry.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this DNS translation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this DNS translation.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable this DNS translation.	<i>disable</i>	Disable this DNS translation.		
Option	Description									
<i>enable</i>	Enable this DNS translation.									
<i>disable</i>	Disable this DNS translation.									
src6	IPv6 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst6.	ipv6-address	Not Specified	::						
dst6	IPv6 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src6.	ipv6-address	Not Specified	::						
prefix	If src6 and dst6 are subnets rather than single IP addresses, enter the prefix for both src6 and dst6.	integer	Minimum value: 1 Maximum value: 128	128						

## emailfilter

This section includes syntax for the following commands:

- [config emailfilter mheader on page 103](#)
- [config emailfilter fortishield on page 113](#)
- [config emailfilter options on page 114](#)
- [config emailfilter profile on page 106](#)
- [config emailfilter iptrust on page 105](#)
- [config emailfilter bwl on page 101](#)
- [config emailfilter dnsbl on page 104](#)
- [config emailfilter bword on page 99](#)

### config emailfilter bword

Configure AntiSpam banned word list.

```
config emailfilter bword
  Description: Configure AntiSpam banned word list.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter banned word.
      edit <id>
        set status [enable|disable]
        set pattern {string}
        set pattern-type [wildcard|regexp]
        set action [spam|clear]
        set where [subject|body|...]
        set language [western|simch|...]
        set score {integer}
      next
    end
  next
end
```

### config emailfilter bword

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default														
status	Enable/disable status.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.											
Option	Description																	
<i>enable</i>	Enable status.																	
<i>disable</i>	Disable status.																	
pattern	Pattern for the banned word.	string	Maximum length: 127															
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wildcard</i></td> <td>Wildcard pattern.</td> </tr> <tr> <td><i>regexp</i></td> <td>Perl regular expression.</td> </tr> </tbody> </table>	Option	Description	<i>wildcard</i>	Wildcard pattern.	<i>regexp</i>	Perl regular expression.											
Option	Description																	
<i>wildcard</i>	Wildcard pattern.																	
<i>regexp</i>	Perl regular expression.																	
action	Mark spam or good.	option	-	spam														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>spam</i></td> <td>Mark as spam email.</td> </tr> <tr> <td><i>clear</i></td> <td>Mark as good email.</td> </tr> </tbody> </table>	Option	Description	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.											
Option	Description																	
<i>spam</i>	Mark as spam email.																	
<i>clear</i>	Mark as good email.																	
where	Component of the email to be scanned.	option	-	all														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subject</i></td> <td>Banned word in email subject.</td> </tr> <tr> <td><i>body</i></td> <td>Banned word in email body.</td> </tr> <tr> <td><i>all</i></td> <td>Banned word in both subject and body.</td> </tr> </tbody> </table>	Option	Description	<i>subject</i>	Banned word in email subject.	<i>body</i>	Banned word in email body.	<i>all</i>	Banned word in both subject and body.									
Option	Description																	
<i>subject</i>	Banned word in email subject.																	
<i>body</i>	Banned word in email body.																	
<i>all</i>	Banned word in both subject and body.																	
language	Language for the banned word.	option	-	western														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>western</i></td> <td>Western.</td> </tr> <tr> <td><i>simch</i></td> <td>Simplified Chinese.</td> </tr> <tr> <td><i>trach</i></td> <td>Traditional Chinese.</td> </tr> <tr> <td><i>japanese</i></td> <td>Japanese.</td> </tr> <tr> <td><i>korean</i></td> <td>Korean.</td> </tr> <tr> <td><i>french</i></td> <td>French.</td> </tr> </tbody> </table>	Option	Description	<i>western</i>	Western.	<i>simch</i>	Simplified Chinese.	<i>trach</i>	Traditional Chinese.	<i>japanese</i>	Japanese.	<i>korean</i>	Korean.	<i>french</i>	French.			
Option	Description																	
<i>western</i>	Western.																	
<i>simch</i>	Simplified Chinese.																	
<i>trach</i>	Traditional Chinese.																	
<i>japanese</i>	Japanese.																	
<i>korean</i>	Korean.																	
<i>french</i>	French.																	

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>thai</i></td> <td>Thai.</td> </tr> <tr> <td><i>spanish</i></td> <td>Spanish.</td> </tr> </tbody> </table>	Option	Description	<i>thai</i>	Thai.	<i>spanish</i>	Spanish.			
Option	Description									
<i>thai</i>	Thai.									
<i>spanish</i>	Spanish.									
score	Score value.	integer	Minimum value: 1 Maximum value: 99999	10						

## config emailfilter bwl

Configure anti-spam black/white list.

```

config emailfilter bwl
  Description: Configure anti-spam black/white list.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Anti-spam black/white list entries.
      edit <id>
        set status [enable|disable]
        set type [ip|email]
        set action [reject|spam|...]
        set addr-type [ipv4|ipv6]
        set ip4-subnet {ipv4-classnet}
        set ip6-subnet {ipv6-network}
        set pattern-type [wildcard|regexp]
        set email-pattern {string}
      next
    end
  next
end

```

## config emailfilter bwl

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default								
status	Enable/disable status.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.					
Option	Description											
<i>enable</i>	Enable status.											
<i>disable</i>	Disable status.											
type	Entry type.	option	-	ip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ip</i></td> <td>By IP address.</td> </tr> <tr> <td><i>email</i></td> <td>By email address.</td> </tr> </tbody> </table>	Option	Description	<i>ip</i>	By IP address.	<i>email</i>	By email address.					
Option	Description											
<i>ip</i>	By IP address.											
<i>email</i>	By email address.											
action	Reject, mark as spam or good email.	option	-	spam								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>reject</i></td> <td>Reject the connection.</td> </tr> <tr> <td><i>spam</i></td> <td>Mark as spam email.</td> </tr> <tr> <td><i>clear</i></td> <td>Mark as good email.</td> </tr> </tbody> </table>	Option	Description	<i>reject</i>	Reject the connection.	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.			
Option	Description											
<i>reject</i>	Reject the connection.											
<i>spam</i>	Mark as spam email.											
<i>clear</i>	Mark as good email.											
addr-type	IP address type.	option	-	ipv4								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>IPv4 Address type.</td> </tr> <tr> <td><i>ipv6</i></td> <td>IPv6 Address type.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	IPv4 Address type.	<i>ipv6</i>	IPv6 Address type.					
Option	Description											
<i>ipv4</i>	IPv4 Address type.											
<i>ipv6</i>	IPv6 Address type.											
ip4-subnet	IPv4 network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0								
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128								
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wildcard</i></td> <td>Wildcard pattern.</td> </tr> <tr> <td><i>regexp</i></td> <td>Perl regular expression.</td> </tr> </tbody> </table>	Option	Description	<i>wildcard</i>	Wildcard pattern.	<i>regexp</i>	Perl regular expression.					
Option	Description											
<i>wildcard</i>	Wildcard pattern.											
<i>regexp</i>	Perl regular expression.											
email-pattern	Email address pattern.	string	Maximum length: 127									

## config emailfilter mheader

Configure AntiSpam MIME header.

```
config emailfilter mheader
  Description: Configure AntiSpam MIME header.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter mime header content.
      edit <id>
        set status [enable|disable]
        set fieldname {string}
        set fieldbody {string}
        set pattern-type [wildcard|regexp]
        set action [spam|clear]
      next
    end
  next
end
```

## config emailfilter mheader

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default						
status	Enable/disable status.	option	-	enable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.			
Option	Description									
<i>enable</i>	Enable status.									
<i>disable</i>	Disable status.									
fieldname	Pattern for header field name.	string	Maximum length: 63							
fieldbody	Pattern for the header field body.	string	Maximum length: 127							
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wildcard</i></td> <td>Wildcard pattern.</td> </tr> <tr> <td><i>regexp</i></td> <td>Perl regular expression.</td> </tr> </tbody> </table>	Option	Description	<i>wildcard</i>	Wildcard pattern.	<i>regexp</i>	Perl regular expression.			
Option	Description									
<i>wildcard</i>	Wildcard pattern.									
<i>regexp</i>	Perl regular expression.									
action	Mark spam or good.	option	-	spam						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>spam</i></td> <td>Mark as spam email.</td> </tr> <tr> <td><i>clear</i></td> <td>Mark as good email.</td> </tr> </tbody> </table>	Option	Description	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.			
Option	Description									
<i>spam</i>	Mark as spam email.									
<i>clear</i>	Mark as good email.									

## config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

```
config emailfilter dnsbl
  Description: Configure AntiSpam DNSBL/ORBL.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter DNSBL and ORBL server.
      edit <id>
        set status [enable|disable]
        set server {string}
        set action [reject|spam]
      next
    end
  next
end
```

## config emailfilter dnsbl

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.			
Option	Description									
<i>enable</i>	Enable status.									
<i>disable</i>	Disable status.									
server	DNSBL or ORBL server name.	string	Maximum length: 127							
action	Reject connection or mark as spam email.	option	-	spam						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>reject</i></td> <td>Reject the connection.</td> </tr> <tr> <td><i>spam</i></td> <td>Mark as spam email.</td> </tr> </tbody> </table>	Option	Description	<i>reject</i>	Reject the connection.	<i>spam</i>	Mark as spam email.			
Option	Description									
<i>reject</i>	Reject the connection.									
<i>spam</i>	Mark as spam email.									

## config emailfilter iptrust

Configure AntiSpam IP trust.

```
config emailfilter iptrust
  Description: Configure AntiSpam IP trust.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter trusted IP addresses.
      edit <id>
        set status [enable|disable]
        set addr-type [ipv4|ipv6]
        set ip4-subnet {ipv4-classnet}
        set ip6-subnet {ipv6-network}
      next
    end
  next
end
```

## config emailfilter iptrust

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default						
status	Enable/disable status.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.			
Option	Description									
<i>enable</i>	Enable status.									
<i>disable</i>	Disable status.									
addr-type	Type of address.	option	-	ipv4						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ipv4</i></td><td>IPv4 Address type.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 Address type.</td></tr></tbody></table>	Option	Description	<i>ipv4</i>	IPv4 Address type.	<i>ipv6</i>	IPv6 Address type.			
Option	Description									
<i>ipv4</i>	IPv4 Address type.									
<i>ipv6</i>	IPv6 Address type.									
ip4-subnet	IPv4 network address or network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128						

## config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
  Description: Configure Email Filter profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    set spam-log [disable|enable]
    set spam-log-fortiguard-response [disable|enable]
    set spam-filtering [enable|disable]
    set external [enable|disable]
    set options {option1}, {option2}, ...
  config imap
    Description: IMAP.
    set log-all [disable|enable]
    set action [pass|tag]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
  end
  config pop3
    Description: POP3.
    set log-all [disable|enable]
    set action [pass|tag]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
  end
  config smtp
```

```

    Description: SMTP.
    set log-all [disable|enable]
    set action [pass|tag|...]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
    set hdrrip [disable|enable]
    set local-override [disable|enable]
end
config mapi
    Description: MAPI.
    set log-all [disable|enable]
    set action [pass|discard]
end
config msn-hotmail
    Description: MSN Hotmail.
    set log-all [disable|enable]
end
config yahoo-mail
    Description: Yahoo! Mail.
    set log-all [disable|enable]
end
config gmail
    Description: Gmail.
    set log-all [disable|enable]
end
config other-webmails
    Description: Other supported webmails.
    set log-all [disable|enable]
end
set spam-bword-threshold {integer}
set spam-bword-table {integer}
set spam-bwl-table {integer}
set spam-mheader-table {integer}
set spam-rbl-table {integer}
set spam-iptrust-table {integer}
next
end

```

## config emailfilter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
feature-set	Flow/proxy feature set.	option	-	flow
	<b>Option</b>	<b>Description</b>		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		

Parameter	Description	Type	Size	Default
replacemsg-group	Replacement message group.	string	Maximum length: 35	
spam-log	Enable/disable spam logging for email filtering.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable spam logging for email filtering.		
	<i>enable</i>	Enable spam logging for email filtering.		
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging FortiGuard spam response.		
	<i>enable</i>	Enable logging FortiGuard spam response.		
spam-filtering	Enable/disable spam filtering.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
external	Enable/disable external Email inspection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	Options.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>bannedword</i>	Content block.		
	<i>spambwl</i>	Black/white list.		
	<i>spamfsip</i>	Email IP address FortiGuard AntiSpam black list check.		
	<i>spamfssubmit</i>	Add FortiGuard AntiSpam spam submission text.		
	<i>spamfsschsum</i>	Email checksum FortiGuard AntiSpam check.		
	<i>spamfsurl</i>	Email content URL FortiGuard AntiSpam check.		
	<i>spamhelodns</i>	Email helo/ehlo domain DNS check.		

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>spamraddrdns</i></td> <td>Email return address DNS check.</td> </tr> <tr> <td><i>spamrbl</i></td> <td>Email DNSBL &amp; ORBL check.</td> </tr> <tr> <td><i>spamhdrcheck</i></td> <td>Email mime header check.</td> </tr> <tr> <td><i>spamfspath</i></td> <td>Email content phishing URL FortiGuard AntiSpam check.</td> </tr> </tbody> </table>	Option	Description	<i>spamraddrdns</i>	Email return address DNS check.	<i>spamrbl</i>	Email DNSBL & ORBL check.	<i>spamhdrcheck</i>	Email mime header check.	<i>spamfspath</i>	Email content phishing URL FortiGuard AntiSpam check.			
Option	Description													
<i>spamraddrdns</i>	Email return address DNS check.													
<i>spamrbl</i>	Email DNSBL & ORBL check.													
<i>spamhdrcheck</i>	Email mime header check.													
<i>spamfspath</i>	Email content phishing URL FortiGuard AntiSpam check.													
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10										
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
spam-bwl-table	Anti-spam black/white list table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
spam-mheader-table	Anti-spam MIME header table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
spam-rbl-table	Anti-spam DNSBL table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										

## config imap

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of all email traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of all email traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.					
Option	Description											
<i>disable</i>	Disable logging of all email traffic.											
<i>enable</i>	Enable logging of all email traffic.											
action	Action for spam email.	option	-	tag								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow spam email to pass through.</td> </tr> <tr> <td><i>tag</i></td> <td>Tag spam email with configured text in subject or header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow spam email to pass through.	<i>tag</i>	Tag spam email with configured text in subject or header.					
Option	Description											
<i>pass</i>	Allow spam email to pass through.											
<i>tag</i>	Tag spam email with configured text in subject or header.											
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subject</i></td> <td>Prepend text to spam email subject.</td> </tr> <tr> <td><i>header</i></td> <td>Append a user defined mime header to spam email.</td> </tr> <tr> <td><i>spaminfo</i></td> <td>Append spam info to spam email header.</td> </tr> </tbody> </table>	Option	Description	<i>subject</i>	Prepend text to spam email subject.	<i>header</i>	Append a user defined mime header to spam email.	<i>spaminfo</i>	Append spam info to spam email header.			
Option	Description											
<i>subject</i>	Prepend text to spam email subject.											
<i>header</i>	Append a user defined mime header to spam email.											
<i>spaminfo</i>	Append spam info to spam email header.											
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam								

### config pop3

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of all email traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of all email traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									
action	Action for spam email.	option	-	tag						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow spam email to pass through.</td> </tr> <tr> <td><i>tag</i></td> <td>Tag spam email with configured text in subject or header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow spam email to pass through.	<i>tag</i>	Tag spam email with configured text in subject or header.			
Option	Description									
<i>pass</i>	Allow spam email to pass through.									
<i>tag</i>	Tag spam email with configured text in subject or header.									
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subject</i></td> <td>Prepend text to spam email subject.</td> </tr> <tr> <td><i>header</i></td> <td>Append a user defined mime header to spam email.</td> </tr> <tr> <td><i>spaminfo</i></td> <td>Append spam info to spam email header.</td> </tr> </tbody> </table>	Option	Description	<i>subject</i>	Prepend text to spam email subject.	<i>header</i>	Append a user defined mime header to spam email.	<i>spaminfo</i>	Append spam info to spam email header.			
Option	Description											
<i>subject</i>	Prepend text to spam email subject.											
<i>header</i>	Append a user defined mime header to spam email.											
<i>spaminfo</i>	Append spam info to spam email header.											
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam								

## config smtp

Parameter	Description	Type	Size	Default								
log-all	Enable/disable logging of all email traffic.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of all email traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of all email traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.					
Option	Description											
<i>disable</i>	Disable logging of all email traffic.											
<i>enable</i>	Enable logging of all email traffic.											
action	Action for spam email.	option	-	discard								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow spam email to pass through.</td> </tr> <tr> <td><i>tag</i></td> <td>Tag spam email with configured text in subject or header.</td> </tr> <tr> <td><i>discard</i></td> <td>Discard (block) spam email.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow spam email to pass through.	<i>tag</i>	Tag spam email with configured text in subject or header.	<i>discard</i>	Discard (block) spam email.			
Option	Description											
<i>pass</i>	Allow spam email to pass through.											
<i>tag</i>	Tag spam email with configured text in subject or header.											
<i>discard</i>	Discard (block) spam email.											
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subject</i></td> <td>Prepend text to spam email subject.</td> </tr> <tr> <td><i>header</i></td> <td>Append a user defined mime header to spam email.</td> </tr> <tr> <td><i>spaminfo</i></td> <td>Append spam info to spam email header.</td> </tr> </tbody> </table>	Option	Description	<i>subject</i>	Prepend text to spam email subject.	<i>header</i>	Append a user defined mime header to spam email.	<i>spaminfo</i>	Append spam info to spam email header.			
Option	Description											
<i>subject</i>	Prepend text to spam email subject.											
<i>header</i>	Append a user defined mime header to spam email.											
<i>spaminfo</i>	Append spam info to spam email header.											
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam								
hdrp	Enable/disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.	<i>enable</i>	Enable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.			
Option	Description									
<i>disable</i>	Disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.									
<i>enable</i>	Enable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.									
local-override	Enable/disable local filter to override SMTP remote check result.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable local filter to override SMTP remote check result.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable local filter to override SMTP remote check result.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable local filter to override SMTP remote check result.	<i>enable</i>	Enable local filter to override SMTP remote check result.			
Option	Description									
<i>disable</i>	Disable local filter to override SMTP remote check result.									
<i>enable</i>	Enable local filter to override SMTP remote check result.									

### config mapi

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of all email traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of all email traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									
action	Action for spam email.	option	-	pass						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow spam email to pass through.</td> </tr> <tr> <td><i>discard</i></td> <td>Discard (block) spam email.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow spam email to pass through.	<i>discard</i>	Discard (block) spam email.			
Option	Description									
<i>pass</i>	Allow spam email to pass through.									
<i>discard</i>	Discard (block) spam email.									

### config msn-hotmail

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of all email traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of all email traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									



## config yahoo-mail

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable logging of all email traffic.</td></tr><tr><td><i>enable</i></td><td>Enable logging of all email traffic.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									

## config gmail

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable logging of all email traffic.</td></tr><tr><td><i>enable</i></td><td>Enable logging of all email traffic.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									

## config other-webmails

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable logging of all email traffic.</td></tr><tr><td><i>enable</i></td><td>Enable logging of all email traffic.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									

## config emailfilter fortishield

Configure FortiGuard - AntiSpam.

```
config emailfilter fortishield
  Description: Configure FortiGuard - AntiSpam.
  set spam-submit-srv {string}
  set spam-submit-force [enable|disable]
  set spam-submit-txt2htm [enable|disable]
end
```

## config emailfilter fortishield

Parameter	Description	Type	Size	Default						
spam-submit-srv	Hostname of the spam submission server.	string	Maximum length: 63	www.nospammer.net						
spam-submit-force	Enable/disable force insertion of a new mime entity for the submission text.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
spam-submit-txt2htm	Enable/disable conversion of text email to HTML email.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

## config emailfilter options

Configure AntiSpam options.

```
config emailfilter options
  Description: Configure AntiSpam options.
  set dns-timeout {integer}
end
```

## config emailfilter options

Parameter	Description	Type	Size	Default
dns-timeout	DNS query time out .	integer	Minimum value: 1 Maximum value: 30	7

## endpoint-control

This section includes syntax for the following commands:

- [config endpoint-control fctems on page 115](#)

### config endpoint-control fctems

Configure FortiClient Enterprise Management Server (EMS) entries.

```
config endpoint-control fctems
  Description: Configure FortiClient Enterprise Management Server (EMS) entries.
  edit <name>
    set fortinetone-cloud-authentication [enable|disable]
    set server {string}
    set https-port {integer}
    set source-ip {ipv4-address-any}
    set pull-sysinfo [enable|disable]
    set pull-vulnerabilities [enable|disable]
    set pull-avatars [enable|disable]
    set pull-tags [enable|disable]
    set cloud-server-type [production|alpha|...]
    set call-timeout {integer}
    set status-check-interval {integer}
    set certificate {string}
  next
end
```

### config endpoint-control fctems

Parameter	Description	Type	Size	Default						
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr><tr><td><i>disable</i></td><td>Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.	<i>disable</i>	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.			
Option	Description									
<i>enable</i>	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.									
<i>disable</i>	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.									
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default								
https-port	FortiClient EMS HTTPS access port number. .	integer	Minimum value: 1 Maximum value: 65535	443								
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0								
pull-sysinfo	Enable/disable pulling SysInfo from EMS.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable pulling FortiClient user SysInfo from EMS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable pulling FortiClient user SysInfo from EMS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.	<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.					
Option	Description											
<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.											
<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.											
pull-vulnerabilities	Enable/disable pulling vulnerabilities from EMS.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable pulling client vulnerabilities from EMS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable pulling client vulnerabilities from from EMS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable pulling client vulnerabilities from EMS.	<i>disable</i>	Disable pulling client vulnerabilities from from EMS.					
Option	Description											
<i>enable</i>	Enable pulling client vulnerabilities from EMS.											
<i>disable</i>	Disable pulling client vulnerabilities from from EMS.											
pull-avatars	Enable/disable pulling avatars from EMS.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable pulling FortiClient user avatars from EMS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable pulling FortiClient user avatars from EMS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user avatars from EMS.	<i>disable</i>	Disable pulling FortiClient user avatars from EMS.					
Option	Description											
<i>enable</i>	Enable pulling FortiClient user avatars from EMS.											
<i>disable</i>	Disable pulling FortiClient user avatars from EMS.											
pull-tags	Enable/disable pulling FortiClient user tags from EMS.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable pulling FortiClient user tags from EMS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable pulling FortiClient user tags from EMS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user tags from EMS.	<i>disable</i>	Disable pulling FortiClient user tags from EMS.					
Option	Description											
<i>enable</i>	Enable pulling FortiClient user tags from EMS.											
<i>disable</i>	Disable pulling FortiClient user tags from EMS.											
cloud-server-type	Cloud server type.	option	-	production								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>production</i></td> <td>Production FortiClient EMS Cloud Controller.</td> </tr> <tr> <td><i>alpha</i></td> <td>Alpha FortiClient EMS Cloud Controller.</td> </tr> <tr> <td><i>beta</i></td> <td>Beta FortiClient EMS Cloud Controller.</td> </tr> </tbody> </table>	Option	Description	<i>production</i>	Production FortiClient EMS Cloud Controller.	<i>alpha</i>	Alpha FortiClient EMS Cloud Controller.	<i>beta</i>	Beta FortiClient EMS Cloud Controller.			
Option	Description											
<i>production</i>	Production FortiClient EMS Cloud Controller.											
<i>alpha</i>	Alpha FortiClient EMS Cloud Controller.											
<i>beta</i>	Beta FortiClient EMS Cloud Controller.											

---

Parameter	Description	Type	Size	Default
call-timeout	FortiClient EMS call timeout in seconds .	integer	Minimum value: 1 Maximum value: 180	30
status-check-interval	FortiClient EMS call timeout in seconds .	integer	Minimum value: 1 Maximum value: 180	5
certificate	FortiClient EMS certificate.	string	Maximum length: 35	

## extender

This section includes syntax for the following commands:

- [config extender modem-status](#) on page 119
- [config extender lte-carrier-list](#) on page 119
- [config extender extender-info](#) on page 118
- [config extender sys-info](#) on page 118
- [config extender lte-carrier-by-mcc-mnc](#) on page 119

### config extender sys-info

Display detailed extender system information.

```
config extender sys-info
  Description: Display detailed extender system information.
  set <sn> {string}
end
```

### config extender sys-info

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

### config extender extender-info

Display extender struct information.

```
config extender extender-info
  Description: Display extender struct information.
  set <sn> {string}
end
```

### config extender extender-info

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

---

## config extender modem-status

Display detailed extender modem status.

```
config extender modem-status
  Description: Display detailed extender modem status.
  set <sn> {string}
end
```

## config extender modem-status

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

## config extender lte-carrier-list

Display extender modem carrier list.

```
config extender lte-carrier-list
  Description: Display extender modem carrier list.
  set <sn> {string}
end
```

## config extender lte-carrier-list

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

## config extender lte-carrier-by-mcc-mnc

Display extender modem carrier based on MCC and MNC.

```
config extender lte-carrier-by-mcc-mnc
  Description: Display extender modem carrier based on MCC and MNC.
  set <sn> {string}
end
```

## config extender lte-carrier-by-mcc-mnc

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

## extender-controller

This section includes syntax for the following commands:

- [config extender-controller extender on page 122](#)
- [config extender-controller dataplan on page 120](#)

### config extender-controller dataplan

FortiExtender dataplan configuration.

```
config extender-controller dataplan
  Description: FortiExtender dataplan configuration.
  edit <name>
    set modem-id [modem1|modem2|...]
    set type [carrier|slot|...]
    set slot [sim1|sim2]
    set iccid {string}
    set carrier {string}
    set apn {string}
    set auth-type [none|pap|...]
    set username {string}
    set password {password}
    set pdn [ipv4-only|ipv6-only|...]
    set signal-threshold {integer}
    set signal-period {integer}
    set capacity {integer}
    set monthly-fee {integer}
    set billing-date {integer}
    set overage [disable|enable]
    set preferred-subnet {integer}
    set private-network [disable|enable]
  next
end
```

### config extender-controller dataplan

Parameter	Description	Type	Size	Default								
modem-id	Dataplan's modem specifics, if any.	option	-	all								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>modem1</i></td><td>Modem one.</td></tr><tr><td><i>modem2</i></td><td>Modem two.</td></tr><tr><td><i>all</i></td><td>All modems.</td></tr></tbody></table>	Option	Description	<i>modem1</i>	Modem one.	<i>modem2</i>	Modem two.	<i>all</i>	All modems.			
Option	Description											
<i>modem1</i>	Modem one.											
<i>modem2</i>	Modem two.											
<i>all</i>	All modems.											
type	Type preferences configuration.	option	-	generic								



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>carrier</i></td> <td>Assign by SIM carrier.</td> </tr> <tr> <td><i>slot</i></td> <td>Assign to SIM slot 1 or 2.</td> </tr> <tr> <td><i>iccid</i></td> <td>Assign to a specific SIM by ICCID.</td> </tr> <tr> <td><i>generic</i></td> <td>Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.</td> </tr> </tbody> </table>	Option	Description	<i>carrier</i>	Assign by SIM carrier.	<i>slot</i>	Assign to SIM slot 1 or 2.	<i>iccid</i>	Assign to a specific SIM by ICCID.	<i>generic</i>	Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.			
Option	Description													
<i>carrier</i>	Assign by SIM carrier.													
<i>slot</i>	Assign to SIM slot 1 or 2.													
<i>iccid</i>	Assign to a specific SIM by ICCID.													
<i>generic</i>	Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.													
slot	SIM slot configuration.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sim1</i></td> <td>Sim slot one.</td> </tr> <tr> <td><i>sim2</i></td> <td>Sim slot two.</td> </tr> </tbody> </table>	Option	Description	<i>sim1</i>	Sim slot one.	<i>sim2</i>	Sim slot two.							
Option	Description													
<i>sim1</i>	Sim slot one.													
<i>sim2</i>	Sim slot two.													
iccid	ICCID configuration.	string	Maximum length: 31											
carrier	Carrier configuration.	string	Maximum length: 31											
apn	APN configuration.	string	Maximum length: 63											
auth-type	Authentication type.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No authentication.</td> </tr> <tr> <td><i>pap</i></td> <td>PAP.</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No authentication.	<i>pap</i>	PAP.	<i>chap</i>	CHAP.					
Option	Description													
<i>none</i>	No authentication.													
<i>pap</i>	PAP.													
<i>chap</i>	CHAP.													
username	Username.	string	Maximum length: 31											
password	Password.	password	Not Specified											
pdn	PDN type.	option	-	ipv4-only										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4-only</i></td> <td>IPv4 only PDN activation.</td> </tr> <tr> <td><i>ipv6-only</i></td> <td>IPv6 only PDN activation.</td> </tr> <tr> <td><i>ipv4-ipv6</i></td> <td>Both IPv4 and IPv6 PDN activations.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4-only</i>	IPv4 only PDN activation.	<i>ipv6-only</i>	IPv6 only PDN activation.	<i>ipv4-ipv6</i>	Both IPv4 and IPv6 PDN activations.					
Option	Description													
<i>ipv4-only</i>	IPv4 only PDN activation.													
<i>ipv6-only</i>	IPv6 only PDN activation.													
<i>ipv4-ipv6</i>	Both IPv4 and IPv6 PDN activations.													

Parameter	Description	Type	Size	Default						
signal-threshold	Signal threshold. Specify the range between 50 - 100, where 50/100 means -50/-100 dBm.	integer	Minimum value: 50 Maximum value: 100	100						
signal-period	Signal period (600 to 18000 seconds).	integer	Minimum value: 600 Maximum value: 18000	3600						
capacity	Capacity in MB .	integer	Minimum value: 0 Maximum value: 102400000	0						
monthly-fee	Monthly fee of dataplan .	integer	Minimum value: 0 Maximum value: 1000000	0						
billing-date	Billing day of the month .	integer	Minimum value: 1 Maximum value: 31	1						
overage	Enable/disable dataplan overage detection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dataplan overage detection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dataplan overage detection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dataplan overage detection.	<i>enable</i>	Enable dataplan overage detection.			
Option	Description									
<i>disable</i>	Disable dataplan overage detection.									
<i>enable</i>	Enable dataplan overage detection.									
preferred-subnet	Preferred subnet mask .	integer	Minimum value: 8 Maximum value: 32	32						
private-network	Enable/disable dataplan private network support.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dataplan private network support.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dataplan private network support.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dataplan private network support.	<i>enable</i>	Enable dataplan private network support.			
Option	Description									
<i>disable</i>	Disable dataplan private network support.									
<i>enable</i>	Enable dataplan private network support.									

## config extender-controller extender

Extender controller configuration.

```

config extender-controller extender
  Description: Extender controller configuration.
  edit <name>
    set id {string}
    set authorized [disable|enable]
    set ext-name {string}
    set description {string}
    set vdom {integer}
    set login-password {password}
  config controller-report
    Description: FortiExtender controller report configuration.
    set status [disable|enable]
    set interval {integer}
    set signal-threshold {integer}
  end
config modem1
  Description: Configuration options for modem 1.
  set ifname {string}
  set redundant-mode [disable|enable]
  set redundant-intf {string}
  set conn-status {integer}
  set default-sim [sim1|sim2|...]
  set gps [disable|enable]
  set sim1-pin [disable|enable]
  set sim2-pin [disable|enable]
  set sim1-pin-code {password}
  set sim2-pin-code {password}
  set preferred-carrier {string}
  config auto-switch
    Description: FortiExtender auto switch configuration.
    set disconnect [disable|enable]
    set disconnect-threshold {integer}
    set disconnect-period {integer}
    set signal [disable|enable]
    set dataplan [disable|enable]
    set switch-back {option1}, {option2}, ...
    set switch-back-time {string}
    set switch-back-timer {integer}
  end
end
config modem2
  Description: Configuration options for modem 2.
  set ifname {string}
  set redundant-mode [disable|enable]
  set redundant-intf {string}
  set conn-status {integer}
  set default-sim [sim1|sim2|...]
  set gps [disable|enable]
  set sim1-pin [disable|enable]
  set sim2-pin [disable|enable]
  set sim1-pin-code {password}
  set sim2-pin-code {password}
  set preferred-carrier {string}
  config auto-switch
    Description: FortiExtender auto switch configuration.
    set disconnect [disable|enable]
    set disconnect-threshold {integer}

```

```

    set disconnect-period {integer}
    set signal [disable|enable]
    set dataplan [disable|enable]
    set switch-back {option1}, {option2}, ...
    set switch-back-time {string}
    set switch-back-timer {integer}
  end
end
next
end

```

## config extender-controller extender

Parameter	Description	Type	Size	Default						
id	FortiExtender serial number.	string	Maximum length: 19							
authorized	FortiExtender Administration (enable or disable).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Controller is configured to not provide service to this FortiExtender.</td> </tr> <tr> <td><i>enable</i></td> <td>Controller is configured to provide service to this FortiExtender.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.	<i>enable</i>	Controller is configured to provide service to this FortiExtender.			
Option	Description									
<i>disable</i>	Controller is configured to not provide service to this FortiExtender.									
<i>enable</i>	Controller is configured to provide service to this FortiExtender.									
ext-name	FortiExtender name.	string	Maximum length: 31							
description	Description.	string	Maximum length: 255							
vdom	VDOM	integer	Minimum value: 0 Maximum value: 4294967295	0						
login-password	FortiExtender login password.	password	Not Specified							

## config controller-report

Parameter	Description	Type	Size	Default						
status	FortiExtender controller report status.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Controller is configured to not provide service to this FortiExtender.</td> </tr> <tr> <td><i>enable</i></td> <td>Controller is configured to provide service to this FortiExtender.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.	<i>enable</i>	Controller is configured to provide service to this FortiExtender.			
Option	Description									
<i>disable</i>	Controller is configured to not provide service to this FortiExtender.									
<i>enable</i>	Controller is configured to provide service to this FortiExtender.									

Parameter	Description	Type	Size	Default
interval	Controller report interval.	integer	Minimum value: 0 Maximum value: 4294967295	300
signal-threshold	Controller report signal threshold.	integer	Minimum value: 0 Maximum value: 4294967295	10

### config modem1

Parameter	Description	Type	Size	Default										
ifname	FortiExtender interface name.	string	Maximum length: 15											
redundant-mode	FortiExtender mode.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable interface redundancy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable interface redundancy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable interface redundancy.	<i>enable</i>	Enable interface redundancy.							
Option	Description													
<i>disable</i>	Disable interface redundancy.													
<i>enable</i>	Enable interface redundancy.													
redundant-intf	Redundant interface.	string	Maximum length: 15											
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0										
default-sim	Default SIM selection.	option	-	sim1										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sim1</i></td> <td>Use SIM #1 by default.</td> </tr> <tr> <td><i>sim2</i></td> <td>Use SIM #2 by default.</td> </tr> <tr> <td><i>carrier</i></td> <td>Assign default SIM based on carrier.</td> </tr> <tr> <td><i>cost</i></td> <td>Assign default SIM based on cost.</td> </tr> </tbody> </table>	Option	Description	<i>sim1</i>	Use SIM #1 by default.	<i>sim2</i>	Use SIM #2 by default.	<i>carrier</i>	Assign default SIM based on carrier.	<i>cost</i>	Assign default SIM based on cost.			
Option	Description													
<i>sim1</i>	Use SIM #1 by default.													
<i>sim2</i>	Use SIM #2 by default.													
<i>carrier</i>	Assign default SIM based on carrier.													
<i>cost</i>	Assign default SIM based on cost.													
gps	FortiExtender GPS enable/disable.	option	-	enable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable GPS.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable GPS.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable GPS.	<i>enable</i>	Enable GPS.			
Option	Description									
<i>disable</i>	Disable GPS.									
<i>enable</i>	Enable GPS.									
sim1-pin	SIM #1 PIN status.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SIM #1 pin.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SIM #1 pin.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SIM #1 pin.	<i>enable</i>	Enable SIM #1 pin.			
Option	Description									
<i>disable</i>	Disable SIM #1 pin.									
<i>enable</i>	Enable SIM #1 pin.									
sim2-pin	SIM #2 PIN status.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SIM #2 pin.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SIM #2 pin.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SIM #2 pin.	<i>enable</i>	Enable SIM #2 pin.			
Option	Description									
<i>disable</i>	Disable SIM #2 pin.									
<i>enable</i>	Enable SIM #2 pin.									
sim1-pin-code	SIM #1 PIN password.	password	Not Specified							
sim2-pin-code	SIM #2 PIN password.	password	Not Specified							
preferred-carrier	Preferred carrier.	string	Maximum length: 31							

### config auto-switch

Parameter	Description	Type	Size	Default						
disconnect	Auto switch by disconnect.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable switching of SIM card based on cellular disconnections.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable switching of SIM card based on cellular disconnections.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable switching of SIM card based on cellular disconnections.	<i>enable</i>	Enable switching of SIM card based on cellular disconnections.			
Option	Description									
<i>disable</i>	Disable switching of SIM card based on cellular disconnections.									
<i>enable</i>	Enable switching of SIM card based on cellular disconnections.									
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 0 Maximum value: 4294967295	3						
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600						
signal	Automatically switch based on signal strength.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable switching of SIM card based on cellular signal quality.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable switching of SIM card based on cellular signal quality.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable switching of SIM card based on cellular signal quality.	<i>enable</i>	Enable switching of SIM card based on cellular signal quality.			
Option	Description									
<i>disable</i>	Disable switching of SIM card based on cellular signal quality.									
<i>enable</i>	Enable switching of SIM card based on cellular signal quality.									
dataplan	Automatically switch based on data usage.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable switching of SIM card based on cellular data usage.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable switching of SIM card based on cellular data usage.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable switching of SIM card based on cellular data usage.	<i>enable</i>	Enable switching of SIM card based on cellular data usage.			
Option	Description									
<i>disable</i>	Disable switching of SIM card based on cellular data usage.									
<i>enable</i>	Enable switching of SIM card based on cellular data usage.									
switch-back	Auto switch with switch back multi-options.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>time</i></td> <td>Switch back based on specific time in UTC (HH:MM).</td> </tr> <tr> <td><i>timer</i></td> <td>Switch back based on an interval.</td> </tr> </tbody> </table>	Option	Description	<i>time</i>	Switch back based on specific time in UTC (HH:MM).	<i>timer</i>	Switch back based on an interval.			
Option	Description									
<i>time</i>	Switch back based on specific time in UTC (HH:MM).									
<i>timer</i>	Switch back based on an interval.									
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01						
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time .	integer	Minimum value: 3600 Maximum value: 2147483647	86400						

## config modem2

Parameter	Description	Type	Size	Default						
ifname	FortiExtender interface name.	string	Maximum length: 15							
redundant-mode	FortiExtender mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable interface redundancy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable interface redundancy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable interface redundancy.	<i>enable</i>	Enable interface redundancy.			
Option	Description									
<i>disable</i>	Disable interface redundancy.									
<i>enable</i>	Enable interface redundancy.									
redundant-intf	Redundant interface.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default										
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0										
default-sim	Default SIM selection.	option	-	sim1										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sim1</i></td> <td>Use SIM #1 by default.</td> </tr> <tr> <td><i>sim2</i></td> <td>Use SIM #2 by default.</td> </tr> <tr> <td><i>carrier</i></td> <td>Assign default SIM based on carrier.</td> </tr> <tr> <td><i>cost</i></td> <td>Assign default SIM based on cost.</td> </tr> </tbody> </table>	Option	Description	<i>sim1</i>	Use SIM #1 by default.	<i>sim2</i>	Use SIM #2 by default.	<i>carrier</i>	Assign default SIM based on carrier.	<i>cost</i>	Assign default SIM based on cost.			
Option	Description													
<i>sim1</i>	Use SIM #1 by default.													
<i>sim2</i>	Use SIM #2 by default.													
<i>carrier</i>	Assign default SIM based on carrier.													
<i>cost</i>	Assign default SIM based on cost.													
gps	FortiExtender GPS enable/disable.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable GPS.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable GPS.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable GPS.	<i>enable</i>	Enable GPS.							
Option	Description													
<i>disable</i>	Disable GPS.													
<i>enable</i>	Enable GPS.													
sim1-pin	SIM #1 PIN status.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SIM #1 pin.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SIM #1 pin.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SIM #1 pin.	<i>enable</i>	Enable SIM #1 pin.							
Option	Description													
<i>disable</i>	Disable SIM #1 pin.													
<i>enable</i>	Enable SIM #1 pin.													
sim2-pin	SIM #2 PIN status.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SIM #2 pin.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SIM #2 pin.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SIM #2 pin.	<i>enable</i>	Enable SIM #2 pin.							
Option	Description													
<i>disable</i>	Disable SIM #2 pin.													
<i>enable</i>	Enable SIM #2 pin.													
sim1-pin-code	SIM #1 PIN password.	password	Not Specified											
sim2-pin-code	SIM #2 PIN password.	password	Not Specified											
preferred-carrier	Preferred carrier.	string	Maximum length: 31											

### config auto-switch

Parameter	Description	Type	Size	Default
disconnect	Auto switch by disconnect.	option	-	disable



Parameter	Description	Type	Size	Default
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 0 Maximum value: 4294967295	3
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600
signal	Automatically switch based on signal strength.	option	-	disable
dataplan	Automatically switch based on data usage.	option	-	disable
switch-back	Auto switch with switch back multi-options.	option	-	
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time .	integer	Minimum value: 3600 Maximum value: 2147483647	86400

## file-filter

This section includes syntax for the following commands:

- [config file-filter profile on page 130](#)

### config file-filter profile

Configure file-filter profiles.

```
config file-filter profile
  Description: Configure file-filter profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    set log [disable|enable]
    set extended-log [disable|enable]
    set scan-archive-contents [disable|enable]
  config rules
    Description: File filter rules.
    edit <name>
      set comment {var-string}
      set protocol {option1}, {option2}, ...
      set action [log-only|block]
      set direction [incoming|outgoing|...]
      set password-protected [yes|any]
      set file-type <name1>, <name2>, ...
    next
  end
next
end
```

### config file-filter profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
feature-set	Flow/proxy feature set.	option	-	flow						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>flow</i></td><td>Flow feature set.</td></tr><tr><td><i>proxy</i></td><td>Proxy feature set.</td></tr></tbody></table>	Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.			
Option	Description									
<i>flow</i>	Flow feature set.									
<i>proxy</i>	Proxy feature set.									
replacemsg-group	Replacement message group	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
log	Enable/disable file-filter logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.			
Option	Description									
<i>disable</i>	Disable logging.									
<i>enable</i>	Enable logging.									
extended-log	Enable/disable file-filter extended logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable extended logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable extended logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable extended logging.	<i>enable</i>	Enable extended logging.			
Option	Description									
<i>disable</i>	Disable extended logging.									
<i>enable</i>	Enable extended logging.									
scan-archive-contents	Enable/disable archive contents scan. (Not for CIFS)	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable scanning archive contents.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable scanning archive contents.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable scanning archive contents.	<i>enable</i>	Enable scanning archive contents.			
Option	Description									
<i>disable</i>	Disable scanning archive contents.									
<i>enable</i>	Enable scanning archive contents.									

## config rules

Parameter	Description	Type	Size	Default																		
comment	Comment.	var-string	Maximum length: 255																			
protocol	Protocols to apply rule to.	option	-	http ftp smtp imap pop3 mapi cifs ssh																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>Filter on HTTP.</td> </tr> <tr> <td><i>ftp</i></td> <td>Filter on FTP.</td> </tr> <tr> <td><i>smtp</i></td> <td>Filter on SMTP.</td> </tr> <tr> <td><i>imap</i></td> <td>Filter on IMAP.</td> </tr> <tr> <td><i>pop3</i></td> <td>Filter on POP3.</td> </tr> <tr> <td><i>mapi</i></td> <td>Filter on MAPI. (Proxy mode only.)</td> </tr> <tr> <td><i>cifs</i></td> <td>Filter on CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>Filter on SFTP and SCP. (Proxy mode only.)</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	Filter on HTTP.	<i>ftp</i>	Filter on FTP.	<i>smtp</i>	Filter on SMTP.	<i>imap</i>	Filter on IMAP.	<i>pop3</i>	Filter on POP3.	<i>mapi</i>	Filter on MAPI. (Proxy mode only.)	<i>cifs</i>	Filter on CIFS.	<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)			
Option	Description																					
<i>http</i>	Filter on HTTP.																					
<i>ftp</i>	Filter on FTP.																					
<i>smtp</i>	Filter on SMTP.																					
<i>imap</i>	Filter on IMAP.																					
<i>pop3</i>	Filter on POP3.																					
<i>mapi</i>	Filter on MAPI. (Proxy mode only.)																					
<i>cifs</i>	Filter on CIFS.																					
<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)																					

Parameter	Description	Type	Size	Default								
action	Action taken for matched file.	option	-	log-only								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>log-only</i></td> <td>Allow the content and write a log message.</td> </tr> <tr> <td><i>block</i></td> <td>Block the content and write a log message.</td> </tr> </tbody> </table>	Option	Description	<i>log-only</i>	Allow the content and write a log message.	<i>block</i>	Block the content and write a log message.					
Option	Description											
<i>log-only</i>	Allow the content and write a log message.											
<i>block</i>	Block the content and write a log message.											
direction	Traffic direction. (HTTP, FTP, SSH, CIFS only)	option	-	any								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>incoming</i></td> <td>Match files transmitted in the session's reply direction.</td> </tr> <tr> <td><i>outgoing</i></td> <td>Match files transmitted in the session's originating direction.</td> </tr> <tr> <td><i>any</i></td> <td>Match files transmitted in the session's originating and reply directions.</td> </tr> </tbody> </table>	Option	Description	<i>incoming</i>	Match files transmitted in the session's reply direction.	<i>outgoing</i>	Match files transmitted in the session's originating direction.	<i>any</i>	Match files transmitted in the session's originating and reply directions.			
Option	Description											
<i>incoming</i>	Match files transmitted in the session's reply direction.											
<i>outgoing</i>	Match files transmitted in the session's originating direction.											
<i>any</i>	Match files transmitted in the session's originating and reply directions.											
password-protected	Match password-protected files.	option	-	any								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>yes</i></td> <td>Match only password-protected files.</td> </tr> <tr> <td><i>any</i></td> <td>Match any file.</td> </tr> </tbody> </table>	Option	Description	<i>yes</i>	Match only password-protected files.	<i>any</i>	Match any file.					
Option	Description											
<i>yes</i>	Match only password-protected files.											
<i>any</i>	Match any file.											
file-type <name>	Select file type. File type name.	string	Maximum length: 39									

## firewall

This section includes syntax for the following commands:

- [config firewall internet-service-botnet on page 169](#)
- [config firewall shaping-policy on page 326](#)
- [config firewall proute on page 380](#)
- [config firewall multicast-policy6 on page 352](#)
- [config firewall interface-policy on page 354](#)
- [config firewall internet-service-owner on page 167](#)
- [config firewall ssh local-ca on page 374](#)
- [config firewall shaper per-ip on page 174](#)
- [config firewall decrypted-traffic-mirror on page 301](#)
- [config firewall wildcard-fqdn group on page 149](#)
- [config firewall vip on page 185](#)
- [config firewall interface-policy6 on page 357](#)
- [config firewall ssh host-key on page 375](#)
- [config firewall internet-service-definition on page 168](#)
- [config firewall DoS-policy on page 360](#)
- [config firewall schedule group on page 180](#)
- [config firewall dnstranslation on page 349](#)
- [config firewall ssh local-key on page 373](#)
- [config firewall addrgrp on page 146](#)
- [config firewall sniffer on page 364](#)
- [config firewall policy on page 309](#)
- [config firewall shaper per-ip-shaper on page 173](#)
- [config firewall service custom on page 151](#)
- [config firewall service group on page 155](#)
- [config firewall address on page 135](#)
- [config firewall internet-service-sld on page 166](#)
- [config firewall internet-service-ipbl-vendor on page 167](#)
- [config firewall ippool on page 181](#)
- [config firewall wildcard-fqdn custom on page 149](#)
- [config firewall iprope list on page 379](#)
- [config firewall service category on page 150](#)
- [config firewall address6 on page 142](#)
- [config firewall iprope appctrl list on page 380](#)
- [config firewall proxy-policy on page 342](#)
- [config firewall vipgrp6 on page 250](#)
- [config firewall local-in-policy6 on page 334](#)
- [config firewall ip-translation on page 377](#)
- [config firewall ssl-server on page 298](#)
- [config firewall ippool6 on page 183](#)

- 
- [config firewall country on page 156](#)
  - [config firewall vip46 on page 214](#)
  - [config firewall vendor-mac-summary on page 170](#)
  - [config firewall traffic-class on page 326](#)
  - [config firewall internet-service-group on page 159](#)
  - [config firewall security-policy on page 303](#)
  - [config firewall local-in-policy on page 333](#)
  - [config firewall profile-group on page 297](#)
  - [config firewall shaper traffic on page 174](#)
  - [config firewall internet-service-list on page 168](#)
  - [config firewall address6-template on page 141](#)
  - [config firewall ipmacbinding table on page 253](#)
  - [config firewall ldb-monitor on page 184](#)
  - [config firewall internet-service-reputation on page 162](#)
  - [config firewall multicast-policy on page 350](#)
  - [config firewall schedule onetime on page 179](#)
  - [config firewall internet-service-addition on page 164](#)
  - [config firewall identity-based-route on page 302](#)
  - [config firewall shaper traffic-shaper on page 170](#)
  - [config firewall ssl-ssh-profile on page 275](#)
  - [config firewall auth-portal on page 302](#)
  - [config firewall DoS-policy6 on page 362](#)
  - [config firewall vendor-mac on page 170](#)
  - [config firewall proxy-address on page 174](#)
  - [config firewall ipv6-eh-filter on page 378](#)
  - [config firewall vip6 on page 218](#)
  - [config firewall vipgrp on page 249](#)
  - [config firewall policy64 on page 337](#)
  - [config firewall iprope appctrl status on page 380](#)
  - [config firewall central-snat-map on page 369](#)
  - [config firewall internet-service-extension on page 160](#)
  - [config firewall internet-service-name on page 158](#)
  - [config firewall policy46 on page 339](#)
  - [config firewall multicast-address6 on page 145](#)
  - [config firewall multicast-address on page 139](#)
  - [config firewall internet-service-ipbl-reason on page 167](#)
  - [config firewall internet-service on page 157](#)
  - [config firewall vipgrp46 on page 250](#)
  - [config firewall internet-service-append on page 165](#)
  - [config firewall internet-service-custom-group on page 166](#)
  - [config firewall city on page 156](#)
  - [config firewall ipmacbinding setting on page 252](#)
  - [config firewall profile-protocol-options on page 253](#)
  - [config firewall internet-service-custom on page 163](#)
  - [config firewall region on page 156](#)

- [config firewall schedule recurring on page 179](#)
- [config firewall vip64 on page 245](#)
- [config firewall proute6 on page 380](#)
- [config firewall vipgrp64 on page 251](#)
- [config firewall shaping-profile on page 331](#)
- [config firewall proxy-addrgrp on page 177](#)
- [config firewall ssh setting on page 374](#)
- [config firewall ttl-policy on page 336](#)
- [config firewall ssl setting on page 371](#)
- [config firewall addrgrp6 on page 148](#)

## config firewall address

Configure IPv4 addresses.

```
config firewall address
  Description: Configure IPv4 addresses.
  edit <name>
    set uuid {uuid}
    set subnet {ipv4-classnet-any}
    set type [ipmask|iprange|...]
    set sub-type [sdn|clearpass-spt|...]
    set clearpass-spt [unknown|healthy|...]
    set start-mac {mac-address}
    set end-mac {mac-address}
    set start-ip {ipv4-address-any}
    set end-ip {ipv4-address-any}
    set fqdn {string}
    set country {string}
    set wildcard-fqdn {string}
    set cache-ttl {integer}
    set wildcard {ipv4-classnet-any}
    set sdn {string}
    set fsso-group <name1>, <name2>, ...
    set interface {string}
    set tenant {string}
    set organization {string}
    set epg-name {string}
    set subnet-name {string}
    set sdn-tag {string}
    set policy-group {string}
    set obj-tag {string}
    set obj-type [ip|mac]
    set comment {var-string}
    set associated-interface {string}
    set color {integer}
    set filter {var-string}
    set sdn-addr-type [private|public|...]
    set obj-id {var-string}
  config list
    Description: IP address list.
    edit <ip>
    next
```

```

end
config tagging
  Description: Config object tagging.
  edit <name>
    set category {string}
    set tags <name1>, <name2>, ...
  next
end
set allow-routing [enable|disable]
set fabric-object [enable|disable]
next
end

```

## config firewall address

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
type	Type of address.	option	-	ipmask
	<b>Option</b>	<b>Description</b>		
	<i>ipmask</i>	Standard IPv4 address with subnet mask.		
	<i>iprange</i>	Range of IPv4 addresses between two specified addresses (inclusive).		
	<i>fqdn</i>	Fully Qualified Domain Name address.		
	<i>geography</i>	IP addresses from a specified country.		
	<i>wildcard</i>	Standard IPv4 using a wildcard subnet mask.		
	<i>dynamic</i>	Dynamic address object.		
	<i>interface-subnet</i>	IP and subnet of interface.		
	<i>mac</i>	Range of MAC addresses.		
sub-type	Sub-type of address.	option	-	sdn
	<b>Option</b>	<b>Description</b>		
	<i>sdn</i>	SDN address.		
	<i>clearpass-spt</i>	ClearPass SPT (System Posture Token) address.		
	<i>fsso</i>	FSSO address.		
	<i>ems-tag</i>	FortiClient EMS tag.		



Parameter	Description	Type	Size	Default														
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>unknown</i></td> <td>UNKNOWN.</td> </tr> <tr> <td><i>healthy</i></td> <td>HEALTHY.</td> </tr> <tr> <td><i>quarantine</i></td> <td>QUARANTINE.</td> </tr> <tr> <td><i>checkup</i></td> <td>CHECKUP.</td> </tr> <tr> <td><i>transient</i></td> <td>TRANSIENT.</td> </tr> <tr> <td><i>infected</i></td> <td>INFECTED.</td> </tr> </tbody> </table>	Option	Description	<i>unknown</i>	UNKNOWN.	<i>healthy</i>	HEALTHY.	<i>quarantine</i>	QUARANTINE.	<i>checkup</i>	CHECKUP.	<i>transient</i>	TRANSIENT.	<i>infected</i>	INFECTED.			
Option	Description																	
<i>unknown</i>	UNKNOWN.																	
<i>healthy</i>	HEALTHY.																	
<i>quarantine</i>	QUARANTINE.																	
<i>checkup</i>	CHECKUP.																	
<i>transient</i>	TRANSIENT.																	
<i>infected</i>	INFECTED.																	
start-mac	First MAC address in the range.	mac-address	Not Specified	00:00:00:00:00:00														
end-mac	Last MAC address in the range.	mac-address	Not Specified	00:00:00:00:00:00														
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255															
country	IP addresses associated to a specific country.	string	Maximum length: 2															
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255															
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400	0														
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0														
sdn	SDN.	string	Maximum length: 35															
fssso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511															

Parameter	Description	Type	Size	Default								
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35									
tenant	Tenant.	string	Maximum length: 35									
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35									
epg-name	Endpoint group name.	string	Maximum length: 255									
subnet-name	Subnet name.	string	Maximum length: 255									
sdn-tag	SDN Tag.	string	Maximum length: 15									
policy-group	Policy group name.	string	Maximum length: 15									
obj-tag	Tag of dynamic address object.	string	Maximum length: 255									
obj-type	Object type.	option	-	ip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ip</i></td> <td>IP address.</td> </tr> <tr> <td><i>mac</i></td> <td>MAC address</td> </tr> </tbody> </table>		Option	Description	<i>ip</i>	IP address.	<i>mac</i>	MAC address				
Option	Description											
<i>ip</i>	IP address.											
<i>mac</i>	MAC address											
comment	Comment.	var-string	Maximum length: 255									
associated-interface	Network interface associated with address.	string	Maximum length: 35									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0								
filter	Match criteria filter.	var-string	Maximum length: 2047									
sdn-addr-type	Type of addresses to collect.	option	-	private								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>private</i></td> <td>Collect private addresses only.</td> </tr> <tr> <td><i>public</i></td> <td>Collect public addresses only.</td> </tr> <tr> <td><i>all</i></td> <td>Collect both public and private addresses.</td> </tr> </tbody> </table>		Option	Description	<i>private</i>	Collect private addresses only.	<i>public</i>	Collect public addresses only.	<i>all</i>	Collect both public and private addresses.		
Option	Description											
<i>private</i>	Collect private addresses only.											
<i>public</i>	Collect public addresses only.											
<i>all</i>	Collect both public and private addresses.											

Parameter	Description	Type	Size	Default
obj-id	Object ID for NSX.	var-string	Maximum length: 255	
allow-routing	Enable/disable use of this address in the static route configuration.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of this address in the static route configuration.		
	<i>disable</i>	Disable use of this address in the static route configuration.		
fabric-object	Security Fabric global object setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall multicast-address

Configure multicast addresses.

```

config firewall multicast-address
  Description: Configure multicast addresses.
  edit <name>
    set type [multicastrange|broadcastmask]
    set subnet {ipv4-classnet-any}
    set start-ip {ipv4-address-any}
    set end-ip {ipv4-address-any}
    set comment {var-string}
    set associated-interface {string}
    set color {integer}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
  next
end
next

```

end

## config firewall multicast-address

Parameter	Description	Type	Size	Default						
type	Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.	option	-	multicastrange						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>multicastrange</i></td><td>Multicast range.</td></tr><tr><td><i>broadcastmask</i></td><td>Broadcast IP/mask.</td></tr></tbody></table>	Option	Description	<i>multicastrange</i>	Multicast range.	<i>broadcastmask</i>	Broadcast IP/mask.			
Option	Description									
<i>multicastrange</i>	Multicast range.									
<i>broadcastmask</i>	Broadcast IP/mask.									
subnet	Broadcast address and subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0						
start-ip	First IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0						
end-ip	Final IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0						
comment	Comment.	var-string	Maximum length: 255							
associated-interface	Interface associated with the address object. When setting up a policy, only addresses associated with this interface are available.	string	Maximum length: 35							
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0						

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall address6-template

Configure IPv6 address templates.

```
config firewall address6-template
  Description: Configure IPv6 address templates.
  edit <name>
    set ip6 {ipv6-network}
    set subnet-segment-count {integer}
    config subnet-segment
      Description: IPv6 subnet segments.
      edit <id>
        set name {string}
        set bits {integer}
        set exclusive [enable|disable]
        config values
          Description: Subnet segment values.
          edit <name>
            set value {string}
          next
        end
      next
    end
  next
end
```

## config firewall address6-template

Parameter	Description	Type	Size	Default
ip6	IPv6 address prefix.	ipv6-network	Not Specified	::/0
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6	0

## config subnet-segment

Parameter	Description	Type	Size	Default
name	Subnet segment name.	string	Maximum length: 63	
bits	Number of bits.	integer	Minimum value: 1 Maximum value: 16	0
exclusive	Enable/disable exclusive value.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable exclusive value.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable exclusive value.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable exclusive value.	<i>disable</i>	Disable exclusive value.			
Option	Description									
<i>enable</i>	Enable exclusive value.									
<i>disable</i>	Disable exclusive value.									

### config values

Parameter	Description	Type	Size	Default
value	Subnet segment value.	string	Maximum length: 35	

## config firewall address6

Configure IPv6 firewall addresses.

```

config firewall address6
  Description: Configure IPv6 firewall addresses.
  edit <name>
    set uuid {uuid}
    set type [ipprefix|iprange|...]
    set start-mac {mac-address}
    set end-mac {mac-address}
    set sdn {string}
    set ip6 {ipv6-network}
    set start-ip {ipv6-address}
    set end-ip {ipv6-address}
    set fqdn {string}
    set country {string}
    set cache-ttl {integer}
    set color {integer}
    set obj-id {var-string}
  config list
    Description: IP address list.
    edit <ip>
      next
    end
  config tagging
    Description: Config object tagging
    edit <name>
      set category {string}
      set tags <name1>, <name2>, ...
    next
  end
  set comment {var-string}
  set template {string}
  config subnet-segment
    Description: IPv6 subnet segments.
    edit <name>
      set type [any|specific]
      set value {string}

```

```

    next
end
set host-type [any|specific]
set host {ipv6-address}
set fabric-object [enable|disable]
next
end

```

## config firewall address6

Parameter	Description	Type	Size	Default																
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000																
type	Type of IPv6 address object .	option	-	ipprefix																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipprefix</i></td> <td>Uses the IP prefix to define a range of IPv6 addresses.</td> </tr> <tr> <td><i>iprange</i></td> <td>Range of IPv6 addresses between two specified addresses (inclusive).</td> </tr> <tr> <td><i>fqdn</i></td> <td>Fully qualified domain name.</td> </tr> <tr> <td><i>geography</i></td> <td>IPv6 addresses from a specified country.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Dynamic address object for SDN.</td> </tr> <tr> <td><i>template</i></td> <td>Template.</td> </tr> <tr> <td><i>mac</i></td> <td>Range of MAC addresses.</td> </tr> </tbody> </table>	Option	Description	<i>ipprefix</i>	Uses the IP prefix to define a range of IPv6 addresses.	<i>iprange</i>	Range of IPv6 addresses between two specified addresses (inclusive).	<i>fqdn</i>	Fully qualified domain name.	<i>geography</i>	IPv6 addresses from a specified country.	<i>dynamic</i>	Dynamic address object for SDN.	<i>template</i>	Template.	<i>mac</i>	Range of MAC addresses.			
Option	Description																			
<i>ipprefix</i>	Uses the IP prefix to define a range of IPv6 addresses.																			
<i>iprange</i>	Range of IPv6 addresses between two specified addresses (inclusive).																			
<i>fqdn</i>	Fully qualified domain name.																			
<i>geography</i>	IPv6 addresses from a specified country.																			
<i>dynamic</i>	Dynamic address object for SDN.																			
<i>template</i>	Template.																			
<i>mac</i>	Range of MAC addresses.																			
start-mac	First MAC address in the range.	mac-address	Not Specified	00:00:00:00:00:00																
end-mac	Last MAC address in the range.	mac-address	Not Specified	00:00:00:00:00:00																
sdn	SDN.	string	Maximum length: 35																	
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified	::/0																
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::																
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::																
fqdn	Fully qualified domain name.	string	Maximum length: 255																	

Parameter	Description	Type	Size	Default						
country	IPv6 addresses associated to a specific country.	string	Maximum length: 2							
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400	0						
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0						
obj-id	Object ID for NSX.	var-string	Maximum length: 255							
comment	Comment.	var-string	Maximum length: 255							
template	IPv6 address template.	string	Maximum length: 63							
host-type	Host type.	option	-	any						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Wildcard.</td> </tr> <tr> <td><i>specific</i></td> <td>Specific host address.</td> </tr> </tbody> </table>		Option	Description	<i>any</i>	Wildcard.	<i>specific</i>	Specific host address.		
Option	Description									
<i>any</i>	Wildcard.									
<i>specific</i>	Specific host address.									
host	Host Address.	ipv6-address	Not Specified	::						
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Object is set as a security fabric-wide global object.</td> </tr> <tr> <td><i>disable</i></td> <td>Object is local to this security fabric member.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.		
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	



## config subnet-segment

Parameter	Description	Type	Size	Default						
type	Subnet segment type.	option	-	any						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>any</i></td><td>Wildcard.</td></tr><tr><td><i>specific</i></td><td>Specific subnet segment address.</td></tr></tbody></table>	Option	Description	<i>any</i>	Wildcard.	<i>specific</i>	Specific subnet segment address.			
Option	Description									
<i>any</i>	Wildcard.									
<i>specific</i>	Specific subnet segment address.									
value	Subnet segment value.	string	Maximum length: 35							

## config firewall multicast-address6

Configure IPv6 multicast address.

```
config firewall multicast-address6
  Description: Configure IPv6 multicast address.
  edit <name>
    set ip6 {ipv6-network}
    set comment {var-string}
    set color {integer}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
  next
end
```

## config firewall multicast-address6

Parameter	Description	Type	Size	Default
ip6	IPv6 address prefix (format: xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx/xxx).	ipv6-network	Not Specified	::/0
comment	Comment.	var-string	Maximum length: 255	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall addrgrp

Configure IPv4 address groups.

```
config firewall addrgrp
  Description: Configure IPv4 address groups.
  edit <name>
    set type [default|folder]
    set uuid {uuid}
    set member <name1>, <name2>, ...
    set comment {var-string}
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    set color {integer}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set allow-routing [enable|disable]
    set fabric-object [enable|disable]
  next
end
```

## config firewall addrgrp

Parameter	Description	Type	Size	Default						
type	Address group type.	option	-	default						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>default</i></td><td>Default address group type (address may belong to multiple groups).</td></tr><tr><td><i>folder</i></td><td>Address folder group (members may not belong to any other group).</td></tr></tbody></table>	Option	Description	<i>default</i>	Default address group type (address may belong to multiple groups).	<i>folder</i>	Address folder group (members may not belong to any other group).			
Option	Description									
<i>default</i>	Default address group type (address may belong to multiple groups).									
<i>folder</i>	Address folder group (members may not belong to any other group).									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

Parameter	Description	Type	Size	Default						
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79							
comment	Comment.	var-string	Maximum length: 255							
exclude	Enable/disable address exclusion.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable address exclusion.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable address exclusion.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable address exclusion.	<i>disable</i>	Disable address exclusion.			
Option	Description									
<i>enable</i>	Enable address exclusion.									
<i>disable</i>	Disable address exclusion.									
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79							
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
allow-routing	Enable/disable use of this group in the static route configuration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of this group in the static route configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of this group in the static route configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of this group in the static route configuration.	<i>disable</i>	Disable use of this group in the static route configuration.			
Option	Description									
<i>enable</i>	Enable use of this group in the static route configuration.									
<i>disable</i>	Disable use of this group in the static route configuration.									
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Object is set as a security fabric-wide global object.</td> </tr> <tr> <td><i>disable</i></td> <td>Object is local to this security fabric member.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.			
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall addrgrp6

Configure IPv6 address groups.

```
config firewall addrgrp6
  Description: Configure IPv6 address groups.
  edit <name>
    set uuid {uuid}
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
  config tagging
    Description: Config object tagging.
    edit <name>
      set category {string}
      set tags <name1>, <name2>, ...
    next
  end
  set fabric-object [enable|disable]
next
end
```

## config firewall addrgrp6

Parameter	Description	Type	Size	Default						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0						
comment	Comment.	var-string	Maximum length: 255							
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.			
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall wildcard-fqdn custom

Config global/VDOM Wildcard FQDN address.

```
config firewall wildcard-fqdn custom
  Description: Config global/VDOM Wildcard FQDN address.
  edit <name>
    set uuid {uuid}
    set wildcard-fqdn {string}
    set color {integer}
    set comment {var-string}
  next
end
```

## config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	

## config firewall wildcard-fqdn group

Config global Wildcard FQDN address groups.

```
config firewall wildcard-fqdn group
  Description: Config global Wildcard FQDN address groups.
  edit <name>
    set uuid {uuid}
    set member <name1>, <name2>, ...
```

```

    set color {integer}
    set comment {var-string}
  next
end

```

## config firewall wildcard-fqdn group

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
member <name>	Address group members. Address name.	string	Maximum length: 79	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	

## config firewall service category

Configure service categories.

```

config firewall service category
  Description: Configure service categories.
  edit <name>
    set comment {var-string}
    set fabric-object [enable|disable]
  next
end

```

## config firewall service category

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Object is set as a security fabric-wide global object.</td> </tr> <tr> <td><i>disable</i></td> <td>Object is local to this security fabric member.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.			
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

## config firewall service custom

Configure custom services.

```
config firewall service custom
  Description: Configure custom services.
  edit <name>
    set proxy [enable|disable]
    set category {string}
    set protocol [TCP/UDP/SCTP/ICMP|...]
    set helper [auto|disable|...]
    set iprange {user}
    set fqdn {string}
    set protocol-number {integer}
    set icmp-type {integer}
    set icmp-code {integer}
    set tcp-portrange {user}
    set udp-portrange {user}
    set sctp-portrange {user}
    set tcp-halfclose-timer {integer}
    set tcp-halfopen-timer {integer}
    set tcp-timewait-timer {integer}
    set udp-idle-timer {integer}
    set session-ttl {user}
    set check-reset-range [disable|strict|...]
    set comment {var-string}
    set color {integer}
    set visibility [enable|disable]
    set app-service-type [disable|app-id|...]
    set app-category <id1>, <id2>, ...
    set application <id1>, <id2>, ...
    set fabric-object [enable|disable]
  next
end
```

## config firewall service custom

Parameter	Description	Type	Size	Default						
proxy	Enable/disable web proxy service.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
category	Service category.	string	Maximum length: 63							
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP						

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TCP/UDP/SCTP</i></td> <td>TCP, UDP and SCTP.</td> </tr> <tr> <td><i>ICMP</i></td> <td>ICMP.</td> </tr> <tr> <td><i>ICMP6</i></td> <td>ICMP6.</td> </tr> <tr> <td><i>IP</i></td> <td>IP.</td> </tr> <tr> <td><i>HTTP</i></td> <td>HTTP - for web proxy.</td> </tr> <tr> <td><i>FTP</i></td> <td>FTP - for web proxy.</td> </tr> <tr> <td><i>CONNECT</i></td> <td>Connect - for web proxy.</td> </tr> <tr> <td><i>SOCKS-TCP</i></td> <td>Socks TCP - for web proxy.</td> </tr> <tr> <td><i>SOCKS-UDP</i></td> <td>Socks UDP - for web proxy.</td> </tr> <tr> <td><i>ALL</i></td> <td>All - for web proxy.</td> </tr> </tbody> </table>	Option	Description	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.	<i>ICMP</i>	ICMP.	<i>ICMP6</i>	ICMP6.	<i>IP</i>	IP.	<i>HTTP</i>	HTTP - for web proxy.	<i>FTP</i>	FTP - for web proxy.	<i>CONNECT</i>	Connect - for web proxy.	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.	<i>SOCKS-UDP</i>	Socks UDP - for web proxy.	<i>ALL</i>	All - for web proxy.																	
Option	Description																																							
<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.																																							
<i>ICMP</i>	ICMP.																																							
<i>ICMP6</i>	ICMP6.																																							
<i>IP</i>	IP.																																							
<i>HTTP</i>	HTTP - for web proxy.																																							
<i>FTP</i>	FTP - for web proxy.																																							
<i>CONNECT</i>	Connect - for web proxy.																																							
<i>SOCKS-TCP</i>	Socks TCP - for web proxy.																																							
<i>SOCKS-UDP</i>	Socks UDP - for web proxy.																																							
<i>ALL</i>	All - for web proxy.																																							
helper	Helper name.	option	-	auto																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically select helper based on protocol and port.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable helper.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>tftp</i></td> <td>TFTP.</td> </tr> <tr> <td><i>ras</i></td> <td>RAS.</td> </tr> <tr> <td><i>h323</i></td> <td>H323.</td> </tr> <tr> <td><i>tns</i></td> <td>TNS.</td> </tr> <tr> <td><i>mms</i></td> <td>MMS.</td> </tr> <tr> <td><i>sip</i></td> <td>SIP.</td> </tr> <tr> <td><i>pptp</i></td> <td>PPTP.</td> </tr> <tr> <td><i>rtsp</i></td> <td>RTSP.</td> </tr> <tr> <td><i>dns-udp</i></td> <td>DNS UDP.</td> </tr> <tr> <td><i>dns-tcp</i></td> <td>DNS TCP.</td> </tr> <tr> <td><i>pmap</i></td> <td>PMAP.</td> </tr> <tr> <td><i>rsh</i></td> <td>RSH.</td> </tr> <tr> <td><i>dcercp</i></td> <td>DCERPC.</td> </tr> <tr> <td><i>mgcp</i></td> <td>MGCP.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically select helper based on protocol and port.	<i>disable</i>	Disable helper.	<i>ftp</i>	FTP.	<i>tftp</i>	TFTP.	<i>ras</i>	RAS.	<i>h323</i>	H323.	<i>tns</i>	TNS.	<i>mms</i>	MMS.	<i>sip</i>	SIP.	<i>pptp</i>	PPTP.	<i>rtsp</i>	RTSP.	<i>dns-udp</i>	DNS UDP.	<i>dns-tcp</i>	DNS TCP.	<i>pmap</i>	PMAP.	<i>rsh</i>	RSH.	<i>dcercp</i>	DCERPC.	<i>mgcp</i>	MGCP.			
Option	Description																																							
<i>auto</i>	Automatically select helper based on protocol and port.																																							
<i>disable</i>	Disable helper.																																							
<i>ftp</i>	FTP.																																							
<i>tftp</i>	TFTP.																																							
<i>ras</i>	RAS.																																							
<i>h323</i>	H323.																																							
<i>tns</i>	TNS.																																							
<i>mms</i>	MMS.																																							
<i>sip</i>	SIP.																																							
<i>pptp</i>	PPTP.																																							
<i>rtsp</i>	RTSP.																																							
<i>dns-udp</i>	DNS UDP.																																							
<i>dns-tcp</i>	DNS TCP.																																							
<i>pmap</i>	PMAP.																																							
<i>rsh</i>	RSH.																																							
<i>dcercp</i>	DCERPC.																																							
<i>mgcp</i>	MGCP.																																							



Parameter	Description	Type	Size	Default
iprange	Start and end of the IP range associated with service.	user	Not Specified	
fqdn	Fully qualified domain name.	string	Maximum length: 255	
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295	
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255	
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
udp-portrange	Multiple UDP port ranges.	user	Not Specified	
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet .	integer	Minimum value: 0 Maximum value: 86400	0
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet .	integer	Minimum value: 0 Maximum value: 86400	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds .	integer	Minimum value: 0 Maximum value: 300	0
udp-idle-timer	UDP half close timeout .	integer	Minimum value: 0 Maximum value: 86400	0
session-ttl	Session TTL .	user	Not Specified	

Parameter	Description	Type	Size	Default								
check-reset-range	Configure the type of ICMP error message verification.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable RST range check.</td> </tr> <tr> <td><i>strict</i></td> <td>Check RST range strictly.</td> </tr> <tr> <td><i>default</i></td> <td>Using system default setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable RST range check.	<i>strict</i>	Check RST range strictly.	<i>default</i>	Using system default setting.			
Option	Description											
<i>disable</i>	Disable RST range check.											
<i>strict</i>	Check RST range strictly.											
<i>default</i>	Using system default setting.											
comment	Comment.	var-string	Maximum length: 255									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0								
visibility	Enable/disable the visibility of the service on the GUI.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Show in service selection.</td> </tr> <tr> <td><i>disable</i></td> <td>Hide from service selection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Show in service selection.	<i>disable</i>	Hide from service selection.					
Option	Description											
<i>enable</i>	Show in service selection.											
<i>disable</i>	Hide from service selection.											
app-service-type	Application service type.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable application type.</td> </tr> <tr> <td><i>app-id</i></td> <td>Application ID.</td> </tr> <tr> <td><i>app-category</i></td> <td>Applicatin category.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable application type.	<i>app-id</i>	Application ID.	<i>app-category</i>	Applicatin category.			
Option	Description											
<i>disable</i>	Disable application type.											
<i>app-id</i>	Application ID.											
<i>app-category</i>	Applicatin category.											
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295									
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295									
fabric-object	Security Fabric global object setting.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Object is set as a security fabric-wide global object.</td> </tr> <tr> <td><i>disable</i></td> <td>Object is local to this security fabric member.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.			
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

## config firewall service group

Configure service groups.

```
config firewall service group
  Description: Configure service groups.
  edit <name>
    set proxy [enable|disable]
    set member <name1>, <name2>, ...
    set comment {var-string}
    set color {integer}
    set fabric-object [enable|disable]
  next
end
```

## config firewall service group

Parameter	Description	Type	Size	Default						
proxy	Enable/disable web proxy service group.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
member <name>	Service objects contained within the group. Address name.	string	Maximum length: 79							
comment	Comment.	var-string	Maximum length: 255							
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Object is set as a security fabric-wide global object.</td> </tr> <tr> <td><i>disable</i></td> <td>Object is local to this security fabric member.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.			
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

---

## config firewall city

Define city table.

```
config firewall city
  Description: Define city table.
  edit <id>
    set name {string}
  next
end
```

## config firewall city

Parameter	Description	Type	Size	Default
name	City name.	string	Maximum length: 63	

## config firewall region

Define region table.

```
config firewall region
  Description: Define region table.
  edit <id>
    set name {string}
    set city <id1>, <id2>, ...
  next
end
```

## config firewall region

Parameter	Description	Type	Size	Default
name	Region name.	string	Maximum length: 63	
city <id>	City ID list. City ID.	integer	Minimum value: 0 Maximum value: 65535	

## config firewall country

Define country table.

```
config firewall country
  Description: Define country table.
  edit <id>
```

```

    set name {string}
    set region <id1>, <id2>, ...
  next
end

```

## config firewall country

Parameter	Description	Type	Size	Default
name	Country name.	string	Maximum length: 63	
region <id>	Region ID list. Region ID.	integer	Minimum value: 0 Maximum value: 65535	

## config firewall internet-service

Show Internet Service application.

```

config firewall internet-service
  Description: Show Internet Service application.
  edit <id>
    set name {string}
    set icon-id {integer}
    set direction [src|dst|...]
    set database [isdb|irdb]
    set ip-range-number {integer}
    set extra-ip-range-number {integer}
    set ip-number {integer}
    set singularity {integer}
    set obsolete {integer}
  next
end

```

## config firewall internet-service

Parameter	Description	Type	Size	Default
name	Internet Service name.	string	Maximum length: 63	
icon-id	Icon ID of Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
direction	How this service may be used in a firewall policy (source, destination or both).	option	-	both								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>src</i></td> <td>As source in the firewall policy.</td> </tr> <tr> <td><i>dst</i></td> <td>As destination in the firewall policy.</td> </tr> <tr> <td><i>both</i></td> <td>Both directions in the firewall policy.</td> </tr> </tbody> </table>	Option	Description	<i>src</i>	As source in the firewall policy.	<i>dst</i>	As destination in the firewall policy.	<i>both</i>	Both directions in the firewall policy.			
Option	Description											
<i>src</i>	As source in the firewall policy.											
<i>dst</i>	As destination in the firewall policy.											
<i>both</i>	Both directions in the firewall policy.											
database	Database name this Internet Service belongs to.	option	-	isdb								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>isdb</i></td> <td>Internet Service Database.</td> </tr> <tr> <td><i>irdb</i></td> <td>Internet RRR Database.</td> </tr> </tbody> </table>	Option	Description	<i>isdb</i>	Internet Service Database.	<i>irdb</i>	Internet RRR Database.					
Option	Description											
<i>isdb</i>	Internet Service Database.											
<i>irdb</i>	Internet RRR Database.											
ip-range-number	Number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0								
extra-ip-range-number	Extra number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0								
ip-number	Total number of IP addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0								
singularity	Singular level of the Internet Service.	integer	Minimum value: 0 Maximum value: 65535	0								
obsolete	Indicates whether the Internet Service can be used.	integer	Minimum value: 0 Maximum value: 255	0								

## config firewall internet-service-name

Define internet service names.

```
config firewall internet-service-name
    Description: Define internet service names.
```

```

edit <name>
  set type [default|location]
  set internet-service-id {integer}
  set country-id {integer}
  set region-id {integer}
  set city-id {integer}
next
end

```

## config firewall internet-service-name

Parameter	Description	Type	Size	Default						
type	Internet Service name type.	option	-	default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Automatically generated Internet Service.</td> </tr> <tr> <td><i>location</i></td> <td>Geography location based Internet Service.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Automatically generated Internet Service.	<i>location</i>	Geography location based Internet Service.			
Option	Description									
<i>default</i>	Automatically generated Internet Service.									
<i>location</i>	Geography location based Internet Service.									
internet-service-id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
country-id	Country or Area ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
region-id	Region ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
city-id	City ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config firewall internet-service-group

Configure group of Internet Service.

```

config firewall internet-service-group
  Description: Configure group of Internet Service.
  edit <name>
    set comment {var-string}
  end
end

```

```

    set direction [source|destination|...]
    set member <name1>, <name2>, ...
  next
end

```

## config firewall internet-service-group

Parameter	Description	Type	Size	Default								
comment	Comment.	var-string	Maximum length: 255									
direction	How this service may be used (source, destination or both).	option	-	both								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>source</i></td> <td>As source when applied.</td> </tr> <tr> <td><i>destination</i></td> <td>As destination when applied.</td> </tr> <tr> <td><i>both</i></td> <td>Both directions when applied.</td> </tr> </tbody> </table>	Option	Description	<i>source</i>	As source when applied.	<i>destination</i>	As destination when applied.	<i>both</i>	Both directions when applied.			
Option	Description											
<i>source</i>	As source when applied.											
<i>destination</i>	As destination when applied.											
<i>both</i>	Both directions when applied.											
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79									

## config firewall internet-service-extension

Configure Internet Services Extension.

```

config firewall internet-service-extension
  Description: Configure Internet Services Extension.
  edit <id>
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service extension database.
      edit <id>
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
        set dst <name1>, <name2>, ...
      next
    end
  config disable-entry
    Description: Disable entries in the Internet Service database.
    edit <id>
      set protocol {integer}
      config port-range
        Description: Port ranges in the disable entry.

```



```

edit <id>
    set start-port {integer}
    set end-port {integer}
next
end
config ip-range
    Description: IP ranges in the disable entry.
edit <id>
    set start-ip {ipv4-address-any}
    set end-ip {ipv4-address-any}
next
end
next
end
next
end
end

```

## config firewall internet-service-extension

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	

## config entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	

## config port-range

Parameter	Description	Type	Size	Default
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

## config disable-entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0

## config port-range

Parameter	Description	Type	Size	Default
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

## config ip-range

Parameter	Description	Type	Size	Default
start-ip	Start IP address.	ipv4-address-any	Not Specified	0.0.0.0
end-ip	End IP address.	ipv4-address-any	Not Specified	0.0.0.0

## config firewall internet-service-reputation

Show Internet Service reputation.

```
config firewall internet-service-reputation
  Description: Show Internet Service reputation.
  edit <id>
    set description {string}
  next
end
```

## config firewall internet-service-reputation

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	

## config firewall internet-service-custom

Configure custom Internet Services.

```
config firewall internet-service-custom
  Description: Configure custom Internet Services.
  edit <name>
    set reputation {integer}
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service database and custom database.
      edit <id>
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
        set dst <name1>, <name2>, ...
      next
    end
  next
end
```

## config firewall internet-service-custom

Parameter	Description	Type	Size	Default
reputation	Reputation level of the custom Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	3
comment	Comment.	var-string	Maximum length: 255	

## config entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	

## config port-range

Parameter	Description	Type	Size	Default
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

## config firewall internet-service-addition

Configure Internet Services Addition.

```
config firewall internet-service-addition
  Description: Configure Internet Services Addition.
  edit <id>
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service addition database.
      edit <id>
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      next
    end
  next
end
next
end
```

## config firewall internet-service-addition

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	

## config entry

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0

## config port-range

Parameter	Description	Type	Size	Default
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

## config firewall internet-service-append

Configure additional port mappings for Internet Services.

```
config firewall internet-service-append
  Description: Configure additional port mappings for Internet Services.
  set match-port {integer}
  set append-port {integer}
end
```

## config firewall internet-service-append

Parameter	Description	Type	Size	Default
match-port	Matching TCP/UDP/SCTP destination port (0 to 65535, 0 means any port).	integer	Minimum value: 0 Maximum value: 65535	0
append-port	Appending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	0

## config firewall internet-service-custom-group

Configure custom Internet Service group.

```
config firewall internet-service-custom-group
  Description: Configure custom Internet Service group.
  edit <name>
    set comment {var-string}
    set member <name1>, <name2>, ...
  next
end
```

## config firewall internet-service-custom-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
member <name>	Custom Internet Service group members. Group member name.	string	Maximum length: 79	

## config firewall internet-service-sld

Internet Service Second Level Domain.

```
config firewall internet-service-sld
  Description: Internet Service Second Level Domain.
  edit <id>
    set name {string}
  next
end
```

## config firewall internet-service-sld

Parameter	Description	Type	Size	Default
name	Second Level Domain name.	string	Maximum length: 63	

## config firewall internet-service-ipbl-vendor

IP blacklist vendor.

```
config firewall internet-service-ipbl-vendor
  Description: IP blacklist vendor.
  edit <id>
    set name {string}
  next
end
```

## config firewall internet-service-ipbl-vendor

Parameter	Description	Type	Size	Default
name	IP blacklist vendor name.	string	Maximum length: 63	

## config firewall internet-service-ipbl-reason

IP blacklist reason.

```
config firewall internet-service-ipbl-reason
  Description: IP blacklist reason.
  edit <id>
    set name {string}
  next
end
```

## config firewall internet-service-ipbl-reason

Parameter	Description	Type	Size	Default
name	IP blacklist reason name.	string	Maximum length: 63	

## config firewall internet-service-owner

Internet Service owner.

```
config firewall internet-service-owner
```

```

Description: Internet Service owner.
edit <id>
    set name {string}
next
end

```

### config firewall internet-service-owner

Parameter	Description	Type	Size	Default
name	Internet Service owner name.	string	Maximum length: 63	

### config firewall internet-service-list

Internet Service list.

```

config firewall internet-service-list
    Description: Internet Service list.
    edit <id>
        set name {string}
    next
end

```

### config firewall internet-service-list

Parameter	Description	Type	Size	Default
name	Internet Service category name.	string	Maximum length: 63	

### config firewall internet-service-definition

Configure Internet Service definition.

```

config firewall internet-service-definition
    Description: Configure Internet Service definition.
    edit <id>
        config entry
            Description: Protocol and port information in an Internet Service entry.
            edit <seq-num>
                set category-id {integer}
                set name {string}
                set protocol {integer}
                config port-range
                    Description: Port ranges in the definition entry.
                    edit <id>
                        set start-port {integer}
                        set end-port {integer}
                    next
                end
            end
        end
    end

```



```

    next
  end
  next
end

```

### config entry

Parameter	Description	Type	Size	Default
category-id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0

### config port-range

Parameter	Description	Type	Size	Default
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

## config firewall internet-service-botnet

Show Internet Service botnet.

```

config firewall internet-service-botnet
  Description: Show Internet Service botnet.
  edit <id>
    set name {string}
  next
end

```

## config firewall internet-service-botnet

Parameter	Description	Type	Size	Default
name	Internet Service Botnet name.	string	Maximum length: 63	

## config firewall vendor-mac

Show vendor and the MAC address they have.

```
config firewall vendor-mac
  Description: Show vendor and the MAC address they have.
  edit <id>
    set name {string}
    set mac-number {integer}
  next
end
```

## config firewall vendor-mac

Parameter	Description	Type	Size	Default
name	Vendor name.	string	Maximum length: 63	
mac-number	Total number of MAC addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config firewall vendor-mac-summary

Vendor MAC database summary.

```
config firewall vendor-mac-summary
  Description: Vendor MAC database summary.
end
```

## config firewall shaper traffic-shaper

Configure shared traffic shaper.

```
config firewall shaper traffic-shaper
  Description: Configure shared traffic shaper.
  edit <name>
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
    set bandwidth-unit [kbps|mbps|...]
  next
end
```

```

set priority [low|medium|...]
set per-policy [disable|enable]
set diffserv [enable|disable]
set diffservcode {user}
set dscp-marking-method [multi-stage|static]
set exceed-bandwidth {integer}
set exceed-dscp {user}
set maximum-dscp {user}
set overhead {integer}
set exceed-class-id {integer}
next
end

```

## config firewall shaper traffic-shaper

Parameter	Description	Type	Size	Default								
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper . Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0								
maximum-bandwidth	Upper bandwidth limit enforced by this shaper . 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0								
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kbps</i></td> <td>Kilobits per second.</td> </tr> <tr> <td><i>mbps</i></td> <td>Megabits per second.</td> </tr> <tr> <td><i>gbps</i></td> <td>Gigabits per second.</td> </tr> </tbody> </table>	Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.			
Option	Description											
<i>kbps</i>	Kilobits per second.											
<i>mbps</i>	Megabits per second.											
<i>gbps</i>	Gigabits per second.											
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-	high								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Low priority.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium priority.</td> </tr> <tr> <td><i>high</i></td> <td>High priority.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Low priority.	<i>medium</i>	Medium priority.	<i>high</i>	High priority.			
Option	Description											
<i>low</i>	Low priority.											
<i>medium</i>	Medium priority.											
<i>high</i>	High priority.											

Parameter	Description	Type	Size	Default						
per-policy	Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>All referring policies share one traffic shaper.</td> </tr> <tr> <td><i>enable</i></td> <td>Each referring policy has its own traffic shaper.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	All referring policies share one traffic shaper.	<i>enable</i>	Each referring policy has its own traffic shaper.			
Option	Description									
<i>disable</i>	All referring policies share one traffic shaper.									
<i>enable</i>	Each referring policy has its own traffic shaper.									
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting traffic DiffServ.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting traffic DiffServ.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting traffic DiffServ.	<i>disable</i>	Disable setting traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting traffic DiffServ.									
<i>disable</i>	Disable setting traffic DiffServ.									
diffservcode	DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							
dscp-marking-method	Select DSCP marking method.	option	-	static						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>multi-stage</i></td> <td>Multistage marking.</td> </tr> <tr> <td><i>static</i></td> <td>Static marking.</td> </tr> </tbody> </table>	Option	Description	<i>multi-stage</i>	Multistage marking.	<i>static</i>	Static marking.			
Option	Description									
<i>multi-stage</i>	Multistage marking.									
<i>static</i>	Static marking.									
exceed-bandwidth	Exceed bandwidth used for DSCP multi-stage marking. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0						
exceed-dscp	DSCP mark for traffic in [guaranteed-bandwidth, exceed-bandwidth].	user	Not Specified							
maximum-dscp	DSCP mark for traffic in [exceed-bandwidth, maximum-bandwidth].	user	Not Specified							
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 Maximum value: 100	0						
exceed-class-id	Class ID for traffic in [guaranteed-bandwidth, maximum-bandwidth].	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config firewall shaper per-ip-shaper

Configure per-IP traffic shaper.

```
config firewall shaper per-ip-shaper
  Description: Configure per-IP traffic shaper.
  edit <name>
    set max-bandwidth {integer}
    set bandwidth-unit [kbps|mbps|...]
    set max-concurrent-session {integer}
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
  next
end
```

## config firewall shaper per-ip-shaper

Parameter	Description	Type	Size	Default								
max-bandwidth	Upper bandwidth limit enforced by this shaper . 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0								
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>kbps</i></td><td>Kilobits per second.</td></tr><tr><td><i>mbps</i></td><td>Megabits per second.</td></tr><tr><td><i>gbps</i></td><td>Gigabits per second.</td></tr></tbody></table>	Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.			
Option	Description											
<i>kbps</i>	Kilobits per second.											
<i>mbps</i>	Megabits per second.											
<i>gbps</i>	Gigabits per second.											
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper . 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0								
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting forward (original) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting forward (original) traffic DiffServ.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting forward (original) traffic DiffServ.	<i>disable</i>	Disable setting forward (original) traffic DiffServ.					
Option	Description											
<i>enable</i>	Enable setting forward (original) traffic DiffServ.											
<i>disable</i>	Disable setting forward (original) traffic DiffServ.											

Parameter	Description	Type	Size	Default						
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting reverse (reply) traffic DiffServ.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting reverse (reply) traffic DiffServ.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.									
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							
diffservcode-rev	Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							

## config firewall shaper traffic

Shared traffic shapers.

```
config firewall shaper traffic
  Description: Shared traffic shapers.
end
```

## config firewall shaper per-ip

Per-IP traffic shapers.

```
config firewall shaper per-ip
  Description: Per-IP traffic shapers.
end
```

## config firewall proxy-address

Configure web proxy address.

```
config firewall proxy-address
  Description: Configure web proxy address.
  edit <name>
    set uuid {uuid}
    set type [host-regex|url|...]
    set host {string}
    set host-regex {string}
    set path {string}
    set query {string}
    set referrer [enable|disable]
    set category <id1>, <id2>, ...
    set method {option1}, {option2}, ...
    set ua {option1}, {option2}, ...
    set header-name {string}
    set header {string}
    set case-sensitivity [disable|enable]
```

```

config header-group
  Description: HTTP header group.
  edit <id>
    set header-name {string}
    set header {string}
    set case-sensitivity [disable|enable]
  next
end
set color {integer}
config tagging
  Description: Config object tagging.
  edit <name>
    set category {string}
    set tags <name1>, <name2>, ...
  next
end
set comment {var-string}
next
end

```

## config firewall proxy-address

Parameter	Description	Type	Size	Default																		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000																		
type	Proxy address type.	option	-	url																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>host-regex</i></td> <td>Host regular expression.</td> </tr> <tr> <td><i>url</i></td> <td>HTTP URL.</td> </tr> <tr> <td><i>category</i></td> <td>FortiGuard URL category.</td> </tr> <tr> <td><i>method</i></td> <td>HTTP request method.</td> </tr> <tr> <td><i>ua</i></td> <td>HTTP request user agent.</td> </tr> <tr> <td><i>header</i></td> <td>HTTP request header.</td> </tr> <tr> <td><i>src-advanced</i></td> <td>HTTP advanced source criteria.</td> </tr> <tr> <td><i>dst-advanced</i></td> <td>HTTP advanced destination criteria.</td> </tr> </tbody> </table>	Option	Description	<i>host-regex</i>	Host regular expression.	<i>url</i>	HTTP URL.	<i>category</i>	FortiGuard URL category.	<i>method</i>	HTTP request method.	<i>ua</i>	HTTP request user agent.	<i>header</i>	HTTP request header.	<i>src-advanced</i>	HTTP advanced source criteria.	<i>dst-advanced</i>	HTTP advanced destination criteria.			
Option	Description																					
<i>host-regex</i>	Host regular expression.																					
<i>url</i>	HTTP URL.																					
<i>category</i>	FortiGuard URL category.																					
<i>method</i>	HTTP request method.																					
<i>ua</i>	HTTP request user agent.																					
<i>header</i>	HTTP request header.																					
<i>src-advanced</i>	HTTP advanced source criteria.																					
<i>dst-advanced</i>	HTTP advanced destination criteria.																					
host	Address object for the host.	string	Maximum length: 79																			
host-regex	Host name as a regular expression.	string	Maximum length: 255																			
path	URL path as a regular expression.	string	Maximum length: 255																			

Parameter	Description	Type	Size	Default																		
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255																			
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
Option	Description																					
<i>enable</i>	Enable setting.																					
<i>disable</i>	Disable setting.																					
category <id>	FortiGuard category ID. Fortiguard category id.	integer	Minimum value: 0 Maximum value: 4294967295																			
method	HTTP request methods to be used.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>get</i></td> <td>GET method.</td> </tr> <tr> <td><i>post</i></td> <td>POST method.</td> </tr> <tr> <td><i>put</i></td> <td>PUT method.</td> </tr> <tr> <td><i>head</i></td> <td>HEAD method.</td> </tr> <tr> <td><i>connect</i></td> <td>CONNECT method.</td> </tr> <tr> <td><i>trace</i></td> <td>TRACE method.</td> </tr> <tr> <td><i>options</i></td> <td>OPTIONS method.</td> </tr> <tr> <td><i>delete</i></td> <td>DELETE method.</td> </tr> </tbody> </table>	Option	Description	<i>get</i>	GET method.	<i>post</i>	POST method.	<i>put</i>	PUT method.	<i>head</i>	HEAD method.	<i>connect</i>	CONNECT method.	<i>trace</i>	TRACE method.	<i>options</i>	OPTIONS method.	<i>delete</i>	DELETE method.			
Option	Description																					
<i>get</i>	GET method.																					
<i>post</i>	POST method.																					
<i>put</i>	PUT method.																					
<i>head</i>	HEAD method.																					
<i>connect</i>	CONNECT method.																					
<i>trace</i>	TRACE method.																					
<i>options</i>	OPTIONS method.																					
<i>delete</i>	DELETE method.																					
ua	Names of browsers to be used as user agent.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>chrome</i></td> <td>Google Chrome.</td> </tr> <tr> <td><i>ms</i></td> <td>Microsoft Internet Explorer or EDGE.</td> </tr> <tr> <td><i>firefox</i></td> <td>Mozilla Firefox.</td> </tr> <tr> <td><i>safari</i></td> <td>Apple Safari.</td> </tr> <tr> <td><i>other</i></td> <td>Other browsers.</td> </tr> </tbody> </table>	Option	Description	<i>chrome</i>	Google Chrome.	<i>ms</i>	Microsoft Internet Explorer or EDGE.	<i>firefox</i>	Mozilla Firefox.	<i>safari</i>	Apple Safari.	<i>other</i>	Other browsers.									
Option	Description																					
<i>chrome</i>	Google Chrome.																					
<i>ms</i>	Microsoft Internet Explorer or EDGE.																					
<i>firefox</i>	Mozilla Firefox.																					
<i>safari</i>	Apple Safari.																					
<i>other</i>	Other browsers.																					
header-name	Name of HTTP header.	string	Maximum length: 79																			



Parameter	Description	Type	Size	Default						
header	HTTP header name as a regular expression.	string	Maximum length: 255							
case-sensitivity	Enable to make the pattern case sensitive.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Case insensitive in pattern.</td> </tr> <tr> <td><i>enable</i></td> <td>Case sensitive in pattern.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Case insensitive in pattern.	<i>enable</i>	Case sensitive in pattern.			
Option	Description									
<i>disable</i>	Case insensitive in pattern.									
<i>enable</i>	Case sensitive in pattern.									
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0						
comment	Optional comments.	var-string	Maximum length: 255							

### config header-group

Parameter	Description	Type	Size	Default						
header-name	HTTP header.	string	Maximum length: 79							
header	HTTP header regular expression.	string	Maximum length: 255							
case-sensitivity	Case sensitivity in pattern.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Case insensitive in pattern.</td> </tr> <tr> <td><i>enable</i></td> <td>Case sensitive in pattern.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Case insensitive in pattern.	<i>enable</i>	Case sensitive in pattern.			
Option	Description									
<i>disable</i>	Case insensitive in pattern.									
<i>enable</i>	Case sensitive in pattern.									

### config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

### config firewall proxy-addgrp

Configure web proxy address group.

```

config firewall proxy-addrgrp
  Description: Configure web proxy address group.
  edit <name>
    set type [src|dst]
    set uuid {uuid}
    set member <name1>, <name2>, ...
    set color {integer}
  config tagging
    Description: Config object tagging.
    edit <name>
      set category {string}
      set tags <name1>, <name2>, ...
    next
  end
  set comment {var-string}
next
end

```

## config firewall proxy-addrgrp

Parameter	Description	Type	Size	Default						
type	Source or destination address group type.	option	-	src						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>src</td> <td>Source group.</td> </tr> <tr> <td>dst</td> <td>Destination group.</td> </tr> </tbody> </table>	Option	Description	src	Source group.	dst	Destination group.			
Option	Description									
src	Source group.									
dst	Destination group.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
member <name>	Members of address group. Address name.	string	Maximum length: 79							
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0						
comment	Optional comments.	var-string	Maximum length: 255							

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall schedule onetime

Onetime schedule configuration.

```
config firewall schedule onetime
  Description: Onetime schedule configuration.
  edit <name>
    set start {user}
    set end {user}
    set color {integer}
    set expiration-days {integer}
    set fabric-object [enable|disable]
  next
end
```

## config firewall schedule onetime

Parameter	Description	Type	Size	Default
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
<i>enable</i>	Object is set as a security fabric-wide global object.
<i>disable</i>	Object is local to this security fabric member.

## config firewall schedule recurring

Recurring schedule configuration.

```
config firewall schedule recurring
  Description: Recurring schedule configuration.
  edit <name>
    set start {user}
    set end {user}
    set day {option1}, {option2}, ...
    set color {integer}
```

```

    set fabric-object [enable|disable]
  next
end

```

## config firewall schedule recurring

Parameter	Description	Type	Size	Default																		
start	Time of day to start the schedule, format hh:mm.	user	Not Specified																			
end	Time of day to end the schedule, format hh:mm.	user	Not Specified																			
day	One or more days of the week on which the schedule is valid. Separate the names of the days with a space.	option	-	none																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sunday</i></td> <td>Sunday.</td> </tr> <tr> <td><i>monday</i></td> <td>Monday.</td> </tr> <tr> <td><i>tuesday</i></td> <td>Tuesday.</td> </tr> <tr> <td><i>wednesday</i></td> <td>Wednesday.</td> </tr> <tr> <td><i>thursday</i></td> <td>Thursday.</td> </tr> <tr> <td><i>friday</i></td> <td>Friday.</td> </tr> <tr> <td><i>saturday</i></td> <td>Saturday.</td> </tr> <tr> <td><i>none</i></td> <td>None.</td> </tr> </tbody> </table>	Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.	<i>none</i>	None.			
Option	Description																					
<i>sunday</i>	Sunday.																					
<i>monday</i>	Monday.																					
<i>tuesday</i>	Tuesday.																					
<i>wednesday</i>	Wednesday.																					
<i>thursday</i>	Thursday.																					
<i>friday</i>	Friday.																					
<i>saturday</i>	Saturday.																					
<i>none</i>	None.																					
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0																		
fabric-object	Security Fabric global object setting.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Object is set as a security fabric-wide global object.</td> </tr> <tr> <td><i>disable</i></td> <td>Object is local to this security fabric member.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.															
Option	Description																					
<i>enable</i>	Object is set as a security fabric-wide global object.																					
<i>disable</i>	Object is local to this security fabric member.																					

## config firewall schedule group

Schedule group configuration.

```

config firewall schedule group
  Description: Schedule group configuration.
  edit <name>
    set member <name1>, <name2>, ...
  end
end

```

```

    set color {integer}
    set fabric-object [enable|disable]
  next
end

```

## config firewall schedule group

Parameter	Description	Type	Size	Default
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable

Option	Description
<i>enable</i>	Object is set as a security fabric-wide global object.
<i>disable</i>	Object is local to this security fabric member.

## config firewall ippool

Configure IPv4 IP pools.

```

config firewall ippool
  Description: Configure IPv4 IP pools.
  edit <name>
    set type [overload|one-to-one|...]
    set startip {ipv4-address-any}
    set endip {ipv4-address-any}
    set source-startip {ipv4-address-any}
    set source-endip {ipv4-address-any}
    set block-size {integer}
    set num-blocks-per-user {integer}
    set pba-timeout {integer}
    set permit-any-host [disable|enable]
    set arp-reply [disable|enable]
    set arp-intf {string}
    set associated-interface {string}
    set comments {var-string}
  next
end

```

## config firewall ippool

Parameter	Description	Type	Size	Default										
type	IP pool type (overload, one-to-one, fixed port range, or port block allocation).	option	-	overload										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>overload</i></td> <td>IP addresses in the IP pool can be shared by clients.</td> </tr> <tr> <td><i>one-to-one</i></td> <td>One to one mapping.</td> </tr> <tr> <td><i>fixed-port-range</i></td> <td>Fixed port range.</td> </tr> <tr> <td><i>port-block-allocation</i></td> <td>Port block allocation.</td> </tr> </tbody> </table>	Option	Description	<i>overload</i>	IP addresses in the IP pool can be shared by clients.	<i>one-to-one</i>	One to one mapping.	<i>fixed-port-range</i>	Fixed port range.	<i>port-block-allocation</i>	Port block allocation.			
Option	Description													
<i>overload</i>	IP addresses in the IP pool can be shared by clients.													
<i>one-to-one</i>	One to one mapping.													
<i>fixed-port-range</i>	Fixed port range.													
<i>port-block-allocation</i>	Port block allocation.													
startip	First IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
endip	Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
source-startip	First IPv4 address (inclusive) in the range of the source addresses to be translated (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
source-endip	Final IPv4 address (inclusive) in the range of the source addresses to be translated (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
block-size	Number of addresses in a block .	integer	Minimum value: 64 Maximum value: 4096	128										
num-blocks-per-user	Number of addresses blocks that can be used by a user .	integer	Minimum value: 1 Maximum value: 128	8										
pba-timeout	Port block allocation timeout (seconds).	integer	Minimum value: 3 Maximum value: 300	30										
permit-any-host	Enable/disable full cone NAT.	option	-	disable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable full cone NAT.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable full cone NAT.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable full cone NAT.	<i>enable</i>	Enable full cone NAT.			
Option	Description									
<i>disable</i>	Disable full cone NAT.									
<i>enable</i>	Enable full cone NAT.									
arp-reply	Enable/disable replying to ARP requests when an IP Pool is added to a policy .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable ARP reply.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable ARP reply.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.			
Option	Description									
<i>disable</i>	Disable ARP reply.									
<i>enable</i>	Enable ARP reply.									
arp-intf	Select an interface from available options that will reply to ARP requests. (If blank, any is selected).	string	Maximum length: 15							
associated-interface	Associated interface name.	string	Maximum length: 15							
comments	Comment.	var-string	Maximum length: 255							

## config firewall ippool6

Configure IPv6 IP pools.

```
config firewall ippool6
  Description: Configure IPv6 IP pools.
  edit <name>
    set startip {ipv6-address}
    set endip {ipv6-address}
    set comments {var-string}
  next
end
```

## config firewall ippool6

Parameter	Description	Type	Size	Default
startip	First IPv6 address (inclusive) in the range for the address pool (format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, Default: ::).	ipv6-address	Not Specified	::
endip	Final IPv6 address (inclusive) in the range for the address pool (format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, Default: ::).	ipv6-address	Not Specified	::
comments	Comment.	var-string	Maximum length: 255	

## config firewall ldb-monitor

Configure server load balancing health monitors.

```
config firewall ldb-monitor
  Description: Configure server load balancing health monitors.
  edit <name>
    set type [ping|tcp|...]
    set interval {integer}
    set timeout {integer}
    set retry {integer}
    set port {integer}
    set src-ip {ipv4-address}
    set http-get {string}
    set http-match {string}
    set http-max-redirects {integer}
  next
end
```

## config firewall ldb-monitor

Parameter	Description	Type	Size	Default										
type	Select the Monitor type used by the health check monitor to check the health of the server (PING   TCP   HTTP   HTTPS).	option	-											
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ping</i></td><td>PING health monitor.</td></tr><tr><td><i>tcp</i></td><td>TCP-connect health monitor.</td></tr><tr><td><i>http</i></td><td>HTTP-GET health monitor.</td></tr><tr><td><i>https</i></td><td>HTTP-GET health monitor with SSL.</td></tr></tbody></table>	Option	Description	<i>ping</i>	PING health monitor.	<i>tcp</i>	TCP-connect health monitor.	<i>http</i>	HTTP-GET health monitor.	<i>https</i>	HTTP-GET health monitor with SSL.			
Option	Description													
<i>ping</i>	PING health monitor.													
<i>tcp</i>	TCP-connect health monitor.													
<i>http</i>	HTTP-GET health monitor.													
<i>https</i>	HTTP-GET health monitor with SSL.													
interval	Time between health checks .	integer	Minimum value: 5 Maximum value: 65535	10										
timeout	Time to wait to receive response to a health check from a server. Reaching the timeout means the health check failed .	integer	Minimum value: 1 Maximum value: 255	2										
retry	Number health check attempts before the server is considered down .	integer	Minimum value: 1 Maximum value: 255	3										



Parameter	Description	Type	Size	Default
port	Service port used to perform the health check. If 0, health check monitor inherits port configured for the server .	integer	Minimum value: 0 Maximum value: 65535	0
src-ip	Source IP for ldb-monitor.	ipv4-address	Not Specified	0.0.0.0
http-get	URL used to send a GET request to check the health of an HTTP server.	string	Maximum length: 255	
http-match	String to match the value expected in response to an HTTP-GET request.	string	Maximum length: 255	
http-max-redirects	The maximum number of HTTP redirects to be allowed .	integer	Minimum value: 0 Maximum value: 5	0

## config firewall vip

Configure virtual IP for IPv4.

```
config firewall vip
  Description: Configure virtual IP for IPv4.
  edit <name>
    set id {integer}
    set uuid {uuid}
    set comment {var-string}
    set type [static-nat|load-balance|...]
    set dns-mapping-ttl {integer}
    set ldb-method [static|round-robin|...]
    set src-filter <range1>, <range2>, ...
    set service <name1>, <name2>, ...
    set extip {user}
    set extaddr <name1>, <name2>, ...
    set mappedip <range1>, <range2>, ...
    set mapped-addr {string}
    set extintf {string}
    set arp-reply [disable|enable]
    set server-type [http|https|...]
    set http-redirect [enable|disable]
    set persistence [none|http-cookie|...]
    set nat-source-vip [disable|enable]
    set portforward [disable|enable]
    set protocol [tcp|udp|...]
    set extport {user}
    set mappedport {user}
    set gratuitous-arp-interval {integer}
    set srcintf-filter <interface-name1>, <interface-name2>, ...
    set portmapping-type [1-to-1|m-to-n]
  config realservers
```

```

Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
edit <id>
    set type [ip|address]
    set address {string}
    set ip {ipv4-address-any}
    set port {integer}
    set status [active|standby|...]
    set weight {integer}
    set holddown-interval {integer}
    set healthcheck [disable|enable|...]
    set http-host {string}
    set max-connections {integer}
    set monitor <name1>, <name2>, ...
    set client-ip {user}
next
end
set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set http-multiplex [enable|disable]
set http-ip-header [enable|disable]
set http-ip-header-name {string}
set outlook-web-access [disable|enable]
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
set ssl-mode [half|full]
set ssl-certificate {string}
set ssl-dh-bits [768|1024|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-pfs [require|deny|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-send-empty-frags [enable|disable]
set ssl-client-fallback [disable|enable]
set ssl-client-renegotiation [allow|deny|...]

```

```

set ssl-client-session-state-type [disable|time|...]
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-max {integer}
set ssl-client-rekey-count {integer}
set ssl-server-session-state-type [disable|time|...]
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-max {integer}
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-hpkp [disable|enable|...]
set ssl-hpkp-primary {string}
set ssl-hpkp-backup {string}
set ssl-hpkp-age {integer}
set ssl-hpkp-report-uri {var-string}
set ssl-hpkp-include-subdomains [disable|enable]
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set monitor <name1>, <name2>, ...
set max-embryonic-connections {integer}
set color {integer}
next
end

```

## config firewall vip

Parameter	Description	Type	Size	Default
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
comment	Comment.	var-string	Maximum length: 255	
type	Configure a static NAT, load balance, server load balance, DNS translation, or FQDN VIP.	option	-	static-nat

Option	Description
<i>static-nat</i>	Static NAT.
<i>load-balance</i>	Load balance.
<i>server-load-balance</i>	Server load balance.
<i>dns-translation</i>	DNS translation.
<i>fqdn</i>	Fully qualified domain name.

Parameter	Description	Type	Size	Default																
dns-mapping-ttl	DNS mapping TTL .	integer	Minimum value: 0 Maximum value: 604800	0																
ldb-method	Method used to distribute sessions to real servers.	option	-	static																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Distribute to server based on source IP.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Distribute to server based round robin order.</td> </tr> <tr> <td><i>weighted</i></td> <td>Distribute to server based on weight.</td> </tr> <tr> <td><i>least-session</i></td> <td>Distribute to server with lowest session count.</td> </tr> <tr> <td><i>least-rtt</i></td> <td>Distribute to server with lowest Round-Trip-Time.</td> </tr> <tr> <td><i>first-alive</i></td> <td>Distribute to the first server that is alive.</td> </tr> <tr> <td><i>http-host</i></td> <td>Distribute to server based on host field in HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>least-session</i>	Distribute to server with lowest session count.	<i>least-rtt</i>	Distribute to server with lowest Round-Trip-Time.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.			
Option	Description																			
<i>static</i>	Distribute to server based on source IP.																			
<i>round-robin</i>	Distribute to server based round robin order.																			
<i>weighted</i>	Distribute to server based on weight.																			
<i>least-session</i>	Distribute to server with lowest session count.																			
<i>least-rtt</i>	Distribute to server with lowest Round-Trip-Time.																			
<i>first-alive</i>	Distribute to the first server that is alive.																			
<i>http-host</i>	Distribute to server based on host field in HTTP header.																			
src-filter <range>	Source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y.y). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79																	
service <name>	Service name. Service name.	string	Maximum length: 79																	
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified																	
extaddr <name>	External FQDN address name. Address name.	string	Maximum length: 79																	
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79																	
mapped-addr	Mapped FQDN address name.	string	Maximum length: 79																	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35																	

Parameter	Description	Type	Size	Default																				
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable ARP reply.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable ARP reply.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.																	
Option	Description																							
<i>disable</i>	Disable ARP reply.																							
<i>enable</i>	Enable ARP reply.																							
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS</td> </tr> <tr> <td><i>imaps</i></td> <td>IMAPS</td> </tr> <tr> <td><i>pop3s</i></td> <td>POP3S</td> </tr> <tr> <td><i>smtps</i></td> <td>SMTPS</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL</td> </tr> <tr> <td><i>tcp</i></td> <td>TCP</td> </tr> <tr> <td><i>udp</i></td> <td>UDP</td> </tr> <tr> <td><i>ip</i></td> <td>IP</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP	<i>https</i>	HTTPS	<i>imaps</i>	IMAPS	<i>pop3s</i>	POP3S	<i>smtps</i>	SMTPS	<i>ssl</i>	SSL	<i>tcp</i>	TCP	<i>udp</i>	UDP	<i>ip</i>	IP			
Option	Description																							
<i>http</i>	HTTP																							
<i>https</i>	HTTPS																							
<i>imaps</i>	IMAPS																							
<i>pop3s</i>	POP3S																							
<i>smtps</i>	SMTPS																							
<i>ssl</i>	SSL																							
<i>tcp</i>	TCP																							
<i>udp</i>	UDP																							
<i>ip</i>	IP																							
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redirection of HTTP to HTTPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redirection of HTTP to HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.																	
Option	Description																							
<i>enable</i>	Enable redirection of HTTP to HTTPS.																							
<i>disable</i>	Disable redirection of HTTP to HTTPS.																							
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>http-cookie</i></td> <td>HTTP cookie.</td> </tr> <tr> <td><i>ssl-session-id</i></td> <td>SSL session ID.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.	<i>ssl-session-id</i>	SSL session ID.															
Option	Description																							
<i>none</i>	None.																							
<i>http-cookie</i>	HTTP cookie.																							
<i>ssl-session-id</i>	SSL session ID.																							

Parameter	Description	Type	Size	Default										
nat-source-vip	Enable/disable forcing the source NAT mapped IP to the external IP for all traffic.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.</td> </tr> <tr> <td><i>enable</i></td> <td>Force the source NAT mapped IP to the external IP for all traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.	<i>enable</i>	Force the source NAT mapped IP to the external IP for all traffic.							
Option	Description													
<i>disable</i>	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.													
<i>enable</i>	Force the source NAT mapped IP to the external IP for all traffic.													
portforward	Enable/disable port forwarding.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable port forward.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable port forward.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable port forward.							
Option	Description													
<i>disable</i>	Disable port forward.													
<i>enable</i>	Enable port forward.													
protocol	Protocol to use when forwarding packets.	option	-	tcp										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp</i></td> <td>TCP.</td> </tr> <tr> <td><i>udp</i></td> <td>UDP.</td> </tr> <tr> <td><i>sctp</i></td> <td>SCTP.</td> </tr> <tr> <td><i>icmp</i></td> <td>ICMP.</td> </tr> </tbody> </table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.	<i>icmp</i>	ICMP.			
Option	Description													
<i>tcp</i>	TCP.													
<i>udp</i>	UDP.													
<i>sctp</i>	SCTP.													
<i>icmp</i>	ICMP.													
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified											
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified											
gratuitous-arp-interval	Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to enable.	integer	Minimum value: 5 Maximum value: 8640000	0										
srcintf-filter <interface-name>	Interfaces to which the VIP applies. Separate the names with spaces. Interface name.	string	Maximum length: 79											
portmapping-type	Port mapping type.	option	-	1-to-1										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1-to-1</i></td> <td>One to one.</td> </tr> <tr> <td><i>m-to-n</i></td> <td>Many to many.</td> </tr> </tbody> </table>	Option	Description	<i>1-to-1</i>	One to one.	<i>m-to-n</i>	Many to many.			
Option	Description									
<i>1-to-1</i>	One to one.									
<i>m-to-n</i>	Many to many.									
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of HTTP cookie domain from host field in HTTP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.			
Option	Description									
<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).									
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-share	Control sharing of cookies across virtual servers. same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Only allow HTTP cookie to match this virtual server.</td> </tr> <tr> <td><i>same-ip</i></td> <td>Allow HTTP cookie to match any virtual server with same IP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Only allow HTTP cookie to match this virtual server.	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.			
Option	Description									
<i>disable</i>	Only allow HTTP cookie to match this virtual server.									
<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td> </tr> <tr> <td><i>enable</i></td> <td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.			
Option	Description									
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.									
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HTTP session multiplexing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HTTP session multiplexing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HTTP session multiplexing.	<i>disable</i>	Disable HTTP session multiplexing.			
Option	Description									
<i>enable</i>	Enable HTTP session multiplexing.									
<i>disable</i>	Disable HTTP session multiplexing.									
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding HTTP header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding HTTP header.	<i>disable</i>	Disable adding HTTP header.			
Option	Description									
<i>enable</i>	Enable adding HTTP header.									
<i>disable</i>	Disable adding HTTP header.									
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35							
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Outlook Web Access support.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Outlook Web Access support.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Outlook Web Access support.	<i>enable</i>	Enable Outlook Web Access support.			
Option	Description									
<i>disable</i>	Disable Outlook Web Access support.									
<i>enable</i>	Enable Outlook Web Access support.									
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add HTTP header indicating SSL offload for WebLogic server.</td> </tr> <tr> <td><i>enable</i></td> <td>Add HTTP header indicating SSL offload for WebLogic server.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.			
Option	Description									
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.									
<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.									
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable						



Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add HTTP header indicating SSL offload for WebSphere server.</td> </tr> <tr> <td><i>enable</i></td> <td>Add HTTP header indicating SSL offload for WebSphere server.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.											
Option	Description																	
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.																	
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.																	
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>half</i></td> <td>Client to FortiGate SSL.</td> </tr> <tr> <td><i>full</i></td> <td>Client to FortiGate and FortiGate to Server SSL.</td> </tr> </tbody> </table>	Option	Description	<i>half</i>	Client to FortiGate SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.											
Option	Description																	
<i>half</i>	Client to FortiGate SSL.																	
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.																	
ssl-certificate	The name of the SSL certificate to use for SSL acceleration.	string	Maximum length: 35															
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>768</i></td> <td>768-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1024</i></td> <td>1024-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1536</i></td> <td>1536-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>2048</i></td> <td>2048-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>3072</i></td> <td>3072-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>4096</i></td> <td>4096-bit Diffie-Hellman prime.</td> </tr> </tbody> </table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
Option	Description																	
<i>768</i>	768-bit Diffie-Hellman prime.																	
<i>1024</i>	1024-bit Diffie-Hellman prime.																	
<i>1536</i>	1536-bit Diffie-Hellman prime.																	
<i>2048</i>	2048-bit Diffie-Hellman prime.																	
<i>3072</i>	3072-bit Diffie-Hellman prime.																	
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High encryption. Allow only AES and ChaCha.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td> </tr> <tr> <td><i>custom</i></td> <td>Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	<i>custom</i>	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.							
Option	Description																	
<i>high</i>	High encryption. Allow only AES and ChaCha.																	
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																	
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
<i>custom</i>	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.																	

Parameter	Description	Type	Size	Default												
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High encryption. Allow only AES and ChaCha.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td> </tr> <tr> <td><i>custom</i></td> <td>Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.</td> </tr> <tr> <td><i>client</i></td> <td>Use the same encryption algorithms for both client and server sessions.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	<i>custom</i>	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for both client and server sessions.			
Option	Description															
<i>high</i>	High encryption. Allow only AES and ChaCha.															
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.															
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.															
<i>custom</i>	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.															
<i>client</i>	Use the same encryption algorithms for both client and server sessions.															
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>require</i></td> <td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td> </tr> <tr> <td><i>deny</i></td> <td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td> </tr> </tbody> </table>	Option	Description	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.							
Option	Description															
<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.															
<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.															
<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.															
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.									
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.									
Option	Description																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> <tr> <td><i>client</i></td> <td>Use same value as client configuration.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
<i>client</i>	Use same value as client configuration.																	
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> <tr> <td><i>client</i></td> <td>Use same value as client configuration.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
<i>client</i>	Use same value as client configuration.																	
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send empty fragments.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not send empty fragments.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.											
Option	Description																	
<i>enable</i>	Send empty fragments.																	
<i>disable</i>	Do not send empty fragments.																	

Parameter	Description	Type	Size	Default										
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
Option	Description													
<i>disable</i>	Disable.													
<i>enable</i>	Enable.													
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow a SSL client to renegotiate.</td> </tr> <tr> <td><i>deny</i></td> <td>Abort any client initiated SSL re-negotiation attempt.</td> </tr> <tr> <td><i>secure</i></td> <td>Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.	<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.					
Option	Description													
<i>allow</i>	Allow a SSL client to renegotiate.													
<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.													
<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.													
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not keep session states.</td> </tr> <tr> <td><i>time</i></td> <td>Expire session states after this many minutes.</td> </tr> <tr> <td><i>count</i></td> <td>Expire session states when this maximum is reached.</td> </tr> <tr> <td><i>both</i></td> <td>Expire session states based on time or count, whichever occurs first.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.			
Option	Description													
<i>disable</i>	Do not keep session states.													
<i>time</i>	Expire session states after this many minutes.													
<i>count</i>	Expire session states when this maximum is reached.													
<i>both</i>	Expire session states based on time or count, whichever occurs first.													
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30										
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000										
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576	0										

Parameter	Description	Type	Size	Default										
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not keep session states.</td> </tr> <tr> <td><i>time</i></td> <td>Expire session states after this many minutes.</td> </tr> <tr> <td><i>count</i></td> <td>Expire session states when this maximum is reached.</td> </tr> <tr> <td><i>both</i></td> <td>Expire session states based on time or count, whichever occurs first.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.			
Option	Description													
<i>disable</i>	Do not keep session states.													
<i>time</i>	Expire session states after this many minutes.													
<i>count</i>	Expire session states when this maximum is reached.													
<i>both</i>	Expire session states based on time or count, whichever occurs first.													
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60										
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100										
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HTTP location conversion.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HTTP location conversion.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HTTP location conversion.	<i>disable</i>	Disable HTTP location conversion.							
Option	Description													
<i>enable</i>	Enable HTTP location conversion.													
<i>disable</i>	Disable HTTP location conversion.													
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Match HTTP host in response header.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not match HTTP host.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Match HTTP host in response header.	<i>disable</i>	Do not match HTTP host.							
Option	Description													
<i>enable</i>	Match HTTP host in response header.													
<i>disable</i>	Do not match HTTP host.													
ssl-hpkp	Enable/disable including HPKP header in response.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add a HPKP header to each HTTP response.</td> </tr> <tr> <td><i>enable</i></td> <td>Add a HPKP header to each a HTTP response.</td> </tr> <tr> <td><i>report-only</i></td> <td>Add a HPKP Report-Only header to each HTTP response.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add a HPKP header to each HTTP response.	<i>enable</i>	Add a HPKP header to each a HTTP response.	<i>report-only</i>	Add a HPKP Report-Only header to each HTTP response.					
Option	Description													
<i>disable</i>	Do not add a HPKP header to each HTTP response.													
<i>enable</i>	Add a HPKP header to each a HTTP response.													
<i>report-only</i>	Add a HPKP Report-Only header to each HTTP response.													

Parameter	Description	Type	Size	Default
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79	
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79	
ssl-hpkp-age	Number of seconds the client should honour the HPKP setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255	
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable
		<b>Option</b>	<b>Description</b>	
		<i>disable</i>	HPKP header does not apply to subdomains.	
		<i>enable</i>	HPKP header applies to subdomains.	
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable
		<b>Option</b>	<b>Description</b>	
		<i>disable</i>	Do not add a HSTS header to each a HTTP response.	
		<i>enable</i>	Add a HSTS header to each HTTP response.	
ssl-hsts-age	Number of seconds the client should honour the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable
		<b>Option</b>	<b>Description</b>	
		<i>disable</i>	HSTS header does not apply to subdomains.	
		<i>enable</i>	HSTS header applies to subdomains.	
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

## config realservers

Parameter	Description	Type	Size	Default								
type	Type of address.	option	-	ip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ip</i></td> <td>Standard IPv4 address.</td> </tr> <tr> <td><i>address</i></td> <td>Dynamic address object.</td> </tr> </tbody> </table>	Option	Description	<i>ip</i>	Standard IPv4 address.	<i>address</i>	Dynamic address object.					
Option	Description											
<i>ip</i>	Standard IPv4 address.											
<i>address</i>	Dynamic address object.											
address	Dynamic address of the real server.	string	Maximum length: 79									
ip	IP address of the real server.	ipv4-address-any	Not Specified	0.0.0.0								
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535	0								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>active</i></td> <td>Server status active.</td> </tr> <tr> <td><i>standby</i></td> <td>Server status standby.</td> </tr> <tr> <td><i>disable</i></td> <td>Server status disable.</td> </tr> </tbody> </table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
Option	Description											
<i>active</i>	Server status active.											
<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								

Parameter	Description	Type	Size	Default								
holddown-interval	Time in seconds that the health check monitor continues to monitor and unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable per server health check.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable per server health check.</td> </tr> <tr> <td><i>vip</i></td> <td>Use health check defined in VIP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.			
Option	Description											
<i>disable</i>	Disable per server health check.											
<i>enable</i>	Enable per server health check.											
<i>vip</i>	Use health check defined in VIP.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
max-connections	Max number of active connections that can be directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0								
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79									
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified									

### config ssl-cipher-suites

Parameter	Description	Type	Size	Default								
cipher	Cipher suite name.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-AES-128-GCM-SHA256</i></td> <td>Cipher suite TLS-AES-128-GCM-SHA256.</td> </tr> <tr> <td><i>TLS-AES-256-GCM-SHA384</i></td> <td>Cipher suite TLS-AES-256-GCM-SHA384.</td> </tr> <tr> <td><i>TLS-CHACHA20-POLY1305-SHA256</i></td> <td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.			
Option	Description											
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.											
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.											
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.											



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i></td> <td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.</td> </tr> <tr> <td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i></td> <td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.</td> </tr> <tr> <td><i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i></td> <td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.</td> </tr> <tr> <td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i></td> <td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.</td> </tr> <tr> <td><i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i></td> <td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.</td> </tr> <tr> <td><i>TLS-RSA-WITH-AES-128-CBC-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.</td> </tr> <tr> <td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td> </tr> <tr> <td><i>TLS-RSA-WITH-AES-128-CBC-SHA256</i></td> <td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td> </tr> <tr> <td><i>TLS-RSA-WITH-AES-128-GCM-SHA256</i></td> <td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td> </tr> <tr> <td><i>TLS-RSA-WITH-AES-256-CBC-SHA256</i></td> <td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td> </tr> <tr> <td><i>TLS-RSA-WITH-AES-256-GCM-SHA384</i></td> <td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.			
Option	Description																											
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.																											
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.																											
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																											
<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																											
<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td> </tr> <tr> <td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.									
Option	Description															
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.															
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.															
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															

### config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default										
cipher	Cipher suite name.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-AES-128-GCM-SHA256</i></td> <td>Cipher suite TLS-AES-128-GCM-SHA256.</td> </tr> <tr> <td><i>TLS-AES-256-GCM-SHA384</i></td> <td>Cipher suite TLS-AES-256-GCM-SHA384.</td> </tr> <tr> <td><i>TLS-CHACHA20-POLY1305-SHA256</i></td> <td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td> </tr> <tr> <td><i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td> <td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.			
Option	Description													
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.													
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.													
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.													
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.		
	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		

Parameter	Description	Type	Size	Default												
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															

## config firewall vip46

Configure IPv4 to IPv6 virtual IPs.

```

config firewall vip46
  Description: Configure IPv4 to IPv6 virtual IPs.
  edit <name>
    set id {integer}
    set uuid {uuid}
    set srcintf-filter <interface-name1>, <interface-name2>, ...
    set comment {var-string}
    set type [static-nat|server-load-balance]
    set src-filter <range1>, <range2>, ...
    set extip {user}
    set mappedip {user}
    set arp-reply [disable|enable]
    set portforward [disable|enable]
    set protocol [tcp|udp]
    set extport {user}
    set mappedport {user}
    set color {integer}
    set ldb-method [static|round-robin|...]
    set server-type [http|tcp|...]
  config realservers
    Description: Real servers.
    edit <id>
      set ip {ipv6-address}
      set port {integer}
      set status [active|standby|...]
      set weight {integer}
      set holddown-interval {integer}
      set healthcheck [disable|enable|...]
      set max-connections {integer}
      set monitor <name1>, <name2>, ...
      set client-ip {user}
    next
  end

```

```

    set monitor <name1>, <name2>, ...
  next
end

```

## config firewall vip46

Parameter	Description	Type	Size	Default						
id	Custom defined id.	integer	Minimum value: 0 Maximum value: 65535	0						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
srcintf-filter <interface-name>	Interfaces to which the VIP46 applies. Separate the names with spaces. Interface name.	string	Maximum length: 79							
comment	Comment.	var-string	Maximum length: 255							
type	VIP type: static NAT or server load balance.	option	-	static-nat						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static-nat</i></td> <td>Static NAT.</td> </tr> <tr> <td><i>server-load-balance</i></td> <td>Server load balance.</td> </tr> </tbody> </table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.			
Option	Description									
<i>static-nat</i>	Static NAT.									
<i>server-load-balance</i>	Server load balance.									
src-filter <range>	Source IP filter (x.x.x.x/x). Src-filter range.	string	Maximum length: 79							
extip	Start-external-IP [-end-external-IP].	user	Not Specified							
mappedip	Start-mapped-IPv6-address [-end mapped-IPv6-address].	user	Not Specified							
arp-reply	Enable ARP reply.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable ARP reply.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable ARP reply.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.			
Option	Description									
<i>disable</i>	Disable ARP reply.									
<i>enable</i>	Enable ARP reply.									
portforward	Enable port forwarding.	option	-	disable						

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable port forwarding.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable port forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable port forwarding.	<i>enable</i>	Enable port forwarding.											
Option	Description																	
<i>disable</i>	Disable port forwarding.																	
<i>enable</i>	Enable port forwarding.																	
protocol	Mapped port protocol.	option	-	tcp														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp</i></td> <td>TCP.</td> </tr> <tr> <td><i>udp</i></td> <td>UDP.</td> </tr> </tbody> </table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.											
Option	Description																	
<i>tcp</i>	TCP.																	
<i>udp</i>	UDP.																	
extport	External service port.	user	Not Specified															
mappedport	Mapped service port.	user	Not Specified															
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0														
ldb-method	Load balance method.	option	-	static														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Distribute sessions based on source IP.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Distribute sessions based round robin order.</td> </tr> <tr> <td><i>weighted</i></td> <td>Distribute sessions based on weight.</td> </tr> <tr> <td><i>least-session</i></td> <td>Distribute sessions to the server with the lowest session count.</td> </tr> <tr> <td><i>least-rtt</i></td> <td>Distribute sessions to the server with the lowest Round-Trip-Time.</td> </tr> <tr> <td><i>first-alive</i></td> <td>Distribute sessions to the first server that is alive.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Distribute sessions based on source IP.	<i>round-robin</i>	Distribute sessions based round robin order.	<i>weighted</i>	Distribute sessions based on weight.	<i>least-session</i>	Distribute sessions to the server with the lowest session count.	<i>least-rtt</i>	Distribute sessions to the server with the lowest Round-Trip-Time.	<i>first-alive</i>	Distribute sessions to the first server that is alive.			
Option	Description																	
<i>static</i>	Distribute sessions based on source IP.																	
<i>round-robin</i>	Distribute sessions based round robin order.																	
<i>weighted</i>	Distribute sessions based on weight.																	
<i>least-session</i>	Distribute sessions to the server with the lowest session count.																	
<i>least-rtt</i>	Distribute sessions to the server with the lowest Round-Trip-Time.																	
<i>first-alive</i>	Distribute sessions to the first server that is alive.																	
server-type	Server type.	option	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>tcp</i></td> <td>TCP</td> </tr> <tr> <td><i>udp</i></td> <td>UDP</td> </tr> <tr> <td><i>ip</i></td> <td>IP</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP	<i>tcp</i>	TCP	<i>udp</i>	UDP	<i>ip</i>	IP							
Option	Description																	
<i>http</i>	HTTP																	
<i>tcp</i>	TCP																	
<i>udp</i>	UDP																	
<i>ip</i>	IP																	
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79															



## config realservers

Parameter	Description	Type	Size	Default								
ip	Mapped server IPv6.	ipv6-address	Not Specified	::								
port	Mapped server port.	integer	Minimum value: 1 Maximum value: 65535	0								
status	Server administrative status.	option	-	active								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>active</i></td> <td>Server status active.</td> </tr> <tr> <td><i>standby</i></td> <td>Server status standby.</td> </tr> <tr> <td><i>disable</i></td> <td>Server status disable.</td> </tr> </tbody> </table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
Option	Description											
<i>active</i>	Server status active.											
<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.											
weight	weight	integer	Minimum value: 1 Maximum value: 255	1								
holddown-interval	Hold down interval.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Per server health check.	option	-	vip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable per server health check.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable per server health check.</td> </tr> <tr> <td><i>vip</i></td> <td>Use health check defined in VIP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.			
Option	Description											
<i>disable</i>	Disable per server health check.											
<i>enable</i>	Enable per server health check.											
<i>vip</i>	Use health check defined in VIP.											
max-connections	Maximum number of connections allowed to server.	integer	Minimum value: 0 Maximum value: 2147483647	0								
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79									
client-ip	Restrict server to a client IP in this range.	user	Not Specified									

---

## config firewall vip6

Configure virtual IP for IPv6.

```
config firewall vip6
  Description: Configure virtual IP for IPv6.
  edit <name>
    set id {integer}
    set uuid {uuid}
    set comment {var-string}
    set type [static-nat|server-load-balance]
    set src-filter <range1>, <range2>, ...
    set extip {user}
    set mappedip {user}
    set nat-source-vip [disable|enable]
    set arp-reply [disable|enable]
    set portforward [disable|enable]
    set protocol [tcp|udp|...]
    set extport {user}
    set mappedport {user}
    set color {integer}
    set ldb-method [static|round-robin|...]
    set server-type [http|https|...]
    set http-redirect [enable|disable]
    set persistence [none|http-cookie|...]
  config realservers
    Description: Select the real servers that this server load balancing VIP will
      distribute traffic to.
    edit <id>
      set ip {ipv6-address}
      set port {integer}
      set status [active|standby|...]
      set weight {integer}
      set holddown-interval {integer}
      set healthcheck [disable|enable|...]
      set http-host {string}
      set max-connections {integer}
      set monitor <name1>, <name2>, ...
      set client-ip {user}
    next
  end
  set http-cookie-domain-from-host [disable|enable]
  set http-cookie-domain {string}
  set http-cookie-path {string}
  set http-cookie-generation {integer}
  set http-cookie-age {integer}
  set http-cookie-share [disable|same-ip]
  set https-cookie-secure [disable|enable]
  set http-multiplex [enable|disable]
  set http-ip-header [enable|disable]
  set http-ip-header-name {string}
  set outlook-web-access [disable|enable]
  set weblogic-server [disable|enable]
  set websphere-server [disable|enable]
  set ssl-mode [half|full]
  set ssl-certificate {string}
  set ssl-dh-bits [768|1024|...]
```

```

set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
  Description: SSL/TLS cipher suites acceptable from a client, ordered by priority.
  edit <priority>
    set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
    set versions {option1}, {option2}, ...
  next
end
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
  Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
  edit <priority>
    set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
    set versions {option1}, {option2}, ...
  next
end
set ssl-pfs [require|deny|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-send-empty-frags [enable|disable]
set ssl-client-fallback [disable|enable]
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-type [disable|time|...]
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-max {integer}
set ssl-client-rekey-count {integer}
set ssl-server-session-state-type [disable|time|...]
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-max {integer}
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-hpkp [disable|enable|...]
set ssl-hpkp-primary {string}
set ssl-hpkp-backup {string}
set ssl-hpkp-age {integer}
set ssl-hpkp-report-uri {var-string}
set ssl-hpkp-include-subdomains [disable|enable]
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set monitor <name1>, <name2>, ...
set max-embryonic-connections {integer}
next
end

```

## config firewall vip6

Parameter	Description	Type	Size	Default						
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
comment	Comment.	var-string	Maximum length: 255							
type	Configure a static NAT or server load balance VIP.	option	-	static-nat						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static-nat</i></td> <td>Static NAT.</td> </tr> <tr> <td><i>server-load-balance</i></td> <td>Server load balance.</td> </tr> </tbody> </table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.			
Option	Description									
<i>static-nat</i>	Static NAT.									
<i>server-load-balance</i>	Server load balance.									
src-filter <range>	Source IPv6 filter (x:x:x:x:x:x/x). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79							
extip	IPv6 address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified							
mappedip	Mapped IPv6 address range in the format startIP-endIP.	user	Not Specified							
nat-source-vip	Enable to perform SNAT on traffic from mappedip to the extip for all egress interfaces.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable nat-source-vip.</td> </tr> <tr> <td><i>enable</i></td> <td>Perform SNAT on traffic from mappedip to the extip for all egress interfaces.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable nat-source-vip.	<i>enable</i>	Perform SNAT on traffic from mappedip to the extip for all egress interfaces.			
Option	Description									
<i>disable</i>	Disable nat-source-vip.									
<i>enable</i>	Perform SNAT on traffic from mappedip to the extip for all egress interfaces.									
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable ARP reply.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable ARP reply.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.			
Option	Description									
<i>disable</i>	Disable ARP reply.									
<i>enable</i>	Enable ARP reply.									

Parameter	Description	Type	Size	Default																
portforward	Enable port forwarding.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable port forward.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable/disable port forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable/disable port forwarding.													
Option	Description																			
<i>disable</i>	Disable port forward.																			
<i>enable</i>	Enable/disable port forwarding.																			
protocol	Protocol to use when forwarding packets.	option	-	tcp																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp</i></td> <td>TCP.</td> </tr> <tr> <td><i>udp</i></td> <td>UDP.</td> </tr> <tr> <td><i>sctp</i></td> <td>SCTP.</td> </tr> </tbody> </table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.											
Option	Description																			
<i>tcp</i>	TCP.																			
<i>udp</i>	UDP.																			
<i>sctp</i>	SCTP.																			
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified																	
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified																	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0																
ldb-method	Method used to distribute sessions to real servers.	option	-	static																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Distribute sessions based on source IP.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Distribute sessions based round robin order.</td> </tr> <tr> <td><i>weighted</i></td> <td>Distribute sessions based on weight.</td> </tr> <tr> <td><i>least-session</i></td> <td>Sends new sessions to the server with the lowest session count.</td> </tr> <tr> <td><i>least-rtt</i></td> <td>Distribute new sessions to the server with lowest Round-Trip-Time.</td> </tr> <tr> <td><i>first-alive</i></td> <td>Distribute sessions to the first server that is alive.</td> </tr> <tr> <td><i>http-host</i></td> <td>Distribute sessions to servers based on host field in HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Distribute sessions based on source IP.	<i>round-robin</i>	Distribute sessions based round robin order.	<i>weighted</i>	Distribute sessions based on weight.	<i>least-session</i>	Sends new sessions to the server with the lowest session count.	<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.	<i>first-alive</i>	Distribute sessions to the first server that is alive.	<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.			
Option	Description																			
<i>static</i>	Distribute sessions based on source IP.																			
<i>round-robin</i>	Distribute sessions based round robin order.																			
<i>weighted</i>	Distribute sessions based on weight.																			
<i>least-session</i>	Sends new sessions to the server with the lowest session count.																			
<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.																			
<i>first-alive</i>	Distribute sessions to the first server that is alive.																			
<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.																			
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-																	

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS</td> </tr> <tr> <td><i>imaps</i></td> <td>IMAPS</td> </tr> <tr> <td><i>pop3s</i></td> <td>POP3S</td> </tr> <tr> <td><i>smtps</i></td> <td>SMTPS</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL</td> </tr> <tr> <td><i>tcp</i></td> <td>TCP</td> </tr> <tr> <td><i>udp</i></td> <td>UDP</td> </tr> <tr> <td><i>ip</i></td> <td>IP</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP	<i>https</i>	HTTPS	<i>imaps</i>	IMAPS	<i>pop3s</i>	POP3S	<i>smtps</i>	SMTPS	<i>ssl</i>	SSL	<i>tcp</i>	TCP	<i>udp</i>	UDP	<i>ip</i>	IP			
Option	Description																							
<i>http</i>	HTTP																							
<i>https</i>	HTTPS																							
<i>imaps</i>	IMAPS																							
<i>pop3s</i>	POP3S																							
<i>smtps</i>	SMTPS																							
<i>ssl</i>	SSL																							
<i>tcp</i>	TCP																							
<i>udp</i>	UDP																							
<i>ip</i>	IP																							
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redirection of HTTP to HTTPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redirection of HTTP to HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.																	
Option	Description																							
<i>enable</i>	Enable redirection of HTTP to HTTPS.																							
<i>disable</i>	Disable redirection of HTTP to HTTPS.																							
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>http-cookie</i></td> <td>HTTP cookie.</td> </tr> <tr> <td><i>ssl-session-id</i></td> <td>SSL session ID.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.	<i>ssl-session-id</i>	SSL session ID.															
Option	Description																							
<i>none</i>	None.																							
<i>http-cookie</i>	HTTP cookie.																							
<i>ssl-session-id</i>	SSL session ID.																							
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of HTTP cookie domain from host field in HTTP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.																	
Option	Description																							
<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).																							
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.																							
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35																					

Parameter	Description	Type	Size	Default						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-share	Control sharing of cookies across virtual servers. same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Only allow HTTP cookie to match this virtual server.</td> </tr> <tr> <td><i>same-ip</i></td> <td>Allow HTTP cookie to match any virtual server with same IP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Only allow HTTP cookie to match this virtual server.	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.			
Option	Description									
<i>disable</i>	Only allow HTTP cookie to match this virtual server.									
<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td> </tr> <tr> <td><i>enable</i></td> <td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.			
Option	Description									
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.									
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HTTP session multiplexing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HTTP session multiplexing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HTTP session multiplexing.	<i>disable</i>	Disable HTTP session multiplexing.			
Option	Description									
<i>enable</i>	Enable HTTP session multiplexing.									
<i>disable</i>	Disable HTTP session multiplexing.									
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding HTTP header.					
Option	Description									
<i>enable</i>	Enable adding HTTP header.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable adding HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable adding HTTP header.					
Option	Description									
<i>disable</i>	Disable adding HTTP header.									
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35							
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Outlook Web Access support.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Outlook Web Access support.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Outlook Web Access support.	<i>enable</i>	Enable Outlook Web Access support.			
Option	Description									
<i>disable</i>	Disable Outlook Web Access support.									
<i>enable</i>	Enable Outlook Web Access support.									
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add HTTP header indicating SSL offload for WebLogic server.</td> </tr> <tr> <td><i>enable</i></td> <td>Add HTTP header indicating SSL offload for WebLogic server.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.			
Option	Description									
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.									
<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.									
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add HTTP header indicating SSL offload for WebSphere server.</td> </tr> <tr> <td><i>enable</i></td> <td>Add HTTP header indicating SSL offload for WebSphere server.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.			
Option	Description									
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.									
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.									
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>half</i></td> <td>Client to FortiGate SSL.</td> </tr> <tr> <td><i>full</i></td> <td>Client to FortiGate and FortiGate to Server SSL.</td> </tr> </tbody> </table>	Option	Description	<i>half</i>	Client to FortiGate SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.			
Option	Description									
<i>half</i>	Client to FortiGate SSL.									
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.									
ssl-certificate	The name of the SSL certificate to use for SSL acceleration.	string	Maximum length: 35							
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048						



Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>768</i></td> <td>768-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1024</i></td> <td>1024-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1536</i></td> <td>1536-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>2048</i></td> <td>2048-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>3072</i></td> <td>3072-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>4096</i></td> <td>4096-bit Diffie-Hellman prime.</td> </tr> </tbody> </table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
Option	Description																	
<i>768</i>	768-bit Diffie-Hellman prime.																	
<i>1024</i>	1024-bit Diffie-Hellman prime.																	
<i>1536</i>	1536-bit Diffie-Hellman prime.																	
<i>2048</i>	2048-bit Diffie-Hellman prime.																	
<i>3072</i>	3072-bit Diffie-Hellman prime.																	
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>Use AES or 3DES.</td> </tr> <tr> <td><i>medium</i></td> <td>Use AES, 3DES, or RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Use AES, 3DES, RC4, or DES.</td> </tr> <tr> <td><i>custom</i></td> <td>Use config ssl-cipher-suites to select the cipher suites that are allowed.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	Use AES or 3DES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.							
Option	Description																	
<i>high</i>	Use AES or 3DES.																	
<i>medium</i>	Use AES, 3DES, or RC4.																	
<i>low</i>	Use AES, 3DES, RC4, or DES.																	
<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.																	
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>Use AES or 3DES.</td> </tr> <tr> <td><i>medium</i></td> <td>Use AES, 3DES, or RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Use AES, 3DES, RC4, or DES.</td> </tr> <tr> <td><i>custom</i></td> <td>Use config ssl-server-cipher-suites to select the cipher suites that are allowed.</td> </tr> <tr> <td><i>client</i></td> <td>Use the same encryption algorithms for client and server sessions.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	Use AES or 3DES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for client and server sessions.					
Option	Description																	
<i>high</i>	Use AES or 3DES.																	
<i>medium</i>	Use AES, 3DES, or RC4.																	
<i>low</i>	Use AES, 3DES, RC4, or DES.																	
<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.																	
<i>client</i>	Use the same encryption algorithms for client and server sessions.																	
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>require</i></td> <td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td> </tr> <tr> <td><i>deny</i></td> <td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td> </tr> </tbody> </table>	Option	Description	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.											
Option	Description																	
<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.																	
<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.																	

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.													
Option	Description																	
<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.					
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.					
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> <tr> <td><i>client</i></td> <td>Use same value as client configuration.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
<i>client</i>	Use same value as client configuration.																	
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> <tr> <td><i>client</i></td> <td>Use same value as client configuration.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
<i>client</i>	Use same value as client configuration.																	
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send empty fragments.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not send empty fragments.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.											
Option	Description																	
<i>enable</i>	Send empty fragments.																	
<i>disable</i>	Do not send empty fragments.																	
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.											
Option	Description																	
<i>disable</i>	Disable.																	
<i>enable</i>	Enable.																	
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow a SSL client to renegotiate.</td> </tr> <tr> <td><i>deny</i></td> <td>Abort any SSL connection that attempts to renegotiate.</td> </tr> <tr> <td><i>secure</i></td> <td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.									
Option	Description																	
<i>allow</i>	Allow a SSL client to renegotiate.																	
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.																	
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.																	
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both														

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not keep session states.</td> </tr> <tr> <td><i>time</i></td> <td>Expire session states after this many minutes.</td> </tr> <tr> <td><i>count</i></td> <td>Expire session states when this maximum is reached.</td> </tr> <tr> <td><i>both</i></td> <td>Expire session states based on time or count, whichever occurs first.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.			
Option	Description													
<i>disable</i>	Do not keep session states.													
<i>time</i>	Expire session states after this many minutes.													
<i>count</i>	Expire session states when this maximum is reached.													
<i>both</i>	Expire session states based on time or count, whichever occurs first.													
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30										
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000										
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576	0										
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not keep session states.</td> </tr> <tr> <td><i>time</i></td> <td>Expire session states after this many minutes.</td> </tr> <tr> <td><i>count</i></td> <td>Expire session states when this maximum is reached.</td> </tr> <tr> <td><i>both</i></td> <td>Expire session states based on time or count, whichever occurs first.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.			
Option	Description													
<i>disable</i>	Do not keep session states.													
<i>time</i>	Expire session states after this many minutes.													
<i>count</i>	Expire session states when this maximum is reached.													
<i>both</i>	Expire session states based on time or count, whichever occurs first.													
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60										
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100										

Parameter	Description	Type	Size	Default
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable HTTP location conversion.		
	<i>disable</i>	Disable HTTP location conversion.		
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Match HTTP host in response header.		
	<i>disable</i>	Do not match HTTP host.		
ssl-hpkp	Enable/disable including HPKP header in response.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not add a HPKP header to each HTTP response.		
	<i>enable</i>	Add a HPKP header to each a HTTP response.		
	<i>report-only</i>	Add a HPKP Report-Only header to each HTTP response.		
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79	
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79	
ssl-hpkp-age	Number of minutes the web browser should keep HPKP.	integer	Minimum value: 60 Maximum value: 157680000	5184000
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255	
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	HPKP header does not apply to subdomains.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>HPKP header applies to subdomains.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	HPKP header applies to subdomains.					
Option	Description									
<i>enable</i>	HPKP header applies to subdomains.									
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add a HSTS header to each a HTTP response.</td> </tr> <tr> <td><i>enable</i></td> <td>Add a HSTS header to each HTTP response.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add a HSTS header to each a HTTP response.	<i>enable</i>	Add a HSTS header to each HTTP response.			
Option	Description									
<i>disable</i>	Do not add a HSTS header to each a HTTP response.									
<i>enable</i>	Add a HSTS header to each HTTP response.									
ssl-hsts-age	Number of seconds the client should honour the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>HSTS header does not apply to subdomains.</td> </tr> <tr> <td><i>enable</i></td> <td>HSTS header applies to subdomains.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	HSTS header does not apply to subdomains.	<i>enable</i>	HSTS header applies to subdomains.			
Option	Description									
<i>disable</i>	HSTS header does not apply to subdomains.									
<i>enable</i>	HSTS header applies to subdomains.									
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79							
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000						

## config realservers

Parameter	Description	Type	Size	Default
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535	0

Parameter	Description	Type	Size	Default								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>active</i></td> <td>Server status active.</td> </tr> <tr> <td><i>standby</i></td> <td>Server status standby.</td> </tr> <tr> <td><i>disable</i></td> <td>Server status disable.</td> </tr> </tbody> </table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
Option	Description											
<i>active</i>	Server status active.											
<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
holddown-interval	Time in seconds that the health check monitor continues to monitor an unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable per server health check.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable per server health check.</td> </tr> <tr> <td><i>vip</i></td> <td>Use health check defined in VIP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.			
Option	Description											
<i>disable</i>	Disable per server health check.											
<i>enable</i>	Enable per server health check.											
<i>vip</i>	Use health check defined in VIP.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
max-connections	Max number of active connections that can directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0								
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79									
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified									

## config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.		
	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.		
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-RSA-WITH-RC4-128-MD5</i></td> <td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td> </tr> <tr> <td><i>TLS-RSA-WITH-RC4-128-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td> </tr> <tr> <td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td> </tr> <tr> <td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td> </tr> <tr> <td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
Option	Description															
<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.															
<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.															
<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.															
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.															
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.															
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															

### config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default						
cipher	Cipher suite name.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-AES-128-GCM-SHA256</i></td> <td>Cipher suite TLS-AES-128-GCM-SHA256.</td> </tr> <tr> <td><i>TLS-AES-256-GCM-SHA384</i></td> <td>Cipher suite TLS-AES-256-GCM-SHA384.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.			
Option	Description									
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.									
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-RSA-WITH-RC4-128-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td> </tr> <tr> <td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td> </tr> <tr> <td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td> </tr> <tr> <td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td> <td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.					
Option	Description															
<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.															
<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.															
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.															
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.															
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															

## config firewall vip64

Configure IPv6 to IPv4 virtual IPs.

```
config firewall vip64
  Description: Configure IPv6 to IPv4 virtual IPs.
  edit <name>
    set id {integer}
    set uuid {uuid}
    set comment {var-string}
    set type [static-nat|server-load-balance]
    set src-filter <range1>, <range2>, ...
    set extip {user}
    set mappedip {user}
    set arp-reply [disable|enable]
    set portforward [disable|enable]
    set protocol [tcp|udp]
    set extport {user}
    set mappedport {user}
    set color {integer}
```

```

set ldb-method [static|round-robin|...]
set server-type [http|tcp|...]
config realservers
  Description: Real servers.
  edit <id>
    set ip {ipv4-address-any}
    set port {integer}
    set status [active|standby|...]
    set weight {integer}
    set holddown-interval {integer}
    set healthcheck [disable|enable|...]
    set max-connections {integer}
    set monitor <name1>, <name2>, ...
    set client-ip {user}
  next
end
set monitor <name1>, <name2>, ...
next
end

```

## config firewall vip64

Parameter	Description	Type	Size	Default						
id	Custom defined id.	integer	Minimum value: 0 Maximum value: 65535	0						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
comment	Comment.	var-string	Maximum length: 255							
type	VIP type: static NAT or server load balance.	option	-	static-nat						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static-nat</i></td> <td>Static NAT.</td> </tr> <tr> <td><i>server-load-balance</i></td> <td>Server load balance.</td> </tr> </tbody> </table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.			
Option	Description									
<i>static-nat</i>	Static NAT.									
<i>server-load-balance</i>	Server load balance.									
src-filter <range>	Source IP6 filter (x:x:x:x:x:x/x). Src-filter range.	string	Maximum length: 79							
extip	Start-external-IPv6-address [-end-external-IPv6-address].	user	Not Specified							
mappedip	Start-mapped-IP [-end-mapped-IP].	user	Not Specified							

Parameter	Description	Type	Size	Default														
arp-reply	Enable ARP reply.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable arp reply.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable arp reply.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable arp reply.	<i>enable</i>	Enable arp reply.											
Option	Description																	
<i>disable</i>	Disable arp reply.																	
<i>enable</i>	Enable arp reply.																	
portforward	Enable port forwarding.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable port forwarding.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable port forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable port forwarding.	<i>enable</i>	Enable port forwarding.											
Option	Description																	
<i>disable</i>	Disable port forwarding.																	
<i>enable</i>	Enable port forwarding.																	
protocol	Mapped port protocol.	option	-	tcp														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp</i></td> <td>TCP.</td> </tr> <tr> <td><i>udp</i></td> <td>UDP.</td> </tr> </tbody> </table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.											
Option	Description																	
<i>tcp</i>	TCP.																	
<i>udp</i>	UDP.																	
extport	External service port.	user	Not Specified															
mappedport	Mapped service port.	user	Not Specified															
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0														
ldb-method	Load balance method.	option	-	static														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Distribute sessions based on source IP.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Distribute sessions based round robin order.</td> </tr> <tr> <td><i>weighted</i></td> <td>Distribute sessions based on weight.</td> </tr> <tr> <td><i>least-session</i></td> <td>Distribute sessions to the server with the lowest session count.</td> </tr> <tr> <td><i>least-rtt</i></td> <td>Distribute sessions to the server with the lowest Round-Trip-Time.</td> </tr> <tr> <td><i>first-alive</i></td> <td>Distribute sessions to the first server that is alive.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Distribute sessions based on source IP.	<i>round-robin</i>	Distribute sessions based round robin order.	<i>weighted</i>	Distribute sessions based on weight.	<i>least-session</i>	Distribute sessions to the server with the lowest session count.	<i>least-rtt</i>	Distribute sessions to the server with the lowest Round-Trip-Time.	<i>first-alive</i>	Distribute sessions to the first server that is alive.			
Option	Description																	
<i>static</i>	Distribute sessions based on source IP.																	
<i>round-robin</i>	Distribute sessions based round robin order.																	
<i>weighted</i>	Distribute sessions based on weight.																	
<i>least-session</i>	Distribute sessions to the server with the lowest session count.																	
<i>least-rtt</i>	Distribute sessions to the server with the lowest Round-Trip-Time.																	
<i>first-alive</i>	Distribute sessions to the first server that is alive.																	
server-type	Server type.	option	-															

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>tcp</i></td> <td>TCP</td> </tr> <tr> <td><i>udp</i></td> <td>UDP</td> </tr> <tr> <td><i>ip</i></td> <td>IP</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP	<i>tcp</i>	TCP	<i>udp</i>	UDP	<i>ip</i>	IP			
Option	Description													
<i>http</i>	HTTP													
<i>tcp</i>	TCP													
<i>udp</i>	UDP													
<i>ip</i>	IP													
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79											

### config realservers

Parameter	Description	Type	Size	Default								
ip	Mapped server IP.	ipv4- address- any	Not Specified	0.0.0.0								
port	Mapped server port.	integer	Minimum value: 1 Maximum value: 65535	0								
status	Server administrative status.	option	-	active								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>active</i></td> <td>Server status active.</td> </tr> <tr> <td><i>standby</i></td> <td>Server status standby.</td> </tr> <tr> <td><i>disable</i></td> <td>Server status disable.</td> </tr> </tbody> </table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
Option	Description											
<i>active</i>	Server status active.											
<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.											
weight	weight	integer	Minimum value: 1 Maximum value: 255	1								
holddown- interval	Hold down interval.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Per server health check.	option	-	vip								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable per server health check.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable per server health check.							
Option	Description											
<i>disable</i>	Disable per server health check.											



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable per server health check.</td> </tr> <tr> <td><i>vip</i></td> <td>Use health check defined in VIP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.			
Option	Description									
<i>enable</i>	Enable per server health check.									
<i>vip</i>	Use health check defined in VIP.									
max-connections	Maximum number of connections allowed to server.	integer	Minimum value: 0 Maximum value: 2147483647	0						
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79							
client-ip	Restrict server to a client IP in this range.	user	Not Specified							

## config firewall vipgrp

Configure IPv4 virtual IP groups.

```
config firewall vipgrp
  Description: Configure IPv4 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set interface {string}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
  next
end
```

## config firewall vipgrp

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
interface	interface	string	Maximum length: 35	
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79	

## config firewall vipgrp46

Configure IPv4 to IPv6 virtual IP groups.

```
config firewall vipgrp46
  Description: Configure IPv4 to IPv6 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
  next
end
```

## config firewall vipgrp46

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP46 name.	string	Maximum length: 79	

## config firewall vipgrp6

Configure IPv6 virtual IP groups.

```
config firewall vipgrp6
  Description: Configure IPv6 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
```

```
next
end
```

## config firewall vipgrp6

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). IPv6 VIP name.	string	Maximum length: 79	

## config firewall vipgrp64

Configure IPv6 to IPv4 virtual IP groups.

```
config firewall vipgrp64
  Description: Configure IPv6 to IPv4 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
  next
end
```

## config firewall vipgrp64

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP64 name.	string	Maximum length: 79	

## config firewall ipmacbinding setting

Configure IP to MAC binding settings.

```
config firewall ipmacbinding setting
  Description: Configure IP to MAC binding settings.
  set bindthroughfw [enable|disable]
  set bindtofw [enable|disable]
  set undefinedhost [allow|block]
end
```

## config firewall ipmacbinding setting

Parameter	Description	Type	Size	Default						
bindthroughfw	Enable/disable use of IP/MAC binding to filter packets that would normally go through the firewall.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IP/MAC binding for packets that would normally go through the firewall.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IP/MAC binding for packets that would normally go through the firewall.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IP/MAC binding for packets that would normally go through the firewall.	<i>disable</i>	Disable IP/MAC binding for packets that would normally go through the firewall.			
Option	Description									
<i>enable</i>	Enable IP/MAC binding for packets that would normally go through the firewall.									
<i>disable</i>	Disable IP/MAC binding for packets that would normally go through the firewall.									
bindtofw	Enable/disable use of IP/MAC binding to filter packets that would normally go to the firewall.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IP/MAC binding for packets that would normally go to the firewall.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IP/MAC binding for packets that would normally go to the firewall.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IP/MAC binding for packets that would normally go to the firewall.	<i>disable</i>	Disable IP/MAC binding for packets that would normally go to the firewall.			
Option	Description									
<i>enable</i>	Enable IP/MAC binding for packets that would normally go to the firewall.									
<i>disable</i>	Disable IP/MAC binding for packets that would normally go to the firewall.									
undefinedhost	Select action to take on packets with IP/MAC addresses not in the binding list .	option	-	block						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow packets from MAC addresses not in the IP/MAC list.</td> </tr> <tr> <td><i>block</i></td> <td>Block packets from MAC addresses not in the IP/MAC list.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow packets from MAC addresses not in the IP/MAC list.	<i>block</i>	Block packets from MAC addresses not in the IP/MAC list.			
Option	Description									
<i>allow</i>	Allow packets from MAC addresses not in the IP/MAC list.									
<i>block</i>	Block packets from MAC addresses not in the IP/MAC list.									

## config firewall ipmacbinding table

Configure IP to MAC address pairs in the IP/MAC binding table.

```
config firewall ipmacbinding table
  Description: Configure IP to MAC address pairs in the IP/MAC binding table.
  edit <seq-num>
    set ip {ipv4-address}
    set mac {mac-address}
    set name {string}
    set status [enable|disable]
  next
end
```

## config firewall ipmacbinding table

Parameter	Description	Type	Size	Default
ip	IPv4 address portion of the pair (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
mac	MAC address portion of the pair (format: xx:xx:xx:xx:xx:xx in hexadecimal).	mac-address	Not Specified	00:00:00:00:00:00
name	Name of the pair .	string	Maximum length: 35	noname
status	Enable/disable this IP-mac binding pair.	option	-	disable

Option	Description
<i>enable</i>	Enable this IP-mac binding pair.
<i>disable</i>	Disable this IP-mac binding pair.

## config firewall profile-protocol-options

Configure protocol options.

```
config firewall profile-protocol-options
  Description: Configure protocol options.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set oversize-log [disable|enable]
    set switching-protocols-log [disable|enable]
  config http
    Description: Configure HTTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set comfort-interval {integer}
```

```

set comfort-amount {integer}
set range-block [disable|enable]
set strip-x-forwarded-for [disable|enable]
set post-lang {option1}, {option2}, ...
set streaming-content-bypass [enable|disable]
set switching-protocols [bypass|block]
set unknown-http-version [reject|tunnel|...]
set tunnel-non-http [enable|disable]
set oversize-limit {integer}
set uncompressed-oversize-limit {integer}
set uncompressed-nest-limit {integer}
set stream-based-uncompressed-limit {integer}
set scan-bzip2 [enable|disable]
set block-page-status-code {integer}
set retry-count {integer}
set tcp-window-type [system|static|...]
set tcp-window-minimum {integer}
set tcp-window-maximum {integer}
set tcp-window-size {integer}
set ssl-offloaded [no|yes]
end
config ftp
  Description: Configure FTP protocol options.
  set ports {integer}
  set status [enable|disable]
  set inspect-all [enable|disable]
  set options {option1}, {option2}, ...
  set comfort-interval {integer}
  set comfort-amount {integer}
  set oversize-limit {integer}
  set uncompressed-oversize-limit {integer}
  set uncompressed-nest-limit {integer}
  set scan-bzip2 [enable|disable]
  set ssl-offloaded [no|yes]
end
config imap
  Description: Configure IMAP protocol options.
  set ports {integer}
  set status [enable|disable]
  set inspect-all [enable|disable]
  set proxy-after-tcp-handshake [enable|disable]
  set options {option1}, {option2}, ...
  set oversize-limit {integer}
  set uncompressed-oversize-limit {integer}
  set uncompressed-nest-limit {integer}
  set scan-bzip2 [enable|disable]
  set ssl-offloaded [no|yes]
end
config mapi
  Description: Configure MAPI protocol options.
  set ports {integer}
  set status [enable|disable]
  set options {option1}, {option2}, ...
  set oversize-limit {integer}
  set uncompressed-oversize-limit {integer}
  set uncompressed-nest-limit {integer}
  set scan-bzip2 [enable|disable]

```

```

end
config pop3
    Description: Configure POP3 protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
end
config smtp
    Description: Configure SMTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set server-busy [enable|disable]
    set ssl-offloaded [no|yes]
end
config nntp
    Description: Configure NNTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
config ssh
    Description: Configure SFTP and SCP protocol options.
    set options {option1}, {option2}, ...
    set comfort-interval {integer}
    set comfort-amount {integer}
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
config dns
    Description: Configure DNS protocol options.
    set ports {integer}
    set status [enable|disable]
end
config cifs
    Description: Configure CIFS protocol options.

```

```

set ports {integer}
set status [enable|disable]
set options {option1}, {option2}, ...
set oversize-limit {integer}
set uncompressed-oversize-limit {integer}
set uncompressed-nest-limit {integer}
set scan-bzip2 [enable|disable]
set tcp-window-type [system|static|...]
set tcp-window-minimum {integer}
set tcp-window-maximum {integer}
set tcp-window-size {integer}
set server-credential-type [none|credential-replication|...]
set domain-controller {string}
config server-keytab
    Description: Server keytab.
    edit <principal>
        set keytab {string}
    next
end
end
config mail-signature
    Description: Configure Mail signature.
    set status [disable|enable]
    set signature {string}
end
set rpc-over-http [enable|disable]
next
end

```

## config firewall profile-protocol-options

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
replacemsg-group	Name of the replacement message group to be used	string	Maximum length: 35							
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for antivirus oversize file blocking.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for antivirus oversize file blocking.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for antivirus oversize file blocking.	<i>enable</i>	Enable logging for antivirus oversize file blocking.			
Option	Description									
<i>disable</i>	Disable logging for antivirus oversize file blocking.									
<i>enable</i>	Enable logging for antivirus oversize file blocking.									
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging for HTTP/HTTPS switching protocols.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging for HTTP/HTTPS switching protocols.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.	<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.			
Option	Description									
<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.									
<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.									
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inspection of RPC over HTTP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inspection of RPC over HTTP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inspection of RPC over HTTP.	<i>disable</i>	Disable inspection of RPC over HTTP.			
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTP.									
<i>disable</i>	Disable inspection of RPC over HTTP.									

### config http

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>clientcomfort</i></td> <td>Prevent client timeout.</td> </tr> <tr> <td><i>servercomfort</i></td> <td>Prevent server timeout.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>chunkedbypass</i></td> <td>Bypass chunked transfer encoded sites.</td> </tr> </tbody> </table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.	<i>oversize</i>	Block oversized file/email.	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.					
Option	Description															
<i>clientcomfort</i>	Prevent client timeout.															
<i>servercomfort</i>	Prevent server timeout.															
<i>oversize</i>	Block oversized file/email.															
<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.															
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10												
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1												
range-block	Enable/disable blocking of partial downloads.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable blocking of partial downloads.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable blocking of partial downloads.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable blocking of partial downloads.	<i>enable</i>	Enable blocking of partial downloads.									
Option	Description															
<i>disable</i>	Disable blocking of partial downloads.															
<i>enable</i>	Enable blocking of partial downloads.															
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable changing of HTTP X-Forwarded-For header.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable replacement of X-Forwarded-For value with 1.1.1.1.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.	<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.									
Option	Description															
<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.															
<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.															
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>jisx0201</i></td> <td>Japanese Industrial Standard 0201.</td> </tr> <tr> <td><i>jisx0208</i></td> <td>Japanese Industrial Standard 0208.</td> </tr> <tr> <td><i>jisx0212</i></td> <td>Japanese Industrial Standard 0212.</td> </tr> <tr> <td><i>gb2312</i></td> <td>Guojia Biaozhun 2312 (simplified Chinese).</td> </tr> <tr> <td><i>ksc5601-ex</i></td> <td>Wansung Korean standard 5601.</td> </tr> </tbody> </table>	Option	Description	<i>jisx0201</i>	Japanese Industrial Standard 0201.	<i>jisx0208</i>	Japanese Industrial Standard 0208.	<i>jisx0212</i>	Japanese Industrial Standard 0212.	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).	<i>ksc5601-ex</i>	Wansung Korean standard 5601.			
Option	Description															
<i>jisx0201</i>	Japanese Industrial Standard 0201.															
<i>jisx0208</i>	Japanese Industrial Standard 0208.															
<i>jisx0212</i>	Japanese Industrial Standard 0212.															
<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).															
<i>ksc5601-ex</i>	Wansung Korean standard 5601.															

Parameter	Description	Type	Size	Default																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>euc-jp</i></td> <td>Extended Unicode Japanese.</td> </tr> <tr> <td><i>sjis</i></td> <td>Shift Japanese Industrial Standard.</td> </tr> <tr> <td><i>iso2022-jp</i></td> <td>ISO 2022 Japanese.</td> </tr> <tr> <td><i>iso2022-jp-1</i></td> <td>ISO 2022-1 Japanese.</td> </tr> <tr> <td><i>iso2022-jp-2</i></td> <td>ISO 2022-2 Japanese.</td> </tr> <tr> <td><i>euc-cn</i></td> <td>Extended Unicode Chinese.</td> </tr> <tr> <td><i>ces-gbk</i></td> <td>Extended GB2312 (simplified Chinese).</td> </tr> <tr> <td><i>hz</i></td> <td>Hanzi simplified Chinese.</td> </tr> <tr> <td><i>ces-big5</i></td> <td>Big-5 traditional Chinese.</td> </tr> <tr> <td><i>euc-kr</i></td> <td>Extended Unicode Korean.</td> </tr> <tr> <td><i>iso2022-jp-3</i></td> <td>ISO 2022-3 Japanese.</td> </tr> <tr> <td><i>iso8859-1</i></td> <td>ISO 8859 Part 1 (Western European).</td> </tr> <tr> <td><i>tis620</i></td> <td>Thai Industrial Standard 620.</td> </tr> <tr> <td><i>cp874</i></td> <td>Code Page 874 (Thai).</td> </tr> <tr> <td><i>cp1252</i></td> <td>Code Page 1252 (Western European Latin).</td> </tr> <tr> <td><i>cp1251</i></td> <td>Code Page 1251 (Cyrillic).</td> </tr> </tbody> </table>	Option	Description	<i>euc-jp</i>	Extended Unicode Japanese.	<i>sjis</i>	Shift Japanese Industrial Standard.	<i>iso2022-jp</i>	ISO 2022 Japanese.	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.	<i>euc-cn</i>	Extended Unicode Chinese.	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).	<i>hz</i>	Hanzi simplified Chinese.	<i>ces-big5</i>	Big-5 traditional Chinese.	<i>euc-kr</i>	Extended Unicode Korean.	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).	<i>tis620</i>	Thai Industrial Standard 620.	<i>cp874</i>	Code Page 874 (Thai).	<i>cp1252</i>	Code Page 1252 (Western European Latin).	<i>cp1251</i>	Code Page 1251 (Cyrillic).			
Option	Description																																					
<i>euc-jp</i>	Extended Unicode Japanese.																																					
<i>sjis</i>	Shift Japanese Industrial Standard.																																					
<i>iso2022-jp</i>	ISO 2022 Japanese.																																					
<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.																																					
<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.																																					
<i>euc-cn</i>	Extended Unicode Chinese.																																					
<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).																																					
<i>hz</i>	Hanzi simplified Chinese.																																					
<i>ces-big5</i>	Big-5 traditional Chinese.																																					
<i>euc-kr</i>	Extended Unicode Korean.																																					
<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.																																					
<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).																																					
<i>tis620</i>	Thai Industrial Standard 620.																																					
<i>cp874</i>	Code Page 874 (Thai).																																					
<i>cp1252</i>	Code Page 1252 (Western European Latin).																																					
<i>cp1251</i>	Code Page 1251 (Cyrillic).																																					
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																															
Option	Description																																					
<i>enable</i>	Enable setting.																																					
<i>disable</i>	Disable setting.																																					
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass connections when switching protocols.</td> </tr> <tr> <td><i>block</i></td> <td>Block connections when switching protocols.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass connections when switching protocols.	<i>block</i>	Block connections when switching protocols.																															
Option	Description																																					
<i>bypass</i>	Bypass connections when switching protocols.																																					
<i>block</i>	Block connections when switching protocols.																																					
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject																																		

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>reject</i></td> <td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td> </tr> <tr> <td><i>tunnel</i></td> <td>Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td> </tr> <tr> <td><i>best-effort</i></td> <td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td> </tr> </tbody> </table>	Option	Description	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.			
Option	Description											
<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.											
<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.											
<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.											
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td> </tr> <tr> <td><i>disable</i></td> <td>Drop or tear down non-HTTP sessions accepted by the profile.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.					
Option	Description											
<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.											
<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.											
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12								
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned .	integer	Minimum value: 0 Maximum value: 4294967295	0								
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
block-page-status-code	Code number returned for blocked HTTP pages .	integer	Minimum value: 100 Maximum value: 599	403								
retry-count	Number of attempts to retry HTTP connection .	integer	Minimum value: 0 Maximum value: 100	0								
tcp-window-type	Specify type of TCP window to use for this protocol.	option	-	system								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use system default TCP window size for this protocol (Default).</td> </tr> <tr> <td><i>static</i></td> <td>Manually specify TCP window size.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Vary TCP window size based on available memory, within limits.</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use system default TCP window size for this protocol (Default).	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory, within limits.			
Option	Description											
<i>system</i>	Use system default TCP window size for this protocol (Default).											
<i>static</i>	Manually specify TCP window size.											
<i>dynamic</i>	Vary TCP window size based on available memory, within limits.											
tcp-window-minimum	Minimum dynamic TCP window size .	integer	Minimum value: 65536 Maximum value: 1048576	131072								
tcp-window-maximum	Maximum dynamic TCP window size .	integer	Minimum value: 1048576 Maximum value: 33554432	8388608								
tcp-window-size	Set TCP static window size .	integer	Minimum value: 65536 Maximum value: 33554432	262144								
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									

\*\* Values may differ between models.

## config ftp

Parameter	Description	Type	Size	Default												
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535													
status	Enable/disable the active status of scanning for this protocol.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
options	One or more options that can be applied to the session.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>clientcomfort</i></td> <td>Prevent client timeout.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>splice</i></td> <td>Enable splice mode.</td> </tr> <tr> <td><i>bypass-rest-command</i></td> <td>Bypass REST command.</td> </tr> <tr> <td><i>bypass-mode-command</i></td> <td>Bypass MODE command.</td> </tr> </tbody> </table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.	<i>bypass-rest-command</i>	Bypass REST command.	<i>bypass-mode-command</i>	Bypass MODE command.			
Option	Description															
<i>clientcomfort</i>	Prevent client timeout.															
<i>oversize</i>	Block oversized file/email.															
<i>splice</i>	Enable splice mode.															
<i>bypass-rest-command</i>	Bypass REST command.															
<i>bypass-mode-command</i>	Bypass MODE command.															

Parameter	Description	Type	Size	Default						
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10						
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1						
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									

\*\* Values may differ between models.

## config imap

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						



Parameter	Description	Type	Size	Default						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									

\*\* Values may differ between models.

## config mapi

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

### config pop3

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									

\*\* Values may differ between models.

### config smtp

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.					
Option	Description									
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable setting.							
Option	Description											
<i>disable</i>	Disable setting.											
options	One or more options that can be applied to the session.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fragmail</i></td> <td>Pass fragmented email.</td> </tr> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>splice</i></td> <td>Enable splice mode.</td> </tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.			
Option	Description											
<i>fragmail</i>	Pass fragmented email.											
<i>oversize</i>	Block oversized file/email.											
<i>splice</i>	Enable splice mode.											
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12								
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no</i></td> <td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td> </tr> <tr> <td><i>yes</i></td> <td>SSL decryption and encryption performed by an external device.</td> </tr> </tbody> </table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									

\*\* Values may differ between models.

## config nntp

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>oversize</i>	Block oversized file/email.					
Option	Description									
<i>oversize</i>	Block oversized file/email.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>splice</i></td> <td>Enable splice mode.</td> </tr> </tbody> </table>	Option	Description	<i>splice</i>	Enable splice mode.					
Option	Description									
<i>splice</i>	Enable splice mode.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

## config ssh

Parameter	Description	Type	Size	Default								
options	One or more options that can be applied to the session.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> <tr> <td><i>clientcomfort</i></td> <td>Prevent client timeout.</td> </tr> <tr> <td><i>servercomfort</i></td> <td>Prevent server timeout.</td> </tr> </tbody> </table>	Option	Description	<i>oversize</i>	Block oversized file/email.	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.			
Option	Description											
<i>oversize</i>	Block oversized file/email.											
<i>clientcomfort</i>	Prevent client timeout.											
<i>servercomfort</i>	Prevent server timeout.											
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10								

Parameter	Description	Type	Size	Default						
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1						
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

## config dns

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									



## config cifs

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>oversize</i></td> <td>Block oversized file/email.</td> </tr> </tbody> </table>	Option	Description	<i>oversize</i>	Block oversized file/email.					
Option	Description									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
tcp-window-type	Specify type of TCP window to use for this protocol.	option	-	system						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use system default TCP window size for this protocol (Default).</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use system default TCP window size for this protocol (Default).					
Option	Description									
<i>system</i>	Use system default TCP window size for this protocol (Default).									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Manually specify TCP window size.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Vary TCP window size based on available memory, within limits.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory, within limits.					
Option	Description											
<i>static</i>	Manually specify TCP window size.											
<i>dynamic</i>	Vary TCP window size based on available memory, within limits.											
tcp-window-minimum	Minimum dynamic TCP window size .	integer	Minimum value: 65536 Maximum value: 1048576	131072								
tcp-window-maximum	Maximum dynamic TCP window size .	integer	Minimum value: 1048576 Maximum value: 33554432	8388608								
tcp-window-size	Set TCP static window size .	integer	Minimum value: 65536 Maximum value: 33554432	262144								
server-credential-type	CIFS server credential type.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Credential derivation not set.</td> </tr> <tr> <td><i>credential-replication</i></td> <td>Credential derived using Replication account on Domain Controller.</td> </tr> <tr> <td><i>credential-keytab</i></td> <td>Credential derived using server keytab.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Credential derivation not set.	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.	<i>credential-keytab</i>	Credential derived using server keytab.			
Option	Description											
<i>none</i>	Credential derivation not set.											
<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.											
<i>credential-keytab</i>	Credential derived using server keytab.											
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63									

\*\* Values may differ between models.

### config server-keytab

Parameter	Description	Type	Size	Default
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	

## config mail-signature

Parameter	Description	Type	Size	Default						
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiGate.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable mail signature.</td></tr><tr><td><i>enable</i></td><td>Enable mail signature.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable mail signature.	<i>enable</i>	Enable mail signature.			
Option	Description									
<i>disable</i>	Disable mail signature.									
<i>enable</i>	Enable mail signature.									
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023							

## config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

```
config firewall ssl-ssh-profile
  Description: Configure SSL/SSH protocol options.
  edit <name>
    set comment {var-string}
    config ssl
      Description: Configure SSL options.
      set inspect-all [disable|certificate-inspection|...]
      set client-certificate [bypass|inspect|...]
      set unsupported-ssl-cipher [allow|block]
      set unsupported-ssl-negotiation [allow|block]
      set expired-server-cert [allow|block|...]
      set revoked-server-cert [allow|block|...]
      set untrusted-server-cert [allow|block|...]
      set cert-validation-timeout [allow|block|...]
      set cert-validation-failure [allow|block|...]
      set sni-server-cert-check [enable|strict|...]
    end
    config https
      Description: Configure HTTPS options.
      set ports {integer}
      set status [disable|certificate-inspection|...]
      set proxy-after-tcp-handshake [enable|disable]
      set client-certificate [bypass|inspect|...]
      set unsupported-ssl-cipher [allow|block]
      set unsupported-ssl-negotiation [allow|block]
      set expired-server-cert [allow|block|...]
      set revoked-server-cert [allow|block|...]
      set untrusted-server-cert [allow|block|...]
      set cert-validation-timeout [allow|block|...]
      set cert-validation-failure [allow|block|...]
      set sni-server-cert-check [enable|strict|...]
    end
    config ftps
      Description: Configure FTPS options.
```

```

set ports {integer}
set status [disable|deep-inspection]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
end
config imaps
Description: Configure IMAPS options.
set ports {integer}
set status [disable|deep-inspection]
set proxy-after-tcp-handshake [enable|disable]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
end
config pop3s
Description: Configure POP3S options.
set ports {integer}
set status [disable|deep-inspection]
set proxy-after-tcp-handshake [enable|disable]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
end
config smtps
Description: Configure SMTPS options.
set ports {integer}
set status [disable|deep-inspection]
set proxy-after-tcp-handshake [enable|disable]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
end

```

```

config ssh
  Description: Configure SSH options.
  set ports {integer}
  set status [disable|deep-inspection]
  set inspect-all [disable|deep-inspection]
  set proxy-after-tcp-handshake [enable|disable]
  set unsupported-version [bypass|block]
  set ssh-tun-policy-check [disable|enable]
  set ssh-algorithm [compatible|high-encryption]
end
set whitelist [enable|disable]
set block-blacklisted-certificates [disable|enable]
config ssl-exempt
  Description: Servers to exempt from SSL inspection.
  edit <id>
    set type [fortiguard-category|address|...]
    set fortiguard-category {integer}
    set address {string}
    set address6 {string}
    set wildcard-fqdn {string}
    set regex {string}
  next
end
set server-cert-mode [re-sign|replace]
set use-ssl-server [disable|enable]
set caname {string}
set untrusted-caname {string}
set server-cert {string}
config ssl-server
  Description: SSL server settings used for client certificate request.
  edit <id>
    set ip {ipv4-address-any}
    set https-client-certificate [bypass|inspect|...]
    set smtps-client-certificate [bypass|inspect|...]
    set pop3s-client-certificate [bypass|inspect|...]
    set imaps-client-certificate [bypass|inspect|...]
    set ftps-client-certificate [bypass|inspect|...]
    set ssl-other-client-certificate [bypass|inspect|...]
  next
end
set ssl-anomalies-log [disable|enable]
set ssl-exemptions-log [disable|enable]
set ssl-negotiation-log [disable|enable]
set rpc-over-https [enable|disable]
set mapi-over-https [enable|disable]
next
end

```

## config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
whitelist	Enable/disable exempting servers by FortiGuard whitelist.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
block-blacklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blacklist.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable FortiGuard certificate blacklist.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable FortiGuard certificate blacklist.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable FortiGuard certificate blacklist.	<i>enable</i>	Enable FortiGuard certificate blacklist.			
Option	Description									
<i>disable</i>	Disable FortiGuard certificate blacklist.									
<i>enable</i>	Enable FortiGuard certificate blacklist.									
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>re-sign</i></td> <td>Multiple clients connecting to multiple servers.</td> </tr> <tr> <td><i>replace</i></td> <td>Protect an SSL server.</td> </tr> </tbody> </table>	Option	Description	<i>re-sign</i>	Multiple clients connecting to multiple servers.	<i>replace</i>	Protect an SSL server.			
Option	Description									
<i>re-sign</i>	Multiple clients connecting to multiple servers.									
<i>replace</i>	Protect an SSL server.									
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Don't use SSL server configuration.</td> </tr> <tr> <td><i>enable</i></td> <td>Use SSL server configuration.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Don't use SSL server configuration.	<i>enable</i>	Use SSL server configuration.			
Option	Description									
<i>disable</i>	Don't use SSL server configuration.									
<i>enable</i>	Use SSL server configuration.									
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_SSL						
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted						
server-cert	Certificate used by SSL Inspection to replace server certificate.	string	Maximum length: 35	Fortinet_SSL						
ssl-anomalies-log	Enable/disable logging SSL anomalies.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging SSL anomalies.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging SSL anomalies.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging SSL anomalies.	<i>enable</i>	Enable logging SSL anomalies.			
Option	Description									
<i>disable</i>	Disable logging SSL anomalies.									
<i>enable</i>	Enable logging SSL anomalies.									
ssl-exemptions-log	Enable/disable logging SSL exemptions.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging SSL exemptions.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging SSL exemptions.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging SSL exemptions.	<i>enable</i>	Enable logging SSL exemptions.			
Option	Description									
<i>disable</i>	Disable logging SSL exemptions.									
<i>enable</i>	Enable logging SSL exemptions.									
ssl-negotiation-log	Enable/disable logging SSL negotiation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging SSL negotiation.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging SSL negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging SSL negotiation.	<i>enable</i>	Enable logging SSL negotiation.			
Option	Description									
<i>disable</i>	Disable logging SSL negotiation.									
<i>enable</i>	Enable logging SSL negotiation.									
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inspection of RPC over HTTPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inspection of RPC over HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inspection of RPC over HTTPS.	<i>disable</i>	Disable inspection of RPC over HTTPS.			
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTPS.									
<i>disable</i>	Disable inspection of RPC over HTTPS.									
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inspection of MAPI over HTTPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inspection of MAPI over HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inspection of MAPI over HTTPS.	<i>disable</i>	Disable inspection of MAPI over HTTPS.			
Option	Description									
<i>enable</i>	Enable inspection of MAPI over HTTPS.									
<i>disable</i>	Disable inspection of MAPI over HTTPS.									

## config ssl

Parameter	Description	Type	Size	Default				
inspect-all	Level of SSL inspection.	option	-	disable				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.			
Option	Description							
<i>disable</i>	Disable.							

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>certificate-inspection</i></td> <td>Inspect SSL handshake only.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>certificate-inspection</i>	Inspect SSL handshake only.											
<i>deep-inspection</i>	Full SSL inspection.											
client-certificate	Action based on received client certificate.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.							
Option	Description											
<i>allow</i>	Allow the server certificate.											



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.					
Option	Description											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config https

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>certificate-inspection</i></td> <td>Inspect SSL handshake only.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description											
<i>disable</i>	Disable.											
<i>certificate-inspection</i>	Inspect SSL handshake only.											
<i>deep-inspection</i>	Full SSL inspection.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config ftps

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
client-certificate	Action based on received client certificate.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config imaps

Parameter	Description	Type	Size	Default						
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535							
status	Configure protocol inspection status.	option	-	deep-inspection						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									

Parameter	Description	Type	Size	Default								
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											



## config pop3s

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											

Parameter	Description	Type	Size	Default								
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

Parameter	Description	Type	Size	Default								
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config smtps

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the cipher is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the cipher is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Bypass the session when the negotiation is not supported.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session when the negotiation is not supported.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow the server certificate.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> <tr> <td><i>ignore</i></td> <td>Re-sign the server certificate as trusted.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td> </tr> <tr> <td><i>strict</i></td> <td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config ssh

Parameter	Description	Type	Size	Default						
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535							
status	Configure protocol inspection status.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									

Parameter	Description	Type	Size	Default						
inspect-all	Level of SSL inspection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>deep-inspection</i></td> <td>Full SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>block</i>	Block the session.			
Option	Description									
<i>bypass</i>	Bypass the session.									
<i>block</i>	Block the session.									
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SSH tunnel policy check.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SSH tunnel policy check.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SSH tunnel policy check.	<i>enable</i>	Enable SSH tunnel policy check.			
Option	Description									
<i>disable</i>	Disable SSH tunnel policy check.									
<i>enable</i>	Enable SSH tunnel policy check.									
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>compatible</i></td> <td>Allow a broader set of encryption algorithms for best compatibility.</td> </tr> <tr> <td><i>high-encryption</i></td> <td>Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.	<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.			
Option	Description									
<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.									
<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.									

### config ssl-exempt

Parameter	Description	Type	Size	Default
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-	fortiguard-category

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard-category</i></td> <td>FortiGuard category.</td> </tr> <tr> <td><i>address</i></td> <td>Firewall IPv4 address.</td> </tr> <tr> <td><i>address6</i></td> <td>Firewall IPv6 address.</td> </tr> <tr> <td><i>wildcard-fqdn</i></td> <td>Fully Qualified Domain Name with wildcard characters.</td> </tr> <tr> <td><i>regex</i></td> <td>Regular expression FQDN.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard-category</i>	FortiGuard category.	<i>address</i>	Firewall IPv4 address.	<i>address6</i>	Firewall IPv6 address.	<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.	<i>regex</i>	Regular expression FQDN.			
Option	Description															
<i>fortiguard-category</i>	FortiGuard category.															
<i>address</i>	Firewall IPv4 address.															
<i>address6</i>	Firewall IPv6 address.															
<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.															
<i>regex</i>	Regular expression FQDN.															
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0												
address	IPv4 address object.	string	Maximum length: 79													
address6	IPv6 address object.	string	Maximum length: 79													
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79													
regex	Exempt servers by regular expression.	string	Maximum length: 255													

### config ssl-server

Parameter	Description	Type	Size	Default								
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0								
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
smtpps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Bypass the session.</td> </tr> <tr> <td><i>inspect</i></td> <td>Inspect the session.</td> </tr> <tr> <td><i>block</i></td> <td>Block the session.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											



## config firewall profile-group

Configure profile groups.

```
config firewall profile-group
  Description: Configure profile groups.
  edit <name>
    set profile-protocol-options {string}
    set ssl-ssh-profile {string}
    set av-profile {string}
    set webfilter-profile {string}
    set dnsfilter-profile {string}
    set emailfilter-profile {string}
    set dlp-sensor {string}
    set file-filter-profile {string}
    set ips-sensor {string}
    set application-list {string}
    set voip-profile {string}
    set icap-profile {string}
    set cifs-profile {string}
    set waf-profile {string}
    set ssh-filter-profile {string}
  next
end
```

## config firewall profile-group

Parameter	Description	Type	Size	Default
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	certificate-inspection
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
application-list	Name of an existing Application list.	string	Maximum length: 35	
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	

## config firewall ssl-server

Configure SSL servers.

```
config firewall ssl-server
  Description: Configure SSL servers.
  edit <name>
    set ip {ipv4-address-any}
    set port {integer}
    set ssl-mode [half|full]
    set add-header-x-forwarded-proto [enable|disable]
    set mapped-port {integer}
    set ssl-cert {string}
    set ssl-dh-bits [768|1024|...]
    set ssl-algorithm [high|medium|...]
    set ssl-client-renegotiation [allow|deny|...]
    set ssl-min-version [tls-1.0|tls-1.1|...]
    set ssl-max-version [tls-1.0|tls-1.1|...]
    set ssl-send-empty-frags [enable|disable]
    set url-rewrite [enable|disable]
  next
end
```

## config firewall ssl-server

Parameter	Description	Type	Size	Default										
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0										
port	Server service port .	integer	Minimum value: 1 Maximum value: 65535	443										
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>half</i></td> <td>Client to FortiGate SSL.</td> </tr> <tr> <td><i>full</i></td> <td>Client to FortiGate and FortiGate to Server SSL.</td> </tr> </tbody> </table>	Option	Description	<i>half</i>	Client to FortiGate SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.							
Option	Description													
<i>half</i>	Client to FortiGate SSL.													
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.													
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Add X-Forwarded-Proto header.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not add X-Forwarded-Proto header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Add X-Forwarded-Proto header.	<i>disable</i>	Do not add X-Forwarded-Proto header.							
Option	Description													
<i>enable</i>	Add X-Forwarded-Proto header.													
<i>disable</i>	Do not add X-Forwarded-Proto header.													
mapped-port	Mapped server service port .	integer	Minimum value: 1 Maximum value: 65535	80										
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35	Fortinet_CA_SSL										
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>768</i></td> <td>768-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1024</i></td> <td>1024-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1536</i></td> <td>1536-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>2048</i></td> <td>2048-bit Diffie-Hellman prime.</td> </tr> </tbody> </table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.			
Option	Description													
<i>768</i>	768-bit Diffie-Hellman prime.													
<i>1024</i>	1024-bit Diffie-Hellman prime.													
<i>1536</i>	1536-bit Diffie-Hellman prime.													
<i>2048</i>	2048-bit Diffie-Hellman prime.													
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High encryption. Allow only AES and ChaCha</td> </tr> <tr> <td><i>medium</i></td> <td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
Option	Description											
<i>high</i>	High encryption. Allow only AES and ChaCha											
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow a SSL client to renegotiate.</td> </tr> <tr> <td><i>deny</i></td> <td>Abort any SSL connection that attempts to renegotiate.</td> </tr> <tr> <td><i>secure</i></td> <td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.			
Option	Description											
<i>allow</i>	Allow a SSL client to renegotiate.											
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.											
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.											
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> </tbody> </table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.			
Option	Description											
<i>tls-1.0</i>	TLS 1.0.											
<i>tls-1.1</i>	TLS 1.1.											
<i>tls-1.2</i>	TLS 1.2.											
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> </tbody> </table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.			
Option	Description											
<i>tls-1.0</i>	TLS 1.0.											
<i>tls-1.1</i>	TLS 1.1.											
<i>tls-1.2</i>	TLS 1.2.											
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send empty fragments.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not send empty fragments.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.					
Option	Description											
<i>enable</i>	Send empty fragments.											
<i>disable</i>	Do not send empty fragments.											
url-rewrite	Enable/disable rewriting the URL.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

## config firewall decrypted-traffic-mirror

Configure decrypted traffic mirror.

```
config firewall decrypted-traffic-mirror
  Description: Configure decrypted traffic mirror.
  edit <name>
    set dstmac {mac-address}
    set traffic-type {option1}, {option2}, ...
    set traffic-source [client|server|...]
    set interface <name1>, <name2>, ...
  next
end
```

## config firewall decrypted-traffic-mirror

Parameter	Description	Type	Size	Default								
dstmac	Set destination MAC address for mirrored traffic.	mac-address	Not Specified	ff:ff:ff:ff:ff:ff								
traffic-type	Types of decrypted traffic to be mirrored.	option	-	ssl								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl</i></td> <td>Mirror decrypted SSL traffic.</td> </tr> <tr> <td><i>ssh</i></td> <td>Mirror decrypted SSH traffic.</td> </tr> </tbody> </table>	Option	Description	<i>ssl</i>	Mirror decrypted SSL traffic.	<i>ssh</i>	Mirror decrypted SSH traffic.					
Option	Description											
<i>ssl</i>	Mirror decrypted SSL traffic.											
<i>ssh</i>	Mirror decrypted SSH traffic.											
traffic-source	Source of decrypted traffic to be mirrored.	option	-	client								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>client</i></td> <td>Mirror client side decrypted traffic.</td> </tr> <tr> <td><i>server</i></td> <td>Mirror server side decrypted traffic.</td> </tr> <tr> <td><i>both</i></td> <td>Mirror both client and server side decrypted traffic.</td> </tr> </tbody> </table>	Option	Description	<i>client</i>	Mirror client side decrypted traffic.	<i>server</i>	Mirror server side decrypted traffic.	<i>both</i>	Mirror both client and server side decrypted traffic.			
Option	Description											
<i>client</i>	Mirror client side decrypted traffic.											
<i>server</i>	Mirror server side decrypted traffic.											
<i>both</i>	Mirror both client and server side decrypted traffic.											
interface <name>	Decrypted traffic mirror interface Decrypted traffic mirror interface.	string	Maximum length: 79									

## config firewall identity-based-route

Configure identity based routing.

```
config firewall identity-based-route
  Description: Configure identity based routing.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set gateway {ipv4-address}
        set device {string}
        set groups <name1>, <name2>, ...
      next
    end
  next
end
```

## config firewall identity-based-route

Parameter	Description	Type	Size	Default
comments	Comments.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default
gateway	IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx , Default: 0.0.0.0).	ipv4-address	Not Specified	0.0.0.0
device	Outgoing interface for the rule.	string	Maximum length: 35	
groups <name>	Select one or more group(s) from available groups that are allowed to use this route. Separate group names with a space. Group name.	string	Maximum length: 79	

## config firewall auth-portal

Configure firewall authentication portals.

```
config firewall auth-portal
  Description: Configure firewall authentication portals.
  set groups <name1>, <name2>, ...
  set portal-addr {string}
  set portal-addr6 {string}
  set identity-based-route {string}
end
```

## config firewall auth-portal

Parameter	Description	Type	Size	Default
groups <name>	Firewall user groups permitted to authenticate through this portal. Separate group names with spaces. Group name.	string	Maximum length: 79	
portal-addr	Address (or FQDN) of the authentication portal.	string	Maximum length: 63	
portal-addr6	IPv6 address (or FQDN) of authentication portal.	string	Maximum length: 63	
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35	

## config firewall security-policy

Configure NGFW IPv4/IPv6 application policies.

```
config firewall security-policy
  Description: Configure NGFW IPv4/IPv6 application policies.
  edit <policyid>
    set uuid {uuid}
    set name {string}
    set comments {var-string}
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set srcaddr-negate [enable|disable]
    set dstaddr-negate [enable|disable]
    set internet-service [enable|disable]
    set internet-service-name <name1>, <name2>, ...
    set internet-service-negate [enable|disable]
    set internet-service-group <name1>, <name2>, ...
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-src [enable|disable]
    set internet-service-src-name <name1>, <name2>, ...
    set internet-service-src-negate [enable|disable]
    set internet-service-src-group <name1>, <name2>, ...
    set internet-service-src-custom <name1>, <name2>, ...
    set internet-service-src-custom-group <name1>, <name2>, ...
    set enforce-default-app-port [enable|disable]
    set service <name1>, <name2>, ...
    set service-negate [enable|disable]
    set action [accept|deny]
    set send-deny-packet [disable|enable]
    set schedule {string}
    set status [enable|disable]
    set logtraffic [all|utm|...]
```

```

set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set voip-profile {string}
set icap-profile {string}
set cifs-profile {string}
set ssh-filter-profile {string}
set application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set url-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set fsso-groups <name1>, <name2>, ...
next
end

```

## config firewall security-policy

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
name	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
srcaddr <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination IPv4 address name and address group names. Address name.	string	Maximum length: 79	



Parameter	Description	Type	Size	Default						
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79							
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.			
Option	Description									
<i>enable</i>	Enable source address negate.									
<i>disable</i>	Disable source address negate.									
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable destination address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable destination address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable destination address negate.	<i>disable</i>	Disable destination address negate.			
Option	Description									
<i>enable</i>	Enable destination address negate.									
<i>disable</i>	Disable destination address negate.									
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Services in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Services in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Services in policy.									
<i>disable</i>	Disable use of Internet Services in policy.									
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated Internet Service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated Internet Service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.			
Option	Description									
<i>enable</i>	Enable negated Internet Service match.									
<i>disable</i>	Disable negated Internet Service match.									
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Services source in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Services source in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Services source in policy.									
<i>disable</i>	Disable use of Internet Services source in policy.									
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated Internet Service source match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated Internet Service source match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated Internet Service source match.	<i>disable</i>	Disable negated Internet Service source match.			
Option	Description									
<i>enable</i>	Enable negated Internet Service source match.									
<i>disable</i>	Disable negated Internet Service source match.									
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
service <name>	Service and service group names. Service name.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.			
Option	Description									
<i>enable</i>	Enable negated service match.									
<i>disable</i>	Disable negated service match.									
action	Policy action (accept/deny).	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Allows session that match the firewall policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Blocks sessions that match the firewall policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Allows session that match the firewall policy.	<i>deny</i>	Blocks sessions that match the firewall policy.			
Option	Description									
<i>accept</i>	Allows session that match the firewall policy.									
<i>deny</i>	Blocks sessions that match the firewall policy.									
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable deny-packet sending.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable deny-packet sending.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable deny-packet sending.	<i>enable</i>	Enable deny-packet sending.			
Option	Description									
<i>disable</i>	Disable deny-packet sending.									
<i>enable</i>	Enable deny-packet sending.									
schedule	Schedule name.	string	Maximum length: 35							
status	Enable or disable this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>single</i></td> <td>Do not allow security profile groups.</td> </tr> <tr> <td><i>group</i></td> <td>Allow security profile groups.</td> </tr> </tbody> </table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.					
Option	Description											
<i>single</i>	Do not allow security profile groups.											
<i>group</i>	Allow security profile groups.											
profile-group	Name of profile group.	string	Maximum length: 35									
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default								
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection								
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35									
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35									
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35									
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35									
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35									
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35									
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
application-list	Name of an existing Application list.	string	Maximum length: 35									
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	Application group names. Application group names.	string	Maximum length: 79	
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79	
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79	
fssso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511	

## config firewall policy

Configure IPv4/IPv6 policies.

```
config firewall policy
  Description: Configure IPv4/IPv6 policies.
  edit <policyid>
    set status [enable|disable]
    set name {string}
    set uuid {uuid}
    set srcintf <name1>, <name2>, ...
```

---

```
set dstintf <name1>, <name2>, ...
set srcaddr <name1>, <name2>, ...
set dstaddr <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set dstaddr6 <name1>, <name2>, ...
set internet-service [enable|disable]
set internet-service-name <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-src [enable|disable]
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set reputation-minimum {integer}
set reputation-direction [source|destination]
set src-vendor-mac <id1>, <id2>, ...
set rtp-nat [disable|enable]
set rtp-addr <name1>, <name2>, ...
set action [accept|deny|...]
set send-deny-packet [disable|enable]
set firewall-session-dirty [check-all|check-new]
set schedule {string}
set schedule-timeout [enable|disable]
set service <name1>, <name2>, ...
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set anti-replay [enable|disable]
set tcp-session-without-syn [all|data-only|...]
set geoup-anycast [enable|disable]
set geoup-match [physical-location|registered-location]
set dynamic-shaping [enable|disable]
set utm-status [enable|disable]
set inspection-mode [proxy|flow]
set http-policy-redirect [enable|disable]
set ssh-policy-redirect [enable|disable]
set webproxy-profile {string}
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set voip-profile {string}
set icap-profile {string}
set cifs-profile {string}
set waf-profile {string}
set ssh-filter-profile {string}
set logtraffic [all|utm|...]
```

---

```
set logtraffic-start [enable|disable]
set auto-asic-offload [enable|disable]
set np-acceleration [enable|disable]
set webproxy-forward-server {string}
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set per-ip-shaper {string}
set nat [enable|disable]
set permit-any-host [enable|disable]
set permit-stun-host [enable|disable]
set fixedport [enable|disable]
set ippool [enable|disable]
set poolname <name1>, <name2>, ...
set poolname6 <name1>, <name2>, ...
set session-ttl {user}
set vlan-cos-fwd {integer}
set vlan-cos-rev {integer}
set inbound [enable|disable]
set outbound [enable|disable]
set natinbound [enable|disable]
set natoutbound [enable|disable]
set wccp [enable|disable]
set ntlm [enable|disable]
set ntlm-guest [enable|disable]
set ntlm-enabled-browsers <user-agent-string1>, <user-agent-string2>, ...
set fsso-agent-for-ntlm {string}
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set fsso-groups <name1>, <name2>, ...
set auth-path [enable|disable]
set disclaimer [enable|disable]
set email-collect [enable|disable]
set vpntunnel {string}
set natip {ipv4-classnet}
set match-vip [enable|disable]
set match-vip-only [enable|disable]
set diffserv-forward [enable|disable]
set diffserv-reverse [enable|disable]
set diffservcode-forward {user}
set diffservcode-rev {user}
set tcp-mss-sender {integer}
set tcp-mss-receiver {integer}
set comments {var-string}
set auth-cert {string}
set auth-redirect-addr {string}
set redirect-url {string}
set identity-based-route {string}
set block-notification [enable|disable]
set custom-log-fields <field-id1>, <field-id2>, ...
set replacemsg-override-group {string}
set srcaddr-negate [enable|disable]
set dstaddr-negate [enable|disable]
set service-negate [enable|disable]
set internet-service-negate [enable|disable]
set internet-service-src-negate [enable|disable]
set timeout-send-rst [enable|disable]
set captive-portal-exempt [enable|disable]
```

```

set decrypted-traffic-mirror {string}
set dsri [enable|disable]
set radius-mac-auth-bypass [enable|disable]
set delay-tcp-npu-session [enable|disable]
set vlan-filter {user}
next
end

```

## config firewall policy

Parameter	Description	Type	Size	Default						
status	Enable or disable this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
name	Policy name.	string	Maximum length: 35							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79							
srcaddr <name>	Source IPv4 address and address group names. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination IPv4 address and address group names. Address name.	string	Maximum length: 79							
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79							
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79							
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Services in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Services in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Services in policy.									
<i>disable</i>	Disable use of Internet Services in policy.									
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Services source in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Services source in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Services source in policy.									
<i>disable</i>	Disable use of Internet Services source in policy.									
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default
reputation-minimum	Minimum Reputation to take action.	integer	Minimum value: 0 Maximum value: 4294967295	0
reputation-direction	Direction of the initial traffic for reputation to take effect.	option	-	destination
	<b>Option</b>	<b>Description</b>		
	<i>source</i>	Check reputation for source address.		
	<i>destination</i>	Check reputation for destination address.		
src-vendor-mac <id>	Vendor MAC source ID. Vendor MAC ID.	integer	Minimum value: 0 Maximum value: 4294967295	
rtp-nat	Enable Real Time Protocol (RTP) NAT.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable setting.		
	<i>enable</i>	Enable setting.		
rtp-addr <name>	Address names if this is an RTP NAT policy. Address name.	string	Maximum length: 79	
action	Policy action (accept/deny/ipsec).	option	-	deny
	<b>Option</b>	<b>Description</b>		
	<i>accept</i>	Allows session that match the firewall policy.		
	<i>deny</i>	Blocks sessions that match the firewall policy.		
	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.		
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable deny-packet sending.		
	<i>enable</i>	Enable deny-packet sending.		
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-	check-all

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>check-all</i></td> <td>Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.</td> </tr> <tr> <td><i>check-new</i></td> <td>Continue to allow sessions already accepted by this policy.</td> </tr> </tbody> </table>	Option	Description	<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.	<i>check-new</i>	Continue to allow sessions already accepted by this policy.			
Option	Description									
<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.									
<i>check-new</i>	Continue to allow sessions already accepted by this policy.									
schedule	Schedule name.	string	Maximum length: 35							
schedule-timeout	Enable to force current sessions to end when the schedule object times out. Disable allows them to end from inactivity.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable schedule timeout.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable schedule timeout.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable schedule timeout.	<i>disable</i>	Disable schedule timeout.			
Option	Description									
<i>enable</i>	Enable schedule timeout.									
<i>disable</i>	Disable schedule timeout.									
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79							
tos	ToS (Type of Service) value used for comparison.	user	Not Specified							
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified							
tos-negate	Enable negated TOS match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TOS match negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TOS match negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TOS match negate.	<i>disable</i>	Disable TOS match negate.			
Option	Description									
<i>enable</i>	Enable TOS match negate.									
<i>disable</i>	Disable TOS match negate.									
anti-replay	Enable/disable anti-replay check.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anti-replay check.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anti-replay check.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anti-replay check.	<i>disable</i>	Disable anti-replay check.			
Option	Description									
<i>enable</i>	Enable anti-replay check.									
<i>disable</i>	Disable anti-replay check.									
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Enable TCP session without SYN.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Enable TCP session without SYN.					
Option	Description									
<i>all</i>	Enable TCP session without SYN.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>data-only</i></td> <td>Enable TCP session data only.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TCP session without SYN.</td> </tr> </tbody> </table>	Option	Description	<i>data-only</i>	Enable TCP session data only.	<i>disable</i>	Disable TCP session without SYN.			
Option	Description									
<i>data-only</i>	Enable TCP session data only.									
<i>disable</i>	Disable TCP session without SYN.									
geopip-anycast	Enable/disable recognition of anycast IP addresses using the geography IP database.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable recognition of anycast IP addresses using the geography IP database.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable recognition of anycast IP addresses using the geography IP database.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.	<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.			
Option	Description									
<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.									
<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.									
geopip-match	Match geography address based either on its physical location or registered location.	option	-	physical-location						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>physical-location</i></td> <td>Match geography address to its physical location using the geography IP database.</td> </tr> <tr> <td><i>registered-location</i></td> <td>Match geography address to its registered location using the geography IP database.</td> </tr> </tbody> </table>	Option	Description	<i>physical-location</i>	Match geography address to its physical location using the geography IP database.	<i>registered-location</i>	Match geography address to its registered location using the geography IP database.			
Option	Description									
<i>physical-location</i>	Match geography address to its physical location using the geography IP database.									
<i>registered-location</i>	Match geography address to its registered location using the geography IP database.									
dynamic-shaping	Enable/disable dynamic RADIUS defined traffic shaping.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dynamic RADIUS defined traffic shaping.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dynamic RADIUS defined traffic shaping.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dynamic RADIUS defined traffic shaping.	<i>disable</i>	Disable dynamic RADIUS defined traffic shaping.			
Option	Description									
<i>enable</i>	Enable dynamic RADIUS defined traffic shaping.									
<i>disable</i>	Disable dynamic RADIUS defined traffic shaping.									
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-	flow						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>proxy</i></td> <td>Proxy based inspection.</td> </tr> <tr> <td><i>flow</i></td> <td>Flow based inspection.</td> </tr> </tbody> </table>	Option	Description	<i>proxy</i>	Proxy based inspection.	<i>flow</i>	Flow based inspection.			
Option	Description									
<i>proxy</i>	Proxy based inspection.									
<i>flow</i>	Flow based inspection.									
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HTTP(S) policy redirect.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HTTP(S) policy redirect.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HTTP(S) policy redirect.	<i>disable</i>	Disable HTTP(S) policy redirect.			
Option	Description									
<i>enable</i>	Enable HTTP(S) policy redirect.									
<i>disable</i>	Disable HTTP(S) policy redirect.									
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSH policy redirect.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSH policy redirect.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSH policy redirect.	<i>disable</i>	Disable SSH policy redirect.			
Option	Description									
<i>enable</i>	Enable SSH policy redirect.									
<i>disable</i>	Disable SSH policy redirect.									
webproxy-profile	Webproxy profile name.	string	Maximum length: 63							
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>single</i></td> <td>Do not allow security profile groups.</td> </tr> <tr> <td><i>group</i></td> <td>Allow security profile groups.</td> </tr> </tbody> </table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.			
Option	Description									
<i>single</i>	Do not allow security profile groups.									
<i>group</i>	Allow security profile groups.									
profile-group	Name of profile group.	string	Maximum length: 35							
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default						
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35							
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default								
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35									
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35									
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35									
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35									
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
application-list	Name of an existing Application list.	string	Maximum length: 35									
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35									
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35									
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35									
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35									
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>		Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
logtraffic-start	Record logs when a session starts.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
auto-asic-offload	Enable/disable policy traffic ASIC offloading.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auto ASIC offloading.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ASIC offloading.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.			
Option	Description									
<i>enable</i>	Enable auto ASIC offloading.									
<i>disable</i>	Disable ASIC offloading.									
np-acceleration*	Enable/disable UTM Network Processor acceleration.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable UTM Network Processor acceleration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable UTM Network Processor acceleration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable UTM Network Processor acceleration.	<i>disable</i>	Disable UTM Network Processor acceleration.			
Option	Description									
<i>enable</i>	Enable UTM Network Processor acceleration.									
<i>disable</i>	Disable UTM Network Processor acceleration.									
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63							
traffic-shaper	Traffic shaper.	string	Maximum length: 35							
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35							
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35							
nat	Enable/disable source NAT.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
permit-any-host	Accept UDP packets from any host.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
permit-stun-host	Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ippool	Enable to use IP Pools for source NAT.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79							
poolname6 <name>	IPv6 pool names. IPv6 pool name.	string	Maximum length: 79							
session-ttl	TTL in seconds for sessions accepted by this policy .	user	Not Specified							
vlan-cos-fwd	VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255						
vlan-cos-rev	VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255						
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									



Parameter	Description	Type	Size	Default						
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
wccp	Enable/disable forwarding traffic matching this policy to a configured WCCP server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WCCP setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WCCP setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WCCP setting.	<i>disable</i>	Disable WCCP setting.			
Option	Description									
<i>enable</i>	Enable WCCP setting.									
<i>disable</i>	Disable WCCP setting.									
ntlm	Enable/disable NTLM authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ntlm-guest	Enable/disable NTLM guest user access.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ntlm-enabled-browsers	HTTP-User-Agent value of supported browsers. User agent string.	string	Maximum length: 79							
<user-agent-string>										
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35							
groups	Names of user groups that can authenticate with this policy.	string	Maximum length: 79							
<name>										

Parameter	Description	Type	Size	Default						
	Group name.									
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79							
fssso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511							
auth-path	Enable/disable authentication-based routing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable authentication-based routing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable authentication-based routing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable authentication-based routing.	<i>disable</i>	Disable authentication-based routing.			
Option	Description									
<i>enable</i>	Enable authentication-based routing.									
<i>disable</i>	Disable authentication-based routing.									
disclaimer	Enable/disable user authentication disclaimer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable user authentication disclaimer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable user authentication disclaimer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable user authentication disclaimer.	<i>disable</i>	Disable user authentication disclaimer.			
Option	Description									
<i>enable</i>	Enable user authentication disclaimer.									
<i>disable</i>	Disable user authentication disclaimer.									
email-collect	Enable/disable email collection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable email collection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable email collection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable email collection.	<i>disable</i>	Disable email collection.			
Option	Description									
<i>enable</i>	Enable email collection.									
<i>disable</i>	Disable email collection.									
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35							
natip	Policy-based IPsec VPN: source NAT IP address for outgoing traffic.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
match-vip	Enable to match packets that have had their destination addresses changed by a VIP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Match DNATed packet.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not match DNATed packet.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Match DNATed packet.	<i>disable</i>	Do not match DNATed packet.			
Option	Description									
<i>enable</i>	Match DNATed packet.									
<i>disable</i>	Do not match DNATed packet.									
match-vip-only	Enable/disable matching of only those packets that have had their destination addresses changed by a VIP.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable matching of only those packets that have had their destination addresses changed by a VIP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable matching of only those packets that have had their destination addresses changed by a VIP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.	<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.			
Option	Description									
<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.									
<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.									
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting forward (original) traffic DiffServ.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting forward (original) traffic DiffServ.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting forward (original) traffic DiffServ.	<i>disable</i>	Disable setting forward (original) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting forward (original) traffic DiffServ.									
<i>disable</i>	Disable setting forward (original) traffic DiffServ.									
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting reverse (reply) traffic DiffServ.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting reverse (reply) traffic DiffServ.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.									
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified							
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified							
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535	0						
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535	0						
comments	Comment.	var-string	Maximum length: 1023							
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35							
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default						
redirect-url	URL users are directed to after seeing and accepting the disclaimer or authenticating.	string	Maximum length: 255							
identity-based-route	Name of identity-based routing rule.	string	Maximum length: 35							
block-notification	Enable/disable block notification.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35							
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35							
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.			
Option	Description									
<i>enable</i>	Enable source address negate.									
<i>disable</i>	Disable source address negate.									
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable destination address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable destination address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable destination address negate.	<i>disable</i>	Disable destination address negate.			
Option	Description									
<i>enable</i>	Enable destination address negate.									
<i>disable</i>	Disable destination address negate.									
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.			
Option	Description									
<i>enable</i>	Enable negated service match.									
<i>disable</i>	Disable negated service match.									
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated Internet Service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated Internet Service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.			
Option	Description									
<i>enable</i>	Enable negated Internet Service match.									
<i>disable</i>	Disable negated Internet Service match.									
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated Internet Service source match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated Internet Service source match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated Internet Service source match.	<i>disable</i>	Disable negated Internet Service source match.			
Option	Description									
<i>enable</i>	Enable negated Internet Service source match.									
<i>disable</i>	Disable negated Internet Service source match.									
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of RST packet upon TCP session expiration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of RST packet upon TCP session expiration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of RST packet upon TCP session expiration.	<i>disable</i>	Disable sending of RST packet upon TCP session expiration.			
Option	Description									
<i>enable</i>	Enable sending of RST packet upon TCP session expiration.									
<i>disable</i>	Disable sending of RST packet upon TCP session expiration.									
captive-portal-exempt	Enable to exempt some users from the captive portal.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable exemption of captive portal.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable exemption of captive portal.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable exemption of captive portal.	<i>disable</i>	Disable exemption of captive portal.			
Option	Description									
<i>enable</i>	Enable exemption of captive portal.									
<i>disable</i>	Disable exemption of captive portal.									
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
dsri	Enable DSRI to ignore HTTP server responses.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DSRI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DSRI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MAC authentication bypass.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MAC authentication bypass.					
Option	Description									
<i>enable</i>	Enable MAC authentication bypass.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable MAC authentication bypass.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable MAC authentication bypass.					
Option	Description									
<i>disable</i>	Disable MAC authentication bypass.									
delay-tcp-npu-session	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.	<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.			
Option	Description									
<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.									
<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.									
vlan-filter	Set VLAN filters.	user	Not Specified							

\* This parameter may not exist in some models.

## config firewall traffic-class

Configure names for shaping classes.

```
config firewall traffic-class
  Description: Configure names for shaping classes.
  edit <class-id>
    set class-name {string}
  next
end
```

## config firewall traffic-class

Parameter	Description	Type	Size	Default
class-name	Define the name for this class-id.	string	Maximum length: 35	

## config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
  Description: Configure shaping policies.
  edit <id>
    set name {string}
    set comment {var-string}
    set status [enable|disable]
    set ip-version [4|6]
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
```

```

set srcaddr6 <name1>, <name2>, ...
set dstaddr6 <name1>, <name2>, ...
set internet-service [enable|disable]
set internet-service-name <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-src [enable|disable]
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set service <name1>, <name2>, ...
set schedule {string}
set users <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
set url-category <id1>, <id2>, ...
set srcintf <name1>, <name2>, ...
set dstintf <name1>, <name2>, ...
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set per-ip-shaper {string}
set class-id {integer}
set diffserv-forward [enable|disable]
set diffserv-reverse [enable|disable]
set diffservcode-forward {user}
set diffservcode-rev {user}
next
end

```

## config firewall shaping-policy

Parameter	Description	Type	Size	Default
name	Shaping policy name.	string	Maximum length: 35	
comment	Comments.	var-string	Maximum length: 255	
status	Enable/disable this traffic shaping policy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable traffic shaping policy.		
	<i>disable</i>	Disable traffic shaping policy.		

Parameter	Description	Type	Size	Default						
ip-version	Apply this traffic shaping policy to IPv4 or IPv6 traffic.	option	-	4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Use IPv4 addressing for Configuration Method.</td> </tr> <tr> <td>6</td> <td>Use IPv6 addressing for Configuration Method.</td> </tr> </tbody> </table>	Option	Description	4	Use IPv4 addressing for Configuration Method.	6	Use IPv6 addressing for Configuration Method.			
Option	Description									
4	Use IPv4 addressing for Configuration Method.									
6	Use IPv6 addressing for Configuration Method.									
srcaddr <name>	IPv4 source address and address group names. Address name.	string	Maximum length: 79							
dstaddr <name>	IPv4 destination address and address group names. Address name.	string	Maximum length: 79							
srcaddr6 <name>	IPv6 source address and address group names. Address name.	string	Maximum length: 79							
dstaddr6 <name>	IPv6 destination address and address group names. Address name.	string	Maximum length: 79							
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Service in shaping-policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Service in shaping-policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Service in shaping-policy.	<i>disable</i>	Disable use of Internet Service in shaping-policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Service in shaping-policy.									
<i>disable</i>	Disable use of Internet Service in shaping-policy.									
internet-service-name <name>	Internet Service ID. Internet Service name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Service source in shaping-policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Service source in shaping-policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Service source in shaping-policy.	<i>disable</i>	Disable use of Internet Service source in shaping-policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Service source in shaping-policy.									
<i>disable</i>	Disable use of Internet Service source in shaping-policy.									
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
service <name>	Service and service group names. Service name.	string	Maximum length: 79							
schedule	Schedule name.	string	Maximum length: 35							
users <name>	Apply this traffic shaping policy to individual users that have authenticated with the FortiGate. User name.	string	Maximum length: 79							
groups <name>	Apply this traffic shaping policy to user groups that have authenticated with the FortiGate. Group name.	string	Maximum length: 79							
application <id>	IDs of one or more applications that this shaper applies application control traffic shaping to. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
app-group <name>	One or more application group names.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
	Application group name.									
url-category <id>	IDs of one or more FortiGuard Web Filtering categories that this shaper applies traffic shaping to. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295							
srcintf <name>	One or more incoming (ingress) interfaces. Interface name.	string	Maximum length: 79							
dstintf <name>	One or more outgoing (egress) interfaces. Interface name.	string	Maximum length: 79							
tos	ToS (Type of Service) value used for comparison.	user	Not Specified							
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified							
tos-negate	Enable negated TOS match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TOS match negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TOS match negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TOS match negate.	<i>disable</i>	Disable TOS match negate.			
Option	Description									
<i>enable</i>	Enable TOS match negate.									
<i>disable</i>	Disable TOS match negate.									
traffic-shaper	Traffic shaper to apply to traffic forwarded by the firewall policy.	string	Maximum length: 35							
traffic-shaper-reverse	Traffic shaper to apply to response traffic received by the firewall policy.	string	Maximum length: 35							
per-ip-shaper	Per-IP traffic shaper to apply with this policy.	string	Maximum length: 35							
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting forward (original) traffic DiffServ.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting forward (original) traffic DiffServ.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting forward (original) traffic DiffServ.	<i>disable</i>	Disable setting forward (original) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting forward (original) traffic DiffServ.									
<i>disable</i>	Disable setting forward (original) traffic DiffServ.									
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting reverse (reply) traffic DiffServ.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting reverse (reply) traffic DiffServ.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.									
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified							
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified							

## config firewall shaping-profile

Configure shaping profiles.

```

config firewall shaping-profile
  Description: Configure shaping profiles.
  edit <profile-name>
    set comment {var-string}
    set type [policing|queuing]
    set default-class-id {integer}
  config shaping-entries
    Description: Define shaping entries of this shaping profile.
    edit <id>
      set class-id {integer}
      set priority [top|critical|...]
      set guaranteed-bandwidth-percentage {integer}
      set maximum-bandwidth-percentage {integer}
      set limit {integer}
      set burst-in-msec {integer}
      set cburst-in-msec {integer}
      set red-probability {integer}
      set min {integer}
      set max {integer}
    next
  end
next
end

```

## config firewall shaping-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
type	Select shaping profile type: policing / queuing.	option	-	policing

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>policing</i></td> <td>Enable policing mode.</td> </tr> <tr> <td><i>queuing</i></td> <td>Enable queuing mode.</td> </tr> </tbody> </table>	Option	Description	<i>policing</i>	Enable policing mode.	<i>queuing</i>	Enable queuing mode.			
Option	Description									
<i>policing</i>	Enable policing mode.									
<i>queuing</i>	Enable queuing mode.									
default-class-id	Default class ID to handle unclassified packets (including all local traffic).	integer	Minimum value: 0 Maximum value: 4294967295	0						

### config shaping-entries

Parameter	Description	Type	Size	Default												
class-id	Class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
priority	Priority.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>top</i></td> <td>Top priority.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical priority.</td> </tr> <tr> <td><i>high</i></td> <td>High priority.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium priority.</td> </tr> <tr> <td><i>low</i></td> <td>Low priority.</td> </tr> </tbody> </table>	Option	Description	<i>top</i>	Top priority.	<i>critical</i>	Critical priority.	<i>high</i>	High priority.	<i>medium</i>	Medium priority.	<i>low</i>	Low priority.			
Option	Description															
<i>top</i>	Top priority.															
<i>critical</i>	Critical priority.															
<i>high</i>	High priority.															
<i>medium</i>	Medium priority.															
<i>low</i>	Low priority.															
guaranteed-bandwidth-percentage	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100	0												
maximum-bandwidth-percentage	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1												
limit	Hard limit on the real queue size in packets.	integer	Minimum value: 5 Maximum value: 10000	1000												

Parameter	Description	Type	Size	Default
burst-in-msec	Number of bytes that can be burst at maximum-bandwidth speed. Formula: burst = maximum-bandwidth*burst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
cburst-in-msec	Number of bytes that can be burst as fast as the interface can transmit. Formula: cburst = maximum-bandwidth*cburst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
red-probability	Maximum probability (in percentage) for RED marking.	integer	Minimum value: 0 Maximum value: 20	0
min	Average queue size in packets at which RED drop becomes a possibility.	integer	Minimum value: 3 Maximum value: 3000	83
max	Average queue size in packets at which RED drop probability is maximal.	integer	Minimum value: 3 Maximum value: 3000	250

## config firewall local-in-policy

Configure user defined IPv4 local-in policies.

```

config firewall local-in-policy
  Description: Configure user defined IPv4 local-in policies.
  edit <policyid>
    set uuid {uuid}
    set ha-mgmt-intf-only [enable|disable]
    set intf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set action [accept|deny]
    set service <name1>, <name2>, ...
    set schedule {string}
    set status [enable|disable]
    set comments {var-string}
  next
end

```

## config firewall local-in-policy

Parameter	Description	Type	Size	Default						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
ha-mgmt-intf-only	Enable/disable dedicating the HA management interface only for local-in policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dedicating HA management interface only for local-in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dedicating HA management interface only for local-in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dedicating HA management interface only for local-in policy.	<i>disable</i>	Disable dedicating HA management interface only for local-in policy.			
Option	Description									
<i>enable</i>	Enable dedicating HA management interface only for local-in policy.									
<i>disable</i>	Disable dedicating HA management interface only for local-in policy.									
intf	Incoming interface name from available options.	string	Maximum length: 35							
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79							
action	Action performed on traffic matching the policy .	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Allow traffic matching this policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny or block traffic matching this policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Allow traffic matching this policy.	<i>deny</i>	Deny or block traffic matching this policy.			
Option	Description									
<i>accept</i>	Allow traffic matching this policy.									
<i>deny</i>	Deny or block traffic matching this policy.									
service <name>	Service object from available options. Service name.	string	Maximum length: 79							
schedule	Schedule object from available options.	string	Maximum length: 35							
status	Enable/disable this local-in policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this local-in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this local-in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this local-in policy.	<i>disable</i>	Disable this local-in policy.			
Option	Description									
<i>enable</i>	Enable this local-in policy.									
<i>disable</i>	Disable this local-in policy.									
comments	Comment.	var-string	Maximum length: 1023							

## config firewall local-in-policy6

Configure user defined IPv6 local-in policies.

```

config firewall local-in-policy6
  Description: Configure user defined IPv6 local-in policies.
  edit <policyid>
    set uuid {uuid}
    set intf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set action [accept|deny]
    set service <name1>, <name2>, ...
    set schedule {string}
    set status [enable|disable]
    set comments {var-string}
  next
end

```

## config firewall local-in-policy6

Parameter	Description	Type	Size	Default						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
intf	Incoming interface name from available options.	string	Maximum length: 35							
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79							
action	Action performed on traffic matching the policy .	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Allow local-in traffic matching this policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny or block local-in traffic matching this policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Allow local-in traffic matching this policy.	<i>deny</i>	Deny or block local-in traffic matching this policy.			
Option	Description									
<i>accept</i>	Allow local-in traffic matching this policy.									
<i>deny</i>	Deny or block local-in traffic matching this policy.									
service <name>	Service object from available options. Separate names with a space. Service name.	string	Maximum length: 79							
schedule	Schedule object from available options.	string	Maximum length: 35							
status	Enable/disable this local-in policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this local-in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this local-in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this local-in policy.	<i>disable</i>	Disable this local-in policy.			
Option	Description									
<i>enable</i>	Enable this local-in policy.									
<i>disable</i>	Disable this local-in policy.									

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	

## config firewall ttl-policy

Configure TTL policies.

```
config firewall ttl-policy
  Description: Configure TTL policies.
  edit <id>
    set status [enable|disable]
    set action [accept|deny]
    set srcintf {string}
    set srcaddr <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    set schedule {string}
    set ttl {user}
  next
end
```

## config firewall ttl-policy

Parameter	Description	Type	Size	Default						
status	Enable/disable this TTL policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this TTL policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this TTL policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this TTL policy.	<i>disable</i>	Disable this TTL policy.			
Option	Description									
<i>enable</i>	Enable this TTL policy.									
<i>disable</i>	Disable this TTL policy.									
action	Action to be performed on traffic matching this policy .	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Allow traffic matching this policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny or block traffic matching this policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Allow traffic matching this policy.	<i>deny</i>	Deny or block traffic matching this policy.			
Option	Description									
<i>accept</i>	Allow traffic matching this policy.									
<i>deny</i>	Deny or block traffic matching this policy.									
srcintf	Source interface name from available interfaces.	string	Maximum length: 35							
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79							
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79							



Parameter	Description	Type	Size	Default
schedule	Schedule object from available options.	string	Maximum length: 35	
ttl	Value/range to match against the packet's Time to Live value .	user	Not Specified	

## config firewall policy64

Configure IPv6 to IPv4 policies.

```
config firewall policy64
  Description: Configure IPv6 to IPv4 policies.
  edit <policyid>
    set name {string}
    set uuid {uuid}
    set srcintf {string}
    set dstintf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set action [accept|deny]
    set status [enable|disable]
    set schedule {string}
    set service <name1>, <name2>, ...
    set logtraffic [enable|disable]
    set logtraffic-start [enable|disable]
    set permit-any-host [enable|disable]
    set traffic-shaper {string}
    set traffic-shaper-reverse {string}
    set per-ip-shaper {string}
    set fixedport [enable|disable]
    set ippool [enable|disable]
    set poolname <name1>, <name2>, ...
    set tcp-mss-sender {integer}
    set tcp-mss-receiver {integer}
    set comments {var-string}
  next
end
```

## config firewall policy64

Parameter	Description	Type	Size	Default
name	Policy name.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

Parameter	Description	Type	Size	Default						
srcintf	Source interface name.	string	Maximum length: 35							
dstintf	Destination interface name.	string	Maximum length: 35							
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79							
action	Policy action.	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Action accept.</td> </tr> <tr> <td><i>deny</i></td> <td>Action deny.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Action accept.	<i>deny</i>	Action deny.			
Option	Description									
<i>accept</i>	Action accept.									
<i>deny</i>	Action deny.									
status	Enable/disable policy status.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
schedule	Schedule name.	string	Maximum length: 35							
service <name>	Service name. Address name.	string	Maximum length: 79							
logtraffic	Enable/disable policy log traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
logtraffic-start	Record logs when a session starts and ends.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
permit-any-host	Enable/disable permit any host in.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
traffic-shaper	Traffic shaper.	string	Maximum length: 35							
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35							
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35							
fixedport	Enable/disable policy fixed port.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ippool	Enable/disable policy64 IP pool.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
poolname <name>	Policy IP pool names. IP pool name.	string	Maximum length: 79							
tcp-mss-sender	TCP MSS value of sender.	integer	Minimum value: 0 Maximum value: 65535	0						
tcp-mss-receiver	TCP MSS value of receiver.	integer	Minimum value: 0 Maximum value: 65535	0						
comments	Comment.	var-string	Maximum length: 1023							

## config firewall policy46

Configure IPv4 to IPv6 policies.

```
config firewall policy46
```

Description: Configure IPv4 to IPv6 policies.

```
edit <policyid>
  set permit-any-host [enable|disable]
  set name {string}
  set uuid {uuid}
  set srcintf {string}
  set dstintf {string}
  set srcaddr <name1>, <name2>, ...
  set dstaddr <name1>, <name2>, ...
  set action [accept|deny]
  set status [enable|disable]
  set schedule {string}
  set service <name1>, <name2>, ...
  set logtraffic [enable|disable]
  set logtraffic-start [enable|disable]
  set traffic-shaper {string}
  set traffic-shaper-reverse {string}
  set per-ip-shaper {string}
  set fixedport [enable|disable]
  set tcp-mss-sender {integer}
  set tcp-mss-receiver {integer}
  set comments {var-string}
  set ippool [enable|disable]
  set poolname <name1>, <name2>, ...
next
end
```

## config firewall policy46

Parameter	Description	Type	Size	Default						
permit-any-host	Enable/disable allowing any host.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Allow any host.</td></tr><tr><td><i>disable</i></td><td>Do not allow any host.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Allow any host.	<i>disable</i>	Do not allow any host.			
Option	Description									
<i>enable</i>	Allow any host.									
<i>disable</i>	Do not allow any host.									
name	Policy name.	string	Maximum length: 35							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
srcintf	Source interface name.	string	Maximum length: 35							
dstintf	Destination interface name.	string	Maximum length: 35							
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79							
action	Accept or deny traffic matching the policy.	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Accept matching traffic.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny matching traffic.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Accept matching traffic.	<i>deny</i>	Deny matching traffic.			
Option	Description									
<i>accept</i>	Accept matching traffic.									
<i>deny</i>	Deny matching traffic.									
status	Enable/disable this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
schedule	Schedule name.	string	Maximum length: 35							
service <name>	Service name. Service name.	string	Maximum length: 79							
logtraffic	Enable/disable traffic logging for this policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable traffic logging.	<i>disable</i>	Disable traffic logging.			
Option	Description									
<i>enable</i>	Enable traffic logging.									
<i>disable</i>	Disable traffic logging.									
logtraffic-start	Record logs when a session starts and ends.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
traffic-shaper	Traffic shaper.	string	Maximum length: 35							
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35							
per-ip-shaper	Per IP traffic shaper.	string	Maximum length: 35							
fixedport	Enable/disable fixed port for this policy.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable fixed port for this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable fixed port for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable fixed port for this policy.	<i>disable</i>	Disable fixed port for this policy.			
Option	Description									
<i>enable</i>	Enable fixed port for this policy.									
<i>disable</i>	Disable fixed port for this policy.									
tcp-mss-sender	TCP Maximum Segment Size value of sender .	integer	Minimum value: 0 Maximum value: 65535	0						
tcp-mss-receiver	TCP Maximum Segment Size value of receiver	integer	Minimum value: 0 Maximum value: 65535	0						
comments	Comment.	var-string	Maximum length: 1023							
ippool	Enable/disable use of IP Pools for source NAT.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of IP Pools for source NAT.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of IP Pools for source NAT.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of IP Pools for source NAT.	<i>disable</i>	Disable use of IP Pools for source NAT.			
Option	Description									
<i>enable</i>	Enable use of IP Pools for source NAT.									
<i>disable</i>	Disable use of IP Pools for source NAT.									
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79							

## config firewall proxy-policy

Configure proxy policies.

```
config firewall proxy-policy
  Description: Configure proxy policies.
  edit <policyid>
    set uuid {uuid}
    set name {string}
    set proxy [explicit-web|transparent-web|...]
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set poolname <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set internet-service [enable|disable]
    set internet-service-negate [enable|disable]
    set internet-service-name <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
```

```

set service <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set dstaddr-negate [enable|disable]
set service-negate [enable|disable]
set action [accept|deny|...]
set status [enable|disable]
set schedule {string}
set logtraffic [all|utm|...]
set session-ttl {integer}
set srcaddr6 <name1>, <name2>, ...
set dstaddr6 <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set http-tunnel-auth [enable|disable]
set ssh-policy-redirect [enable|disable]
set webproxy-forward-server {string}
set webproxy-profile {string}
set transparent [enable|disable]
set disclaimer [disable|domain|...]
set utm-status [enable|disable]
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set webfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set icap-profile {string}
set cifs-profile {string}
set waf-profile {string}
set ssh-filter-profile {string}
set replacemsg-override-group {string}
set logtraffic-start [enable|disable]
set comments {var-string}
set redirect-url {var-string}
set decrypted-traffic-mirror {string}
next
end

```

## config firewall proxy-policy

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
name	Policy name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default												
proxy	Type of explicit proxy.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>explicit-web</i></td> <td>Explicit Web Proxy</td> </tr> <tr> <td><i>transparent-web</i></td> <td>Transparent Web Proxy</td> </tr> <tr> <td><i>ftp</i></td> <td>Explicit FTP Proxy</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH Proxy</td> </tr> <tr> <td><i>ssh-tunnel</i></td> <td>SSH Tunnel</td> </tr> </tbody> </table>	Option	Description	<i>explicit-web</i>	Explicit Web Proxy	<i>transparent-web</i>	Transparent Web Proxy	<i>ftp</i>	Explicit FTP Proxy	<i>ssh</i>	SSH Proxy	<i>ssh-tunnel</i>	SSH Tunnel			
Option	Description															
<i>explicit-web</i>	Explicit Web Proxy															
<i>transparent-web</i>	Transparent Web Proxy															
<i>ftp</i>	Explicit FTP Proxy															
<i>ssh</i>	SSH Proxy															
<i>ssh-tunnel</i>	SSH Tunnel															
srcintf <name>	Source interface names. Interface name.	string	Maximum length: 79													
dstintf <name>	Destination interface names. Interface name.	string	Maximum length: 79													
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79													
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79													
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79													
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of Internet Services in policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of Internet Services in policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.									
Option	Description															
<i>enable</i>	Enable use of Internet Services in policy.															
<i>disable</i>	Disable use of Internet Services in policy.															
internet-service-negate	When enabled, Internet Services match against any internet service EXCEPT the selected Internet Service.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated Internet Service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated Internet Service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.									
Option	Description															
<i>enable</i>	Enable negated Internet Service match.															
<i>disable</i>	Disable negated Internet Service match.															
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79													



Parameter	Description	Type	Size	Default						
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
service <name>	Name of service objects. Service name.	string	Maximum length: 79							
srcaddr-negate	When enabled, source addresses match against any address EXCEPT the specified source addresses.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable destination address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable destination address negate.			
Option	Description									
<i>enable</i>	Enable source address negate.									
<i>disable</i>	Disable destination address negate.									
dstaddr-negate	When enabled, destination addresses match against any address EXCEPT the specified destination addresses.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source address negate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable destination address negate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable destination address negate.			
Option	Description									
<i>enable</i>	Enable source address negate.									
<i>disable</i>	Disable destination address negate.									
service-negate	When enabled, services match against any service EXCEPT the specified destination services.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negated service match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negated service match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.			
Option	Description									
<i>enable</i>	Enable negated service match.									
<i>disable</i>	Disable negated service match.									
action	Accept or deny traffic matching the policy parameters.	option	-	deny						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Action accept.</td> </tr> <tr> <td><i>deny</i></td> <td>Action deny.</td> </tr> <tr> <td><i>redirect</i></td> <td>Action redirect.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Action accept.	<i>deny</i>	Action deny.	<i>redirect</i>	Action redirect.			
Option	Description											
<i>accept</i>	Action accept.											
<i>deny</i>	Action deny.											
<i>redirect</i>	Action redirect.											
status	Enable/disable the active status of the policy.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
schedule	Name of schedule object.	string	Maximum length: 35									
logtraffic	Enable/disable logging traffic through the policy.	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions.</td> </tr> <tr> <td><i>utm</i></td> <td>UTM event and matched application traffic log.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable traffic and application log.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions.	<i>utm</i>	UTM event and matched application traffic log.	<i>disable</i>	Disable traffic and application log.			
Option	Description											
<i>all</i>	Log all sessions.											
<i>utm</i>	UTM event and matched application traffic log.											
<i>disable</i>	Disable traffic and application log.											
session-ttl	TTL in seconds for sessions accepted by this policy .	integer	Minimum value: 300 Maximum value: 2764800	0								
srcaddr6 <name>	IPv6 source address objects. Address name.	string	Maximum length: 79									
dstaddr6 <name>	IPv6 destination address objects. Address name.	string	Maximum length: 79									
groups <name>	Names of group objects. Group name.	string	Maximum length: 79									
users <name>	Names of user objects. Group name.	string	Maximum length: 79									
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-	disable								

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSH policy redirect.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSH policy redirect.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSH policy redirect.	<i>disable</i>	Disable SSH policy redirect.							
Option	Description													
<i>enable</i>	Enable SSH policy redirect.													
<i>disable</i>	Disable SSH policy redirect.													
webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63											
webproxy-profile	Name of web proxy profile.	string	Maximum length: 63											
transparent	Enable to use the IP address of the client to connect to the server.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of IP address of client to connect to server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of IP address of client to connect to server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of IP address of client to connect to server.	<i>disable</i>	Disable use of IP address of client to connect to server.							
Option	Description													
<i>enable</i>	Enable use of IP address of client to connect to server.													
<i>disable</i>	Disable use of IP address of client to connect to server.													
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable disclaimer.</td> </tr> <tr> <td><i>domain</i></td> <td>Display disclaimer for domain</td> </tr> <tr> <td><i>policy</i></td> <td>Display disclaimer for policy</td> </tr> <tr> <td><i>user</i></td> <td>Display disclaimer for current user</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable disclaimer.	<i>domain</i>	Display disclaimer for domain	<i>policy</i>	Display disclaimer for policy	<i>user</i>	Display disclaimer for current user			
Option	Description													
<i>disable</i>	Disable disclaimer.													
<i>domain</i>	Display disclaimer for domain													
<i>policy</i>	Display disclaimer for policy													
<i>user</i>	Display disclaimer for current user													
utm-status	Enable the use of UTM profiles/sensors/lists.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>single</i></td> <td>Do not allow security profile groups.</td> </tr> <tr> <td><i>group</i></td> <td>Allow security profile groups.</td> </tr> </tbody> </table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.			
Option	Description									
<i>single</i>	Do not allow security profile groups.									
<i>group</i>	Allow security profile groups.									
profile-group	Name of profile group.	string	Maximum length: 35							
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default						
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35							
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35							
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35							
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35							
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35							
application-list	Name of an existing Application list.	string	Maximum length: 35							
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35							
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35							
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35							
replacemsg-override-group	Authentication replacement message override group.	string	Maximum length: 35							
logtraffic-start	Enable/disable policy log traffic start.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
comments	Optional comments.	var-string	Maximum length: 1023							
redirect-url	Redirect URL for further explicit web proxy processing.	var-string	Maximum length: 1023							
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							

## config firewall dnstranslation

Configure DNS translation.

```
config firewall dnstranslation
  Description: Configure DNS translation.
  edit <id>
    set src {ipv4-address}
    set dst {ipv4-address}
    set netmask {ipv4-netmask}
  next
end
```

## config firewall dnstranslation

Parameter	Description	Type	Size	Default
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255

## config firewall multicast-policy

Configure multicast NAT policies.

```
config firewall multicast-policy
  Description: Configure multicast NAT policies.
  edit <id>
    set uuid {uuid}
    set name {string}
    set comments {var-string}
    set status [enable|disable]
    set logtraffic [enable|disable]
    set srcintf {string}
    set dstintf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set snat [enable|disable]
    set snat-ip {ipv4-address}
    set dnat {ipv4-address-any}
    set action [accept|deny]
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set auto-asic-offload [enable|disable]
  next
end
```

## config firewall multicast-policy

Parameter	Description	Type	Size	Default						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
name	Policy name.	string	Maximum length: 35							
comments	Comment.	var-string	Maximum length: 1023							
status	Enable/disable this policy.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging traffic accepted by this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging traffic accepted by this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging traffic accepted by this policy.	<i>disable</i>	Disable logging traffic accepted by this policy.			
Option	Description									
<i>enable</i>	Enable logging traffic accepted by this policy.									
<i>disable</i>	Disable logging traffic accepted by this policy.									
srcintf	Source interface name.	string	Maximum length: 35							
dstintf	Destination interface name.	string	Maximum length: 35							
srcaddr <name>	Source address objects. Source address objects.	string	Maximum length: 79							
dstaddr <name>	Destination address objects. Destination address objects.	string	Maximum length: 79							
snat	Enable/disable substitution of the outgoing interface IP address for the original source IP address (called source NAT or SNAT).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source NAT.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source NAT.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source NAT.	<i>disable</i>	Disable source NAT.			
Option	Description									
<i>enable</i>	Enable source NAT.									
<i>disable</i>	Disable source NAT.									
snat-ip	IPv4 address to be used as the source address for NATed traffic.	ipv4-address	Not Specified	0.0.0.0						
dnat	IPv4 DNAT address used for multicast destination addresses.	ipv4-address-any	Not Specified	0.0.0.0						
action	Accept or deny traffic matching the policy.	option	-	accept						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Accept traffic matching the policy.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny or block traffic matching the policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Accept traffic matching the policy.	<i>deny</i>	Deny or block traffic matching the policy.			
Option	Description									
<i>accept</i>	Accept traffic matching the policy.									
<i>deny</i>	Deny or block traffic matching the policy.									
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
start-port	Integer value for starting TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	65535
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable

Option	Description
<i>enable</i>	Enable hardware acceleration offloading.
<i>disable</i>	Disable offloading for hardware acceleration.

## config firewall multicast-policy6

Configure IPv6 multicast NAT policies.

```
config firewall multicast-policy6
  Description: Configure IPv6 multicast NAT policies.
  edit <id>
    set status [enable|disable]
    set name {string}
    set logtraffic [enable|disable]
    set srcintf {string}
    set dstintf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set action [accept|deny]
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set auto-asic-offload [enable|disable]
  next
end
```

## config firewall multicast-policy6

Parameter	Description	Type	Size	Default
status	Enable/disable this policy.	option	-	enable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
name	Policy name.	string	Maximum length: 35							
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging traffic accepted by this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging traffic accepted by this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging traffic accepted by this policy.	<i>disable</i>	Disable logging traffic accepted by this policy.			
Option	Description									
<i>enable</i>	Enable logging traffic accepted by this policy.									
<i>disable</i>	Disable logging traffic accepted by this policy.									
srcintf	IPv6 source interface name.	string	Maximum length: 35							
dstintf	IPv6 destination interface name.	string	Maximum length: 35							
srcaddr <name>	IPv6 source address name. Address name.	string	Maximum length: 79							
dstaddr <name>	IPv6 destination address name. Address name.	string	Maximum length: 79							
action	Accept or deny traffic matching the policy.	option	-	accept						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Accept.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Accept.	<i>deny</i>	Deny.			
Option	Description									
<i>accept</i>	Accept.									
<i>deny</i>	Deny.									
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0						
start-port	Integer value for starting TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	1						

Parameter	Description	Type	Size	Default
end-port	Integer value for ending TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	65535
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable

Option	Description
<i>enable</i>	Enable offloading policy traffic for hardware acceleration.
<i>disable</i>	Disable offloading policy traffic for hardware acceleration.

## config firewall interface-policy

Configure IPv4 interface policies.

```

config firewall interface-policy
  Description: Configure IPv4 interface policies.
  edit <policyid>
    set status [enable|disable]
    set comments {var-string}
    set logtraffic [all|utm|...]
    set interface {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    set application-list-status [enable|disable]
    set application-list {string}
    set ips-sensor-status [enable|disable]
    set ips-sensor {string}
    set dsri [enable|disable]
    set av-profile-status [enable|disable]
    set av-profile {string}
    set webfilter-profile-status [enable|disable]
    set webfilter-profile {string}
    set emailfilter-profile-status [enable|disable]
    set emailfilter-profile {string}
    set dlp-sensor-status [enable|disable]
    set dlp-sensor {string}
  next
end

```

## config firewall interface-policy

Parameter	Description	Type	Size	Default
status	Enable/disable this policy.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.					
Option	Description											
<i>enable</i>	Enable this policy.											
<i>disable</i>	Disable this policy.											
comments	Comments.	var-string	Maximum length: 1023									
logtraffic	Logging type to be used in this policy (Options: all   utm   disable, Default: utm).	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
interface	Monitored interface name from available interfaces.	string	Maximum length: 35									
srcaddr <name>	Address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79									
dstaddr <name>	Address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79									
service <name>	Service object from available options. Service name.	string	Maximum length: 79									
application-list-status	Enable/disable application control.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable application control</td> </tr> <tr> <td><i>disable</i></td> <td>Disable application control</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control					
Option	Description											
<i>enable</i>	Enable application control											
<i>disable</i>	Disable application control											
application-list	Application list name.	string	Maximum length: 35									
ips-sensor-status	Enable/disable IPS.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS.							
Option	Description											
<i>enable</i>	Enable IPS.											

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IPS.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IPS.					
Option	Description									
<i>disable</i>	Disable IPS.									
ips-sensor	IPS sensor name.	string	Maximum length: 35							
dsri	Enable/disable DSRI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DSRI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DSRI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
av-profile-status	Enable/disable antivirus.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable antivirus</td> </tr> <tr> <td><i>disable</i></td> <td>Disable antivirus</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus			
Option	Description									
<i>enable</i>	Enable antivirus									
<i>disable</i>	Disable antivirus									
av-profile	Antivirus profile.	string	Maximum length: 35							
webfilter-profile-status	Enable/disable web filtering.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable web filtering.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable web filtering.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable web filtering.	<i>disable</i>	Disable web filtering.			
Option	Description									
<i>enable</i>	Enable web filtering.									
<i>disable</i>	Disable web filtering.									
webfilter-profile	Web filter profile.	string	Maximum length: 35							
emailfilter-profile-status	Enable/disable email filter.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Email filter.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Email filter.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Email filter.	<i>disable</i>	Disable Email filter.			
Option	Description									
<i>enable</i>	Enable Email filter.									
<i>disable</i>	Disable Email filter.									
emailfilter-profile	Email filter profile.	string	Maximum length: 35							
dlp-sensor-status	Enable/disable DLP.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dlp-sensor	DLP sensor name.	string	Maximum length: 35							

## config firewall interface-policy6

Configure IPv6 interface policies.

```

config firewall interface-policy6
  Description: Configure IPv6 interface policies.
  edit <policyid>
    set status [enable|disable]
    set comments {var-string}
    set logtraffic [all|utm|...]
    set interface {string}
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set service6 <name1>, <name2>, ...
    set application-list-status [enable|disable]
    set application-list {string}
    set ips-sensor-status [enable|disable]
    set ips-sensor {string}
    set dsri [enable|disable]
    set av-profile-status [enable|disable]
    set av-profile {string}
    set webfilter-profile-status [enable|disable]
    set webfilter-profile {string}
    set emailfilter-profile-status [enable|disable]
    set emailfilter-profile {string}
    set dlp-sensor-status [enable|disable]
    set dlp-sensor {string}
  next
end

```

## config firewall interface-policy6

Parameter	Description	Type	Size	Default						
status	Enable/disable this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									

Parameter	Description	Type	Size	Default								
comments	Comments.	var-string	Maximum length: 1023									
logtraffic	Logging type to be used in this policy (Options: all   utm   disable, Default: utm).	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
interface	Monitored interface name from available interfaces.	string	Maximum length: 35									
srcaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79									
dstaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79									
service6 <name>	Service name. Address name.	string	Maximum length: 79									
application-list-status	Enable/disable application control.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable application control</td> </tr> <tr> <td><i>disable</i></td> <td>Disable application control</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control					
Option	Description											
<i>enable</i>	Enable application control											
<i>disable</i>	Disable application control											
application-list	Application list name.	string	Maximum length: 35									
ips-sensor-status	Enable/disable IPS.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS.	<i>disable</i>	Disable IPS.					
Option	Description											
<i>enable</i>	Enable IPS.											
<i>disable</i>	Disable IPS.											
ips-sensor	IPS sensor name.	string	Maximum length: 35									
dsri	Enable/disable DSRI.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DSRI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DSRI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
av-profile-status	Enable/disable antivirus.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable antivirus</td> </tr> <tr> <td><i>disable</i></td> <td>Disable antivirus</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus			
Option	Description									
<i>enable</i>	Enable antivirus									
<i>disable</i>	Disable antivirus									
av-profile	Antivirus profile.	string	Maximum length: 35							
webfilter-profile-status	Enable/disable web filtering.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable web filtering.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable web filtering.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable web filtering.	<i>disable</i>	Disable web filtering.			
Option	Description									
<i>enable</i>	Enable web filtering.									
<i>disable</i>	Disable web filtering.									
webfilter-profile	Web filter profile.	string	Maximum length: 35							
emailfilter-profile-status	Enable/disable email filter.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Email filter.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Email filter.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Email filter.	<i>disable</i>	Disable Email filter.			
Option	Description									
<i>enable</i>	Enable Email filter.									
<i>disable</i>	Disable Email filter.									
emailfilter-profile	Email filter profile.	string	Maximum length: 35							
dlp-sensor-status	Enable/disable DLP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dlp-sensor	DLP sensor name.	string	Maximum length: 35							

## config firewall DoS-policy

Configure IPv4 DoS policies.

```
config firewall DoS-policy
  Description: Configure IPv4 DoS policies.
  edit <policyid>
    set status [enable|disable]
    set name {string}
    set comments {var-string}
    set interface {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    config anomaly
      Description: Anomaly name.
      edit <name>
        set status [disable|enable]
        set log [enable|disable]
        set action [pass|block]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
  next
end
```

## config firewall DoS-policy

Parameter	Description	Type	Size	Default						
status	Enable/disable this policy.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
name	Policy name.	string	Maximum length: 35							
comments	Comment.	var-string	Maximum length: 1023							
interface	Incoming interface name from available interfaces.	string	Maximum length: 35							
srcaddr <name>	Source address name from available addresses. Service name.	string	Maximum length: 79							



Parameter	Description	Type	Size	Default
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79	
service <name>	Service object from available options. Service name.	string	Maximum length: 79	

## config anomaly

Parameter	Description	Type	Size	Default						
status	Enable/disable this anomaly.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this status.	<i>enable</i>	Enable this status.			
Option	Description									
<i>disable</i>	Disable this status.									
<i>enable</i>	Enable this status.									
log	Enable/disable anomaly logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
action	Action taken when the threshold is reached.	option	-	pass						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow traffic but record a log message if logging is enabled.</td> </tr> <tr> <td><i>block</i></td> <td>Block traffic if this anomaly is found.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow traffic but record a log message if logging is enabled.	<i>block</i>	Block traffic if this anomaly is found.			
Option	Description									
<i>pass</i>	Allow traffic but record a log message if logging is enabled.									
<i>block</i>	Block traffic if this anomaly is found.									
quarantine	Quarantine method.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
Option	Description									
<i>none</i>	Quarantine is disabled.									
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.					
Option	Description									
<i>disable</i>	Disable quarantine logging.									

Parameter	Description	Type	Size	Default				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable quarantine logging.			
Option	Description							
<i>enable</i>	Enable quarantine logging.							
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0				
threshold (default)	Number of detected instances . Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0				

## config firewall DoS-policy6

Configure IPv6 DoS policies.

```
config firewall DoS-policy6
  Description: Configure IPv6 DoS policies.
  edit <policyid>
    set status [enable|disable]
    set name {string}
    set comments {var-string}
    set interface {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    config anomaly
      Description: Anomaly name.
      edit <name>
        set status [disable|enable]
        set log [enable|disable]
        set action [pass|block]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
  next
end
```

## config firewall DoS-policy6

Parameter	Description	Type	Size	Default						
status	Enable/disable this policy.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
name	Policy name.	string	Maximum length: 35							
comments	Comment.	var-string	Maximum length: 1023							
interface	Incoming interface name from available interfaces.	string	Maximum length: 35							
srcaddr <name>	Source address name from available addresses. Service name.	string	Maximum length: 79							
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79							
service <name>	Service object from available options. Service name.	string	Maximum length: 79							

## config anomaly

Parameter	Description	Type	Size	Default						
status	Enable/disable this anomaly.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable this status.</td></tr><tr><td><i>enable</i></td><td>Enable this status.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable this status.	<i>enable</i>	Enable this status.			
Option	Description									
<i>disable</i>	Disable this status.									
<i>enable</i>	Enable this status.									
log	Enable/disable anomaly logging.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
action	Action taken when the threshold is reached.	option	-	pass						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow traffic but record a log message if logging is enabled.</td> </tr> <tr> <td><i>block</i></td> <td>Block traffic if this anomaly is found.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow traffic but record a log message if logging is enabled.	<i>block</i>	Block traffic if this anomaly is found.			
Option	Description									
<i>pass</i>	Allow traffic but record a log message if logging is enabled.									
<i>block</i>	Block traffic if this anomaly is found.									
quarantine	Quarantine method.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
Option	Description									
<i>none</i>	Quarantine is disabled.									
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
Option	Description									
<i>disable</i>	Disable quarantine logging.									
<i>enable</i>	Enable quarantine logging.									
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0						
threshold (default)	Number of detected instances . Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config firewall sniffer

Configure sniffer.

```
config firewall sniffer
  Description: Configure sniffer.
  edit <id>
    set status [enable|disable]
    set logtraffic [all|utm|...]
    set ipv6 [enable|disable]
    set non-ip [enable|disable]
    set interface {string}
    set host {string}
    set port {string}
```

```

set protocol {string}
set vlan {string}
set application-list-status [enable|disable]
set application-list {string}
set ips-sensor-status [enable|disable]
set ips-sensor {string}
set dsri [enable|disable]
set av-profile-status [enable|disable]
set av-profile {string}
set webfilter-profile-status [enable|disable]
set webfilter-profile {string}
set emailfilter-profile-status [enable|disable]
set emailfilter-profile {string}
set dlp-sensor-status [enable|disable]
set dlp-sensor {string}
set ips-dos-status [enable|disable]
config anomaly
  Description: Configuration method to edit Denial of Service (DoS) anomaly settings.
  edit <name>
    set status [disable|enable]
    set log [enable|disable]
    set action [pass|block]
    set quarantine [none|attacker]
    set quarantine-expiry {user}
    set quarantine-log [disable|enable]
    set threshold {integer}
    set threshold(default) {integer}
  next
end
set max-packet-count {integer}
next
end

```

## config firewall sniffer

Parameter	Description	Type	Size	Default						
status	Enable/disable the active status of the sniffer.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer status.	<i>disable</i>	Disable sniffer status.			
Option	Description									
<i>enable</i>	Enable sniffer status.									
<i>disable</i>	Disable sniffer status.									
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	option	-	utm						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Log all sessions accepted or denied by this policy.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.					
Option	Description									
<i>all</i>	Log all sessions accepted or denied by this policy.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>utm</i></td> <td>Log traffic that has a security profile applied to it.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all logging for this policy.</td> </tr> </tbody> </table>	Option	Description	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description									
<i>utm</i>	Log traffic that has a security profile applied to it.									
<i>disable</i>	Disable all logging for this policy.									
ipv6	Enable/disable sniffing IPv6 packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer for IPv6 packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer for IPv6 packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer for IPv6 packets.	<i>disable</i>	Disable sniffer for IPv6 packets.			
Option	Description									
<i>enable</i>	Enable sniffer for IPv6 packets.									
<i>disable</i>	Disable sniffer for IPv6 packets.									
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer for non-IP packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer for non-IP packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer for non-IP packets.	<i>disable</i>	Disable sniffer for non-IP packets.			
Option	Description									
<i>enable</i>	Enable sniffer for non-IP packets.									
<i>disable</i>	Disable sniffer for non-IP packets.									
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35							
host	Hosts to filter for in sniffer traffic .	string	Maximum length: 63							
port	Ports to sniff .	string	Maximum length: 63							
protocol	Integer value for the protocol type as defined by IANA .	string	Maximum length: 63							
vlan	List of VLANs to sniff.	string	Maximum length: 63							
application-list-status	Enable/disable application control profile.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
application-list	Name of an existing application list.	string	Maximum length: 35							
ips-sensor-status	Enable/disable IPS sensor.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35							
dsri	Enable/disable DSRI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DSRI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DSRI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
av-profile-status	Enable/disable antivirus profile.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
av-profile	Name of an existing antivirus profile.	string	Maximum length: 35							
webfilter-profile-status	Enable/disable web filter profile.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
webfilter-profile	Name of an existing web filter profile.	string	Maximum length: 35							
emailfilter-profile-status	Enable/disable emailfilter.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
dlp-sensor-status	Enable/disable DLP sensor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35							
ips-dos-status	Enable/disable IPS DoS anomaly detection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-packet-count	Maximum packet count .	integer	Minimum value: 1 Maximum value: 10000 **	4000						

\*\* Values may differ between models.

### config anomaly

Parameter	Description	Type	Size	Default						
status	Enable/disable this anomaly.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this status.	<i>enable</i>	Enable this status.			
Option	Description									
<i>disable</i>	Disable this status.									
<i>enable</i>	Enable this status.									
log	Enable/disable anomaly logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
action	Action taken when the threshold is reached.	option	-	pass						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Allow traffic but record a log message if logging is enabled.</td> </tr> <tr> <td><i>block</i></td> <td>Block traffic if this anomaly is found.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow traffic but record a log message if logging is enabled.	<i>block</i>	Block traffic if this anomaly is found.			
Option	Description									
<i>pass</i>	Allow traffic but record a log message if logging is enabled.									
<i>block</i>	Block traffic if this anomaly is found.									
quarantine	Quarantine method.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
Option	Description									
<i>none</i>	Quarantine is disabled.									
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
Option	Description									
<i>disable</i>	Disable quarantine logging.									
<i>enable</i>	Enable quarantine logging.									
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0						
threshold (default)	Number of detected instances . Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config firewall central-snat-map

Configure IPv4 and IPv6 central SNAT policies.

```
config firewall central-snat-map
  Description: Configure IPv4 and IPv6 central SNAT policies.
  edit <policyid>
    set uuid {uuid}
    set status [enable|disable]
    set type [ipv4|ipv6]
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set orig-addr <name1>, <name2>, ...
    set orig-addr6 <name1>, <name2>, ...
```

```

set dst-addr <name1>, <name2>, ...
set dst-addr6 <name1>, <name2>, ...
set protocol {integer}
set orig-port {user}
set nat [disable|enable]
set nat-ippool <name1>, <name2>, ...
set nat-ippool6 <name1>, <name2>, ...
set nat-port {user}
set comments {var-string}
next
end

```

## config firewall central-snat-map

Parameter	Description	Type	Size	Default						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
status	Enable/disable the active status of this policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
type	IPv4/IPv6 source NAT.	option	-	ipv4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Perform IPv4 source NAT.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Perform IPv6 source NAT.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	Perform IPv4 source NAT.	<i>ipv6</i>	Perform IPv6 source NAT.			
Option	Description									
<i>ipv4</i>	Perform IPv4 source NAT.									
<i>ipv6</i>	Perform IPv6 source NAT.									
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79							
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79							
orig-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79							
orig-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79							
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79							
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
protocol	Integer value for the protocol type .	integer	Minimum value: 0 Maximum value: 255	0						
orig-port	Original TCP port (1 to 65535, 0 means any port).	user	Not Specified							
nat	Enable/disable source NAT.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable source NAT.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable source NAT.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable source NAT.	<i>enable</i>	Enable source NAT.			
Option	Description									
<i>disable</i>	Disable source NAT.									
<i>enable</i>	Enable source NAT.									
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79							
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IPv6 pool name.	string	Maximum length: 79							
nat-port	Translated port or port range (1 to 65535, 0 means any port).	user	Not Specified							
comments	Comment.	var-string	Maximum length: 1023							

## config firewall ssl setting

SSL proxy settings.

```
config firewall ssl setting
  Description: SSL proxy settings.
  set proxy-connect-timeout {integer}
  set ssl-dh-bits [768|1024|...]
  set ssl-send-empty-frags [enable|disable]
  set no-matching-cipher-action [bypass|drop]
  set cert-cache-capacity {integer}
  set cert-cache-timeout {integer}
  set session-cache-capacity {integer}
  set session-cache-timeout {integer}
  set kxp-queue-threshold {integer}
  set ssl-queue-threshold {integer}
  set abbreviate-handshake [enable|disable]
end
```

## config firewall ssl setting

Parameter	Description	Type	Size	Default										
proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process .	integer	Minimum value: 1 Maximum value: 60	30										
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>768</td> <td>768-bit Diffie-Hellman prime.</td> </tr> <tr> <td>1024</td> <td>1024-bit Diffie-Hellman prime.</td> </tr> <tr> <td>1536</td> <td>1536-bit Diffie-Hellman prime.</td> </tr> <tr> <td>2048</td> <td>2048-bit Diffie-Hellman prime.</td> </tr> </tbody> </table>	Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.			
Option	Description													
768	768-bit Diffie-Hellman prime.													
1024	1024-bit Diffie-Hellman prime.													
1536	1536-bit Diffie-Hellman prime.													
2048	2048-bit Diffie-Hellman prime.													
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV (for SSL 3.0 and TLS 1.0 only).	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Send empty fragments.</td> </tr> <tr> <td>disable</td> <td>Do not send empty fragments.</td> </tr> </tbody> </table>	Option	Description	enable	Send empty fragments.	disable	Do not send empty fragments.							
Option	Description													
enable	Send empty fragments.													
disable	Do not send empty fragments.													
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-	bypass										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>bypass</td> <td>Bypass connection.</td> </tr> <tr> <td>drop</td> <td>Drop connection.</td> </tr> </tbody> </table>	Option	Description	bypass	Bypass connection.	drop	Drop connection.							
Option	Description													
bypass	Bypass connection.													
drop	Drop connection.													
cert-cache-capacity	Maximum capacity of the host certificate cache .	integer	Minimum value: 0 Maximum value: 500	200										
cert-cache-timeout	Time limit to keep certificate cache .	integer	Minimum value: 1 Maximum value: 120	10										
session-cache-capacity	Capacity of the SSL session cache .	integer	Minimum value: 0 Maximum value: 1000	500										

Parameter	Description	Type	Size	Default
session-cache-timeout	Time limit to keep SSL session state .	integer	Minimum value: 1 Maximum value: 60	20
kxp-queue-threshold *	Maximum length of the CP KXP queue. When the queue becomes full, the proxy switches cipher functions to the main CPU .	integer	Minimum value: 0 Maximum value: 512	16
ssl-queue-threshold *	Maximum length of the CP SSL queue. When the queue becomes full, the proxy switches cipher functions to the main CPU .	integer	Minimum value: 0 Maximum value: 512	32
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable

Option	Description
<i>enable</i>	Enable use of SSL abbreviated handshake.
<i>disable</i>	Disable use of SSL abbreviated handshake.

\* This parameter may not exist in some models.

## config firewall ssh local-key

SSH proxy local keys.

```
config firewall ssh local-key
  Description: SSH proxy local keys.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end
```

## config firewall ssh local-key

Parameter	Description	Type	Size	Default
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	

Parameter	Description	Type	Size	Default
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local key source type.	option	-	user
	<b>Option</b>	<b>Description</b>		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

## config firewall ssh local-ca

SSH proxy local CA.

```
config firewall ssh local-ca
  Description: SSH proxy local CA.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end
```

## config firewall ssh local-ca

Parameter	Description	Type	Size	Default
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local CA source type.	option	-	user
	<b>Option</b>	<b>Description</b>		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

## config firewall ssh setting

SSH proxy settings.

```
config firewall ssh setting
```

```

Description: SSH proxy settings.
set caname {string}
set untrusted-caname {string}
set hostkey-rsa2048 {string}
set hostkey-dsa1024 {string}
set hostkey-ecdsa256 {string}
set hostkey-ecdsa384 {string}
set hostkey-ecdsa521 {string}
set hostkey-ed25519 {string}
set host-trusted-checking [enable|disable]
end

```

## config firewall ssh setting

Parameter	Description	Type	Size	Default
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35	
untrusted-caname	Untrusted CA certificate used by SSH Inspection.	string	Maximum length: 35	
hostkey-rsa2048	RSA certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-dsa1024	DSA certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa256	ECDSA nid256 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa384	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa521	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ed25519	ED25519 hostkey used by SSH proxy.	string	Maximum length: 35	
host-trusted-checking	Enable/disable host trusted checking.	option	-	enable

Option	Description
<i>enable</i>	Enable host key trusted checking.
<i>disable</i>	Disable host key trusted checking.

## config firewall ssh host-key

SSH proxy host public keys.

```

config firewall ssh host-key
Description: SSH proxy host public keys.

```

```

edit <name>
  set status [trusted|revoked]
  set type [RSA|DSA|...]
  set nid [256|384|...]
  set ip {ipv4-address-any}
  set port {integer}
  set hostname {string}
  set public-key {var-string}
next
end

```

## config firewall ssh host-key

Parameter	Description	Type	Size	Default																		
status	Set the trust status of the public key.	option	-	trusted																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>trusted</i></td> <td>The public key is trusted.</td> </tr> <tr> <td><i>revoked</i></td> <td>The public key is revoked.</td> </tr> </tbody> </table>	Option	Description	<i>trusted</i>	The public key is trusted.	<i>revoked</i>	The public key is revoked.															
Option	Description																					
<i>trusted</i>	The public key is trusted.																					
<i>revoked</i>	The public key is revoked.																					
type	Set the type of the public key.	option	-	RSA																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>RSA</i></td> <td>The type of the public key is RSA.</td> </tr> <tr> <td><i>DSA</i></td> <td>The type of the public key is DSA.</td> </tr> <tr> <td><i>ECDSA</i></td> <td>The type of the public key is ECDSA.</td> </tr> <tr> <td><i>ED25519</i></td> <td>The type of the public key is ED25519.</td> </tr> <tr> <td><i>RSA-CA</i></td> <td>The type of the public key is from RSA CA.</td> </tr> <tr> <td><i>DSA-CA</i></td> <td>The type of the public key is from DSA CA.</td> </tr> <tr> <td><i>ECDSA-CA</i></td> <td>The type of the public key is from ECDSA CA.</td> </tr> <tr> <td><i>ED25519-CA</i></td> <td>The type of the public key is from ED25519 CA.</td> </tr> </tbody> </table>	Option	Description	<i>RSA</i>	The type of the public key is RSA.	<i>DSA</i>	The type of the public key is DSA.	<i>ECDSA</i>	The type of the public key is ECDSA.	<i>ED25519</i>	The type of the public key is ED25519.	<i>RSA-CA</i>	The type of the public key is from RSA CA.	<i>DSA-CA</i>	The type of the public key is from DSA CA.	<i>ECDSA-CA</i>	The type of the public key is from ECDSA CA.	<i>ED25519-CA</i>	The type of the public key is from ED25519 CA.			
Option	Description																					
<i>RSA</i>	The type of the public key is RSA.																					
<i>DSA</i>	The type of the public key is DSA.																					
<i>ECDSA</i>	The type of the public key is ECDSA.																					
<i>ED25519</i>	The type of the public key is ED25519.																					
<i>RSA-CA</i>	The type of the public key is from RSA CA.																					
<i>DSA-CA</i>	The type of the public key is from DSA CA.																					
<i>ECDSA-CA</i>	The type of the public key is from ECDSA CA.																					
<i>ED25519-CA</i>	The type of the public key is from ED25519 CA.																					
nid	Set the nid of the ECDSA key.	option	-	256																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>256</i></td> <td>The NID is ecdsa-sha2-nistp256.</td> </tr> <tr> <td><i>384</i></td> <td>The NID is ecdsa-sha2-nistp384.</td> </tr> <tr> <td><i>521</i></td> <td>The NID is ecdsa-sha2-nistp521.</td> </tr> </tbody> </table>	Option	Description	<i>256</i>	The NID is ecdsa-sha2-nistp256.	<i>384</i>	The NID is ecdsa-sha2-nistp384.	<i>521</i>	The NID is ecdsa-sha2-nistp521.													
Option	Description																					
<i>256</i>	The NID is ecdsa-sha2-nistp256.																					
<i>384</i>	The NID is ecdsa-sha2-nistp384.																					
<i>521</i>	The NID is ecdsa-sha2-nistp521.																					
ip	IP address of the SSH server.	ipv4-address-any	Not Specified	0.0.0.0																		



Parameter	Description	Type	Size	Default
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295	22
hostname	Hostname of the SSH server.	string	Maximum length: 255	
public-key	SSH public key.	var-string	Maximum length: 32768	

## config firewall ip-translation

Configure firewall IP-translation.

```
config firewall ip-translation
  Description: Configure firewall IP-translation.
  edit <transid>
    set type {option}
    set startip {ipv4-address-any}
    set endip {ipv4-address-any}
    set map-startip {ipv4-address-any}
  next
end
```

## config firewall ip-translation

Parameter	Description	Type	Size	Default				
type	IP translation type (option: Sctp).	option	-	SCTP				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>SCTP</td> <td>SCTP</td> </tr> </tbody> </table>	Option	Description	SCTP	SCTP			
Option	Description							
SCTP	SCTP							
startip	First IPv4 address .	ipv4-address-any	Not Specified	0.0.0.0				
endip	Final IPv4 address .	ipv4-address-any	Not Specified	0.0.0.0				
map-startip	Address to be used as the starting point for translation in the range .	ipv4-address-any	Not Specified	0.0.0.0				

## config firewall ipv6-eh-filter

Configure IPv6 extension header filter.

```
config firewall ipv6-eh-filter
  Description: Configure IPv6 extension header filter.
  set hop-opt [enable|disable]
  set dest-opt [enable|disable]
  set hdopt-type {integer}
  set routing [enable|disable]
  set routing-type {integer}
  set fragment [enable|disable]
  set auth [enable|disable]
  set no-next [enable|disable]
end
```

## config firewall ipv6-eh-filter

Parameter	Description	Type	Size	Default						
hop-opt	Enable/disable blocking packets with the Hop-by-Hop Options header .	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable blocking packets with the Hop-by-Hop Options header.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with the Hop-by-Hop Options header.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable blocking packets with the Hop-by-Hop Options header.	<i>disable</i>	Disable blocking packets with the Hop-by-Hop Options header.			
Option	Description									
<i>enable</i>	Enable blocking packets with the Hop-by-Hop Options header.									
<i>disable</i>	Disable blocking packets with the Hop-by-Hop Options header.									
dest-opt	Enable/disable blocking packets with Destination Options headers .	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable blocking packets with Destination Options headers.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with Destination Options headers.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable blocking packets with Destination Options headers.	<i>disable</i>	Disable blocking packets with Destination Options headers.			
Option	Description									
<i>enable</i>	Enable blocking packets with Destination Options headers.									
<i>disable</i>	Disable blocking packets with Destination Options headers.									
hdopt-type	Block specific Hop-by-Hop and/or Destination Option types (max. 7 types, each between 0 and 255).	integer	Minimum value: 0 Maximum value: 255							
routing	Enable/disable blocking packets with Routing headers .	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Block packets with Routing headers.</td></tr><tr><td><i>disable</i></td><td>Allow packets with Routing headers.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Block packets with Routing headers.	<i>disable</i>	Allow packets with Routing headers.			
Option	Description									
<i>enable</i>	Block packets with Routing headers.									
<i>disable</i>	Allow packets with Routing headers.									

Parameter	Description	Type	Size	Default						
routing-type	Block specific Routing header types .	integer	Minimum value: 0 Maximum value: 255	0						
fragment	Enable/disable blocking packets with the Fragment header .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Block packets with the Fragment header.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow packets with the Fragment header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Block packets with the Fragment header.	<i>disable</i>	Allow packets with the Fragment header.			
Option	Description									
<i>enable</i>	Block packets with the Fragment header.									
<i>disable</i>	Allow packets with the Fragment header.									
auth	Enable/disable blocking packets with the Authentication header .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Block packets with the Authentication header.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow packets with the Authentication header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Block packets with the Authentication header.	<i>disable</i>	Allow packets with the Authentication header.			
Option	Description									
<i>enable</i>	Block packets with the Authentication header.									
<i>disable</i>	Allow packets with the Authentication header.									
no-next	Enable/disable blocking packets with the No Next header	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Block packets with the No Next header.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow packets with the No Next header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Block packets with the No Next header.	<i>disable</i>	Allow packets with the No Next header.			
Option	Description									
<i>enable</i>	Block packets with the No Next header.									
<i>disable</i>	Allow packets with the No Next header.									

## config firewall iprope list

list

```
config firewall iprope list
  Description: list
  set <group_number> {string}
end
```

## config firewall iprope list

Parameter	Description	Type	Size	Default
<group_number>	Number, hexadecimal.	string	Maximum length: -1	

---

## config firewall iprope appctrl list

List application control policies.

```
config firewall iprope appctrl list
  Description: List application control policies.
end
```

## config firewall iprope appctrl status

Application control policy status.

```
config firewall iprope appctrl status
  Description: Application control policy status.
end
```

## config firewall proute

List policy routing.

```
config firewall proute
  Description: List policy routing.
  set <policy route id> {string}
end
```

## config firewall proute

Parameter	Description	Type	Size	Default
<policy route id>	Number.	string	Maximum length: -1	

## config firewall proute6

List IPv6 policy routing.

```
config firewall proute6
  Description: List IPv6 policy routing.
end
```

## ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 381](#)

### config ftp-proxy explicit

Configure explicit FTP proxy settings.

```
config ftp-proxy explicit
  Description: Configure explicit FTP proxy settings.
  set status [enable|disable]
  set incoming-port {user}
  set incoming-ip {ipv4-address-any}
  set outgoing-ip {ipv4-address-any}
  set sec-default-action [accept|deny]
  set ssl [enable|disable]
  set ssl-cert {string}
  set ssl-dh-bits [768|1024|...]
  set ssl-algorithm [high|medium|...]
end
```

### config ftp-proxy explicit

Parameter	Description	Type	Size	Default						
status	Enable/disable the explicit FTP proxy.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable the explicit FTP proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit FTP proxy.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable the explicit FTP proxy.	<i>disable</i>	Disable the explicit FTP proxy.			
Option	Description									
<i>enable</i>	Enable the explicit FTP proxy.									
<i>disable</i>	Disable the explicit FTP proxy.									
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified							
incoming-ip	Accept incoming FTP requests from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0						
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified							
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-	deny						

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not</td> </tr> <tr> <td><i>deny</i></td> <td>Deny requests unless there is a matching explicit FTP proxy policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not	<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.							
Option	Description													
<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not													
<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.													
ssl	Enable/disable the explicit FTPS proxy.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the explicit FTPS proxy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the explicit FTPS proxy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the explicit FTPS proxy.	<i>disable</i>	Disable the explicit FTPS proxy.							
Option	Description													
<i>enable</i>	Enable the explicit FTPS proxy.													
<i>disable</i>	Disable the explicit FTPS proxy.													
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35	Fortinet_CA_SSL										
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>768</i></td> <td>768-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1024</i></td> <td>1024-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>1536</i></td> <td>1536-bit Diffie-Hellman prime.</td> </tr> <tr> <td><i>2048</i></td> <td>2048-bit Diffie-Hellman prime.</td> </tr> </tbody> </table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.			
Option	Description													
<i>768</i>	768-bit Diffie-Hellman prime.													
<i>1024</i>	1024-bit Diffie-Hellman prime.													
<i>1536</i>	1536-bit Diffie-Hellman prime.													
<i>2048</i>	2048-bit Diffie-Hellman prime.													
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High encryption. Allow only AES and ChaCha</td> </tr> <tr> <td><i>medium</i></td> <td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.					
Option	Description													
<i>high</i>	High encryption. Allow only AES and ChaCha													
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.													
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													

## hardware

This section includes syntax for the following commands:

- [config hardware nic on page 383](#)
- [config hardware cpu on page 383](#)
- [config hardware status on page 383](#)
- [config hardware memory on page 383](#)

### config hardware status

Hardware status.

```
config hardware status
  Description: Hardware status.
end
```

### config hardware cpu

Display detailed information for all installed CPU(s).

```
config hardware cpu
  Description: Display detailed information for all installed CPU(s).
end
```

### config hardware memory

Display system memory information.

```
config hardware memory
  Description: Display system memory information.
end
```

### config hardware nic

Display NIC information.

```
config hardware nic
  Description: Display NIC information.
  set <nic> {string}
end
```

---

## config hardware nic

Parameter	Description	Type	Size	Default
<nic>	NIC name.	string	Maximum length: -1	



## icap

This section includes syntax for the following commands:

- [config icap profile on page 386](#)
- [config icap server on page 385](#)

### config icap server

Configure ICAP servers.

```
config icap server
  Description: Configure ICAP servers.
  edit <name>
    set ip-version [4|6]
    set ip-address {ipv4-address-any}
    set ip6-address {ipv6-address}
    set port {integer}
    set max-connections {integer}
  next
end
```

### config icap server

Parameter	Description	Type	Size	Default		
ip-version	IP version.	option	-	4		
					Option	Description
					4	IPv4 ICAP address.
6	IPv6 ICAP address.					
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0		
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::		
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344		

Parameter	Description	Type	Size	Default
max-connections	Maximum number of concurrent connections to ICAP server. Must not be less than wad-worker-count.	integer	Minimum value: 1 Maximum value: 65535	100

## config icap profile

Configure ICAP profiles.

```

config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    set replacemsg-group {string}
    set request [disable|enable]
    set response [disable|enable]
    set streaming-content-bypass [disable|enable]
    set preview [disable|enable]
    set preview-data-length {integer}
    set request-server {string}
    set response-server {string}
    set request-failure [error|bypass]
    set response-failure [error|bypass]
    set request-path {string}
    set response-path {string}
    set methods {option1}, {option2}, ...
    set response-req-hdr [disable|enable]
    set respmod-default-action [forward|bypass]
  config icap-headers
    Description: Configure ICAP forwarded request headers.
    edit <id>
      set name {string}
      set content {string}
      set base64-encoding [disable|enable]
    next
  end
  config respmod-forward-rules
    Description: ICAP response mode forward rules.
    edit <name>
      set host {string}
      config header-group
        Description: HTTP header group.
        edit <id>
          set header-name {string}
          set header {string}
          set case-sensitivity [disable|enable]
        next
      end
      set action [forward|bypass]
      set http-esp-status-code <code1>, <code2>, ...
    next
  end
next

```

end

## config icap profile

Parameter	Description	Type	Size	Default						
replacemsg-group	Replacement message group.	string	Maximum length: 35							
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable HTTP request passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP request passing to ICAP server.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable HTTP request passing to ICAP server.	<i>enable</i>	Enable HTTP request passing to ICAP server.			
Option	Description									
<i>disable</i>	Disable HTTP request passing to ICAP server.									
<i>enable</i>	Enable HTTP request passing to ICAP server.									
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable HTTP response passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP response passing to ICAP server.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable HTTP response passing to ICAP server.	<i>enable</i>	Enable HTTP response passing to ICAP server.			
Option	Description									
<i>disable</i>	Disable HTTP response passing to ICAP server.									
<i>enable</i>	Enable HTTP response passing to ICAP server.									
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable bypassing of ICAP server for streaming content.</td></tr><tr><td><i>enable</i></td><td>Enable bypassing of ICAP server for streaming content.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable bypassing of ICAP server for streaming content.	<i>enable</i>	Enable bypassing of ICAP server for streaming content.			
Option	Description									
<i>disable</i>	Disable bypassing of ICAP server for streaming content.									
<i>enable</i>	Enable bypassing of ICAP server for streaming content.									
preview	Enable/disable preview of data to ICAP server.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable preview of data to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable preview of data to ICAP server.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable preview of data to ICAP server.	<i>enable</i>	Enable preview of data to ICAP server.			
Option	Description									
<i>disable</i>	Disable preview of data to ICAP server.									
<i>enable</i>	Enable preview of data to ICAP server.									
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096	0						
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default														
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 35															
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>error</i></td> <td>Error.</td> </tr> <tr> <td><i>bypass</i></td> <td>Bypass.</td> </tr> </tbody> </table>	Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.											
Option	Description																	
<i>error</i>	Error.																	
<i>bypass</i>	Bypass.																	
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-	error														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>error</i></td> <td>Error.</td> </tr> <tr> <td><i>bypass</i></td> <td>Bypass.</td> </tr> </tbody> </table>	Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.											
Option	Description																	
<i>error</i>	Error.																	
<i>bypass</i>	Bypass.																	
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127															
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127															
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-	delete get head options post put trace other														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>delete</i></td> <td>Forward HTTP request or response with DELETE method to ICAP server for further processing.</td> </tr> <tr> <td><i>get</i></td> <td>Forward HTTP request or response with GET method to ICAP server for further processing.</td> </tr> <tr> <td><i>head</i></td> <td>Forward HTTP request or response with HEAD method to ICAP server for further processing.</td> </tr> <tr> <td><i>options</i></td> <td>Forward HTTP request or response with OPTIONS method to ICAP server for further processing.</td> </tr> <tr> <td><i>post</i></td> <td>Forward HTTP request or response with POST method to ICAP server for further processing.</td> </tr> <tr> <td><i>put</i></td> <td>Forward HTTP request or response with PUT method to ICAP server for further processing.</td> </tr> </tbody> </table>	Option	Description	<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.	<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.	<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.	<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.	<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.	<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.			
Option	Description																	
<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.																	
<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.																	
<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.																	
<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.																	
<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.																	
<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.																	

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>trace</i></td> <td>Forward HTTP request or response with TRACE method to ICAP server for further processing.</td> </tr> <tr> <td><i>other</i></td> <td>Forward HTTP request or response with All other methods to ICAP server for further processing.</td> </tr> </tbody> </table>	Option	Description	<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.	<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.			
Option	Description									
<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.									
<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.									
response-req-hdr	Enable/disable addition of req-hdr for ICAP response modification (respmod) processing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add req-hdr for response modification (respmod) processing.</td> </tr> <tr> <td><i>enable</i></td> <td>Add req-hdr for response modification (respmod) processing.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.	<i>enable</i>	Add req-hdr for response modification (respmod) processing.			
Option	Description									
<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.									
<i>enable</i>	Add req-hdr for response modification (respmod) processing.									
respmod-default-action	Default action to ICAP response modification (respmod) processing.	option	-	forward						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>forward</i></td> <td>Forward response to icap server unless a rule specifies not to.</td> </tr> <tr> <td><i>bypass</i></td> <td>Don't forward request to icap server unless a rule specifies to forward the request.</td> </tr> </tbody> </table>	Option	Description	<i>forward</i>	Forward response to icap server unless a rule specifies not to.	<i>bypass</i>	Don't forward request to icap server unless a rule specifies to forward the request.			
Option	Description									
<i>forward</i>	Forward response to icap server unless a rule specifies not to.									
<i>bypass</i>	Don't forward request to icap server unless a rule specifies to forward the request.									

### config icap-headers

Parameter	Description	Type	Size	Default						
name	HTTP forwarded header name.	string	Maximum length: 79							
content	HTTP header content.	string	Maximum length: 255							
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of base64 encoding of HTTP content.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of base64 encoding of HTTP content.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of base64 encoding of HTTP content.	<i>enable</i>	Enable use of base64 encoding of HTTP content.			
Option	Description									
<i>disable</i>	Disable use of base64 encoding of HTTP content.									
<i>enable</i>	Enable use of base64 encoding of HTTP content.									

## config respmod-forward-rules

Parameter	Description	Type	Size	Default						
host	Address object for the host.	string	Maximum length: 79							
action	Action to be taken for ICAP server.	option	-	forward						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>forward</i></td> <td>Forward request to ICAP server when this rule is matched.</td> </tr> <tr> <td><i>bypass</i></td> <td>Don't forward request to ICAP server when this rule is matched.</td> </tr> </tbody> </table>	Option	Description	<i>forward</i>	Forward request to ICAP server when this rule is matched.	<i>bypass</i>	Don't forward request to ICAP server when this rule is matched.			
Option	Description									
<i>forward</i>	Forward request to ICAP server when this rule is matched.									
<i>bypass</i>	Don't forward request to ICAP server when this rule is matched.									
http- resp- status-code <code>	HTTP response status code. HTTP response status code.	integer	Minimum value: 100 Maximum value: 599	0 **						

\*\* Values may differ between models.

## config header-group

Parameter	Description	Type	Size	Default						
header-name	HTTP header.	string	Maximum length: 79							
header	HTTP header regular expression.	string	Maximum length: 255							
case- sensitivity	Enable/disable case sensitivity when matching header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Ignore case when matching header.</td> </tr> <tr> <td><i>enable</i></td> <td>Do not ignore case when matching header.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Ignore case when matching header.	<i>enable</i>	Do not ignore case when matching header.			
Option	Description									
<i>disable</i>	Ignore case when matching header.									
<i>enable</i>	Do not ignore case when matching header.									

## ips

This section includes syntax for the following commands:

- [config ips global on page 401](#)
- [config ips sensor on page 391](#)
- [config ips custom on page 399](#)
- [config ips view-map on page 395](#)
- [config ips rule on page 397](#)
- [config ips rule-settings on page 399](#)
- [config ips session on page 405](#)
- [config ips decoder on page 396](#)
- [config ips settings on page 405](#)

### config ips sensor

Configure IPS sensor.

```
config ips sensor
  Description: Configure IPS sensor.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set block-malicious-url [disable|enable]
    set scan-botnet-connections [disable|block|...]
    set extended-log [enable|disable]
  config entries
    Description: IPS sensor filter.
    edit <id>
      set rule <id1>, <id2>, ...
      set location {user}
      set severity {user}
      set protocol {user}
      set os {user}
      set application {user}
      set cve <cve-entry1>, <cve-entry2>, ...
      set status [disable|enable|...]
      set log [disable|enable]
      set log-packet [disable|enable]
      set log-attack-context [disable|enable]
      set action [pass|block|...]
      set rate-count {integer}
      set rate-duration {integer}
      set rate-mode [periodical|continuous]
      set rate-track [none|src-ip|...]
    config exempt-ip
      Description: Traffic from selected source or destination IP addresses is
        exempt from this signature.
      edit <id>
        set src-ip {ipv4-classnet}
```

```

        set dst-ip {ipv4-classnet}
    next
end
set quarantine [none|attacker]
set quarantine-expiry {user}
set quarantine-log [disable|enable]
next
end
next
end

```

## config ips sensor

Parameter	Description	Type	Size	Default								
comment	Comment.	var-string	Maximum length: 255									
replacemsg-group	Replacement message group.	string	Maximum length: 35									
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable malicious URL blocking.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable malicious URL blocking.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable malicious URL blocking.	<i>enable</i>	Enable malicious URL blocking.					
Option	Description											
<i>disable</i>	Disable malicious URL blocking.											
<i>enable</i>	Enable malicious URL blocking.											
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not scan connections to botnet servers.</td> </tr> <tr> <td><i>block</i></td> <td>Block connections to botnet servers.</td> </tr> <tr> <td><i>monitor</i></td> <td>Log connections to botnet servers.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not scan connections to botnet servers.	<i>block</i>	Block connections to botnet servers.	<i>monitor</i>	Log connections to botnet servers.			
Option	Description											
<i>disable</i>	Do not scan connections to botnet servers.											
<i>block</i>	Block connections to botnet servers.											
<i>monitor</i>	Log connections to botnet servers.											
extended-log	Enable/disable extended logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											



## config entries

Parameter	Description	Type	Size	Default								
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295									
location	Protect client or server traffic.	user	Not Specified	all								
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all								
protocol	Protocols to be examined. set protocol ? lists available protocols. all includes all protocols. other includes all unlisted protocols.	user	Not Specified	all								
os	Operating systems to be protected. all includes all operating systems. other includes all unlisted operating systems.	user	Not Specified	all								
application	Applications to be protected. set application ? lists available applications. all includes all applications. other includes all unlisted applications.	user	Not Specified	all								
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor CVE IDs or CVE wildcards.	string	Maximum length: 19									
status	Status of the signatures included in filter. default enables the filter and only use filters with default status of enable. Filters with default status of disable will not be used.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status of selected rules.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status of selected rules.</td> </tr> <tr> <td><i>default</i></td> <td>Default.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status of selected rules.	<i>enable</i>	Enable status of selected rules.	<i>default</i>	Default.			
Option	Description											
<i>disable</i>	Disable status of selected rules.											
<i>enable</i>	Enable status of selected rules.											
<i>default</i>	Default.											
log	Enable/disable logging of signatures included in filter.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of selected rules.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of selected rules.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of selected rules.	<i>enable</i>	Enable logging of selected rules.					
Option	Description											
<i>disable</i>	Disable logging of selected rules.											
<i>enable</i>	Enable logging of selected rules.											

Parameter	Description	Type	Size	Default										
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet logging of selected rules.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable packet logging of selected rules.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet logging of selected rules.	<i>enable</i>	Enable packet logging of selected rules.							
Option	Description													
<i>disable</i>	Disable packet logging of selected rules.													
<i>enable</i>	Enable packet logging of selected rules.													
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of detailed attack context.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of detailed attack context.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of detailed attack context.	<i>enable</i>	Enable logging of detailed attack context.							
Option	Description													
<i>disable</i>	Disable logging of detailed attack context.													
<i>enable</i>	Enable logging of detailed attack context.													
action	Action taken with traffic in which signatures are detected.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow matching traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block or drop matching traffic.</td> </tr> <tr> <td><i>reset</i></td> <td>Reset sessions for matching traffic.</td> </tr> <tr> <td><i>default</i></td> <td>Pass or drop matching traffic, depending on the default action of the signature.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.	<i>reset</i>	Reset sessions for matching traffic.	<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.			
Option	Description													
<i>pass</i>	Pass or allow matching traffic.													
<i>block</i>	Block or drop matching traffic.													
<i>reset</i>	Reset sessions for matching traffic.													
<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.													
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0										
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60										
rate-mode	Rate limit mode.	option	-	continuous										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>periodical</i></td> <td>Allow configured number of packets every rate-duration.</td> </tr> <tr> <td><i>continuous</i></td> <td>Block packets once the rate is reached.</td> </tr> </tbody> </table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.							
Option	Description													
<i>periodical</i>	Allow configured number of packets every rate-duration.													
<i>continuous</i>	Block packets once the rate is reached.													
rate-track	Track the packet protocol field.	option	-	none										

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>none</td> </tr> <tr> <td><i>src-ip</i></td> <td>Source IP.</td> </tr> <tr> <td><i>dest-ip</i></td> <td>Destination IP.</td> </tr> <tr> <td><i>dhcp-client-mac</i></td> <td>DHCP client.</td> </tr> <tr> <td><i>dns-domain</i></td> <td>DNS domain.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
Option	Description															
<i>none</i>	none															
<i>src-ip</i>	Source IP.															
<i>dest-ip</i>	Destination IP.															
<i>dhcp-client-mac</i>	DHCP client.															
<i>dns-domain</i>	DNS domain.															
quarantine	Quarantine method.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Quarantine is disabled.</td> </tr> <tr> <td><i>attacker</i></td> <td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
Option	Description															
<i>none</i>	Quarantine is disabled.															
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.															
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m												
quarantine-log	Enable/disable quarantine logging.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable quarantine logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable quarantine logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.									
Option	Description															
<i>disable</i>	Disable quarantine logging.															
<i>enable</i>	Enable quarantine logging.															

### config exempt-ip

Parameter	Description	Type	Size	Default
src-ip	Source IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0
dst-ip	Destination IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0

### config ips view-map

configure ips view-map

```

config ips view-map
  Description: configure ips view-map
  edit <id>
    set vdom-id {integer}
    set policy-id {integer}
    set id-policy-id {integer}

```

```

    set which [firewall|interface|...]
  next
end

```

## config ips view-map

Parameter	Description	Type	Size	Default
vdom-id	VDOM ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
policy-id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
id-policy-id	ID-based policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
which	Policy.	option	-	firewall

Option	Description
<i>firewall</i>	Firewall policy.
<i>interface</i>	Interface policy.
<i>interface6</i>	Interface policy6.
<i>sniffer</i>	Sniffer policy.
<i>sniffer6</i>	Sniffer policy6.
<i>explicit</i>	explicit proxy policy.

## config ips decoder

Configure IPS decoder.

```

config ips decoder
  Description: Configure IPS decoder.
  edit <name>
    config parameter
      Description: IPS group parameters.
      edit <name>
        set value {string}
      next
    next
  next
end

```

```

    end
  next
end

```

## config parameter

Parameter	Description	Type	Size	Default
value	Parameter value.	string	Maximum length: 199	

## config ips rule

Configure IPS rules.

```

config ips rule
  Description: Configure IPS rules.
  edit <name>
    set status [disable|enable]
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set group {string}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set service {user}
    set rule-id {integer}
    set rev {integer}
    set date {integer}
  config metadata
    Description: Meta data.
    edit <id>
      set metaid {integer}
      set valueid {integer}
    next
  end
next
end

```

## config ips rule

Parameter	Description	Type	Size	Default						
status	Enable/disable status.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									

Parameter	Description	Type	Size	Default						
log	Enable/disable logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.			
Option	Description									
<i>disable</i>	Disable logging.									
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable packet logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.			
Option	Description									
<i>disable</i>	Disable packet logging.									
<i>enable</i>	Enable packet logging.									
action	Action.	option	-	pass						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow matching traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block or drop matching traffic.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.			
Option	Description									
<i>pass</i>	Pass or allow matching traffic.									
<i>block</i>	Block or drop matching traffic.									
group	Group.	string	Maximum length: 63							
severity	Severity.	user	Not Specified							
location	Vulnerable location.	user	Not Specified							
os	Vulnerable operation systems.	user	Not Specified							
application	Vulnerable applications.	user	Not Specified							
service	Vulnerable service.	user	Not Specified							
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0						
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config metadata

Parameter	Description	Type	Size	Default
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config ips rule-settings

Configure IPS rule setting.

```
config ips rule-settings
  Description: Configure IPS rule setting.
  edit <id>
    next
  end
```

## config ips custom

Configure IPS custom signature.

```
config ips custom
  Description: Configure IPS custom signature.
  edit <tag>
    set signature {var-string}
    set rule-id {integer}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set protocol {user}
    set status [disable|enable]
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set comment {string}
  next
end
```

## config ips custom

Parameter	Description	Type	Size	Default						
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095							
rule-id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified							
location	Protect client or server traffic.	user	Not Specified							
os	Operating system(s) that the signature protects. Blank for all operating systems.	user	Not Specified							
application	Applications to be protected. Blank for all applications.	user	Not Specified							
protocol	Protocol(s) that the signature scans. Blank for all protocols.	user	Not Specified							
status	Enable/disable this signature.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
log	Enable/disable logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.			
Option	Description									
<i>disable</i>	Disable logging.									
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet logging.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable packet logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.			
Option	Description									
<i>disable</i>	Disable packet logging.									
<i>enable</i>	Enable packet logging.									
action	Default action (pass or block) for this signature.	option	-	pass						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass or allow matching traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block or drop matching traffic.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.			
Option	Description									
<i>pass</i>	Pass or allow matching traffic.									
<i>block</i>	Block or drop matching traffic.									
comment	Comment.	string	Maximum length: 63							

## config ips global

Configure IPS global parameter.

```

config ips global
  Description: Configure IPS global parameter.
  set fail-open [enable|disable]
  set database [regular|extended]
  set traffic-submit [enable|disable]
  set anomaly-mode [periodical|continuous]
  set session-limit-mode [accurate|heuristic]
  set socket-size {integer}
  set engine-count {integer}
  set sync-session-ttl [enable|disable]
  set np-accel-mode [none|basic]
  set cp-accel-mode [none|basic|...]
  set deep-app-insp-timeout {integer}
  set deep-app-insp-db-limit {integer}
  set exclude-signatures [none|industrial]
  set packet-log-queue-depth {integer}
  set ngfw-max-scan-range {integer}
  config tls-active-probe
    Description: TLS active probe configuration.
    set interface-select-method [auto|sdwan|...]
    set interface {string}
    set vdom {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
  end
end

```

## config ips global

Parameter	Description	Type	Size	Default
fail-open	Enable to allow traffic if the IPS process crashes. Default is disable and IPS traffic is blocked when the IPS process crashes.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS fail open.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS fail open.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS fail open.	<i>disable</i>	Disable IPS fail open.			
Option	Description									
<i>enable</i>	Enable IPS fail open.									
<i>disable</i>	Disable IPS fail open.									
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	regular **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>IPS regular database package.</td> </tr> <tr> <td><i>extended</i></td> <td>IPS extended database package.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	IPS regular database package.	<i>extended</i>	IPS extended database package.			
Option	Description									
<i>regular</i>	IPS regular database package.									
<i>extended</i>	IPS extended database package.									
traffic-submit	Enable/disable submitting attack data found by this FortiGate to FortiGuard.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable traffic submit.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable traffic submit.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable traffic submit.	<i>disable</i>	Disable traffic submit.			
Option	Description									
<i>enable</i>	Enable traffic submit.									
<i>disable</i>	Disable traffic submit.									
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>periodical</i></td> <td>After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.</td> </tr> <tr> <td><i>continuous</i></td> <td>Block packets once an anomaly is detected. Overrides individual anomaly settings.</td> </tr> </tbody> </table>	Option	Description	<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.	<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.			
Option	Description									
<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.									
<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.									
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy ( <i>accurate</i> ) or improved performance ( <i>heuristics</i> ).	option	-	heuristic						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accurate</i></td> <td>Accurately count concurrent sessions, demands more resources.</td> </tr> <tr> <td><i>heuristic</i></td> <td>Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.</td> </tr> </tbody> </table>	Option	Description	<i>accurate</i>	Accurately count concurrent sessions, demands more resources.	<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.			
Option	Description									
<i>accurate</i>	Accurately count concurrent sessions, demands more resources.									
<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.									

Parameter	Description	Type	Size	Default								
socket-size	IPS socket buffer size. Max and default value depend on available memory. Can be changed to tune performance.	integer	Minimum value: 0 Maximum value: 128 **	32 **								
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0								
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of kernel session TTL for IPS sessions.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of kernel session TTL for IPS sessions.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of kernel session TTL for IPS sessions.	<i>disable</i>	Disable use of kernel session TTL for IPS sessions.					
Option	Description											
<i>enable</i>	Enable use of kernel session TTL for IPS sessions.											
<i>disable</i>	Disable use of kernel session TTL for IPS sessions.											
np-accel-mode *	Acceleration mode for IPS processing by NPx processors.	option	-	basic								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>NPx acceleration disabled.</td> </tr> <tr> <td><i>basic</i></td> <td>NPx acceleration enabled.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	NPx acceleration disabled.	<i>basic</i>	NPx acceleration enabled.					
Option	Description											
<i>none</i>	NPx acceleration disabled.											
<i>basic</i>	NPx acceleration enabled.											
cp-accel-mode *	IPS Pattern matching acceleration/offloading to CPx processors.	option	-	advanced								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>CPx acceleration/offloading disabled.</td> </tr> <tr> <td><i>basic</i></td> <td>Offload basic pattern matching to CPx processors.</td> </tr> <tr> <td><i>advanced</i></td> <td>Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	CPx acceleration/offloading disabled.	<i>basic</i>	Offload basic pattern matching to CPx processors.	<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.			
Option	Description											
<i>none</i>	CPx acceleration/offloading disabled.											
<i>basic</i>	Offload basic pattern matching to CPx processors.											
<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.											
deep-app-insp-timeout	Timeout for Deep application inspection .	integer	Minimum value: 0 Maximum value: 2147483647	0								
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database	integer	Minimum value: 0 Maximum value: 2147483647	0								

Parameter	Description	Type	Size	Default						
exclude-signatures	Excluded signatures.	option	-	industrial						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No signatures excluded.</td> </tr> <tr> <td><i>industrial</i></td> <td>Exclude industrial signatures.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No signatures excluded.	<i>industrial</i>	Exclude industrial signatures.			
Option	Description									
<i>none</i>	No signatures excluded.									
<i>industrial</i>	Exclude industrial signatures.									
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128						
ngfw-max-scan-range	NGFW policy-mode app detection threshold.	integer	Minimum value: 0 Maximum value: 4294967295	4096						

\* This parameter may not exist in some models.

\*\* Values may differ between models.

### config tls-active-probe

Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31									
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0								
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified	::								

## config ips settings

Configure IPS VDOM parameter.

```
config ips settings
  Description: Configure IPS VDOM parameter.
  set packet-log-history {integer}
  set packet-log-post-attack {integer}
  set packet-log-memory {integer}
  set ips-packet-quota {integer}
end
```

## config ips settings

Parameter	Description	Type	Size	Default
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected .	integer	Minimum value: 1 Maximum value: 255	1
packet-log-post-attack	Number of packets to log after the IPS signature is detected .	integer	Minimum value: 0 Maximum value: 255	0
packet-log-memory	Maximum memory can be used by packet log .	integer	Minimum value: 64 Maximum value: 8192	256
ips-packet-quota	Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config ips session

Session status.

```
config ips session
  Description: Session status.
end
```

## ipsec

This section includes syntax for the following commands:

- [config ipsec tunnel on page 406](#)

### config ipsec tunnel

IPsec tunnel.

```
config ipsec tunnel
  Description: IPsec tunnel.
end
```

# log

This section includes syntax for the following commands:

- [config log threat-weight](#) on page 408
- [config log fortianalyzer2 setting](#) on page 504
- [config log syslogd3 setting](#) on page 440
- [config log syslogd2 override-filter](#) on page 438
- [config log syslogd filter](#) on page 425
- [config log fortianalyzer2 filter](#) on page 512
- [config log gui-display](#) on page 491
- [config log memory global-setting](#) on page 464
- [config log fortiguard override-setting](#) on page 480
- [config log eventfilter](#) on page 475
- [config log syslogd4 override-filter](#) on page 460
- [config log fortianalyzer2 override-filter](#) on page 514
- [config log fortianalyzer3 override-filter](#) on page 526
- [config log syslogd setting](#) on page 418
- [config log syslogd3 override-setting](#) on page 444
- [config log webtrends filter](#) on page 463
- [config log syslogd override-filter](#) on page 427
- [config log memory filter](#) on page 466
- [config log fortianalyzer-cloud setting](#) on page 528
- [config log syslogd4 filter](#) on page 458
- [config log syslogd3 filter](#) on page 447
- [config log fortianalyzer setting](#) on page 492
- [config log fortiguard override-filter](#) on page 483
- [config log syslogd override-setting](#) on page 421
- [config log fortianalyzer filter](#) on page 500
- [config log syslogd4 override-setting](#) on page 455
- [config log fortianalyzer override-filter](#) on page 502
- [config log fortiguard setting](#) on page 477
- [config log fortianalyzer-cloud override-setting](#) on page 531
- [config log syslogd2 filter](#) on page 436
- [config log syslogd4 setting](#) on page 451
- [config log disk setting](#) on page 467
- [config log fortianalyzer3 filter](#) on page 524
- [config log syslogd2 setting](#) on page 429
- [config log setting](#) on page 487
- [config log null-device setting](#) on page 485
- [config log custom-field](#) on page 417
- [config log null-device filter](#) on page 486
- [config log disk filter](#) on page 473

- [config log syslogd3 override-filter on page 449](#)
- [config log syslogd2 override-setting on page 433](#)
- [config log memory setting on page 465](#)
- [config log fortianalyzer override-setting on page 496](#)
- [config log fortianalyzer3 setting on page 516](#)
- [config log fortianalyzer3 override-setting on page 520](#)
- [config log webtrends setting on page 462](#)
- [config log fortianalyzer-cloud override-filter on page 534](#)
- [config log fortianalyzer-cloud filter on page 532](#)
- [config log fortiguard filter on page 481](#)
- [config log fortianalyzer2 override-setting on page 508](#)

## config log threat-weight

Configure threat weight settings.

```
config log threat-weight
  Description: Configure threat weight settings.
  set status [enable|disable]
  config level
    Description: Score mapping for threat weight levels.
    set low {integer}
    set medium {integer}
    set high {integer}
    set critical {integer}
  end
  set blocked-connection [disable|low|...]
  set failed-connection [disable|low|...]
  set url-block-detected [disable|low|...]
  set botnet-connection-detected [disable|low|...]
  config malware
    Description: Anti-virus malware threat weight settings.
    set virus-infected [disable|low|...]
    set file-blocked [disable|low|...]
    set command-blocked [disable|low|...]
    set oversized [disable|low|...]
    set virus-scan-error [disable|low|...]
    set switch-proto [disable|low|...]
    set mimefragmented [disable|low|...]
    set virus-file-type-executable [disable|low|...]
    set virus-outbreak-prevention [disable|low|...]
    set content-disarm [disable|low|...]
    set malware-list [disable|low|...]
    set fsa-malicious [disable|low|...]
    set fsa-high-risk [disable|low|...]
    set fsa-medium-risk [disable|low|...]
  end
  config ips
    Description: IPS threat weight settings.
    set info-severity [disable|low|...]
    set low-severity [disable|low|...]
    set medium-severity [disable|low|...]
    set high-severity [disable|low|...]
```



```

    set critical-severity [disable|low|...]
end
config web
    Description: Web filtering threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
config geolocation
    Description: Geolocation-based threat weight settings.
    edit <id>
        set country {string}
        set level [disable|low|...]
    next
end
config application
    Description: Application-control threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
end
end

```

## config log threat-weight

Parameter	Description	Type	Size	Default												
status	Enable/disable the threat weight feature.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the threat weight feature.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the threat weight feature.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the threat weight feature.	<i>disable</i>	Disable the threat weight feature.									
Option	Description															
<i>enable</i>	Enable the threat weight feature.															
<i>disable</i>	Disable the threat weight feature.															
blocked-connection	Threat weight score for blocked connections.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for blocked connections.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for blocked connections.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for blocked connections.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for blocked connections.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for blocked connections.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for blocked connections.	<i>low</i>	Use the low level score for blocked connections.	<i>medium</i>	Use the medium level score for blocked connections.	<i>high</i>	Use the high level score for blocked connections.	<i>critical</i>	Use the critical level score for blocked connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for blocked connections.															
<i>low</i>	Use the low level score for blocked connections.															
<i>medium</i>	Use the medium level score for blocked connections.															
<i>high</i>	Use the high level score for blocked connections.															
<i>critical</i>	Use the critical level score for blocked connections.															
failed-connection	Threat weight score for failed connections.	option	-	low												

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for failed connections.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for failed connections.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for failed connections.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for failed connections.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for failed connections.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for failed connections.	<i>low</i>	Use the low level score for failed connections.	<i>medium</i>	Use the medium level score for failed connections.	<i>high</i>	Use the high level score for failed connections.	<i>critical</i>	Use the critical level score for failed connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for failed connections.															
<i>low</i>	Use the low level score for failed connections.															
<i>medium</i>	Use the medium level score for failed connections.															
<i>high</i>	Use the high level score for failed connections.															
<i>critical</i>	Use the critical level score for failed connections.															
url-block-detected	Threat weight score for URL blocking.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for URL blocking.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for URL blocking.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for URL blocking.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for URL blocking.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for URL blocking.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for URL blocking.	<i>low</i>	Use the low level score for URL blocking.	<i>medium</i>	Use the medium level score for URL blocking.	<i>high</i>	Use the high level score for URL blocking.	<i>critical</i>	Use the critical level score for URL blocking.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for URL blocking.															
<i>low</i>	Use the low level score for URL blocking.															
<i>medium</i>	Use the medium level score for URL blocking.															
<i>high</i>	Use the high level score for URL blocking.															
<i>critical</i>	Use the critical level score for URL blocking.															
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-	critical												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for detected botnet connections.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for detected botnet connections.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for detected botnet connections.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for detected botnet connections.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for detected botnet connections.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for detected botnet connections.	<i>low</i>	Use the low level score for detected botnet connections.	<i>medium</i>	Use the medium level score for detected botnet connections.	<i>high</i>	Use the high level score for detected botnet connections.	<i>critical</i>	Use the critical level score for detected botnet connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for detected botnet connections.															
<i>low</i>	Use the low level score for detected botnet connections.															
<i>medium</i>	Use the medium level score for detected botnet connections.															
<i>high</i>	Use the high level score for detected botnet connections.															
<i>critical</i>	Use the critical level score for detected botnet connections.															

### config level

Parameter	Description	Type	Size	Default
low	Low level score value .	integer	Minimum value: 1 Maximum value: 100	5

Parameter	Description	Type	Size	Default
medium	Medium level score value .	integer	Minimum value: 1 Maximum value: 100	10
high	High level score value .	integer	Minimum value: 1 Maximum value: 100	30
critical	Critical level score value .	integer	Minimum value: 1 Maximum value: 100	50

## config malware

Parameter	Description	Type	Size	Default												
virus-infected	Threat weight score for virus (infected) detected.	option	-	critical												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for virus (infected) detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for virus (infected) detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for virus (infected) detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for virus (infected) detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for virus (infected) detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (infected) detected.	<i>low</i>	Use the low level score for virus (infected) detected.	<i>medium</i>	Use the medium level score for virus (infected) detected.	<i>high</i>	Use the high level score for virus (infected) detected.	<i>critical</i>	Use the critical level score for virus (infected) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (infected) detected.															
<i>low</i>	Use the low level score for virus (infected) detected.															
<i>medium</i>	Use the medium level score for virus (infected) detected.															
<i>high</i>	Use the high level score for virus (infected) detected.															
<i>critical</i>	Use the critical level score for virus (infected) detected.															
file-blocked	Threat weight score for blocked file detected.	option	-	low												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for blocked file detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for blocked file detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for blocked file detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for blocked file detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for blocked file detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for blocked file detected.	<i>low</i>	Use the low level score for blocked file detected.	<i>medium</i>	Use the medium level score for blocked file detected.	<i>high</i>	Use the high level score for blocked file detected.	<i>critical</i>	Use the critical level score for blocked file detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for blocked file detected.															
<i>low</i>	Use the low level score for blocked file detected.															
<i>medium</i>	Use the medium level score for blocked file detected.															
<i>high</i>	Use the high level score for blocked file detected.															
<i>critical</i>	Use the critical level score for blocked file detected.															
command-blocked	Threat weight score for blocked command detected.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for blocked command detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for blocked command detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for blocked command detected.	<i>low</i>	Use the low level score for blocked command detected.									
Option	Description															
<i>disable</i>	Disable threat weight scoring for blocked command detected.															
<i>low</i>	Use the low level score for blocked command detected.															

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>medium</i></td> <td>Use the medium level score for blocked command detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for blocked command detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for blocked command detected.</td> </tr> </tbody> </table>	Option	Description	<i>medium</i>	Use the medium level score for blocked command detected.	<i>high</i>	Use the high level score for blocked command detected.	<i>critical</i>	Use the critical level score for blocked command detected.							
Option	Description															
<i>medium</i>	Use the medium level score for blocked command detected.															
<i>high</i>	Use the high level score for blocked command detected.															
<i>critical</i>	Use the critical level score for blocked command detected.															
oversized	Threat weight score for oversized file detected.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for oversized file detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for oversized file detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for oversized file detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for oversized file detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for oversized file detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for oversized file detected.	<i>low</i>	Use the low level score for oversized file detected.	<i>medium</i>	Use the medium level score for oversized file detected.	<i>high</i>	Use the high level score for oversized file detected.	<i>critical</i>	Use the critical level score for oversized file detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for oversized file detected.															
<i>low</i>	Use the low level score for oversized file detected.															
<i>medium</i>	Use the medium level score for oversized file detected.															
<i>high</i>	Use the high level score for oversized file detected.															
<i>critical</i>	Use the critical level score for oversized file detected.															
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for virus (scan error) detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for virus (scan error) detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for virus (scan error) detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for virus (scan error) detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for virus (scan error) detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (scan error) detected.	<i>low</i>	Use the low level score for virus (scan error) detected.	<i>medium</i>	Use the medium level score for virus (scan error) detected.	<i>high</i>	Use the high level score for virus (scan error) detected.	<i>critical</i>	Use the critical level score for virus (scan error) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (scan error) detected.															
<i>low</i>	Use the low level score for virus (scan error) detected.															
<i>medium</i>	Use the medium level score for virus (scan error) detected.															
<i>high</i>	Use the high level score for virus (scan error) detected.															
<i>critical</i>	Use the critical level score for virus (scan error) detected.															
switch-proto	Threat weight score for switch proto detected.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for switch proto detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for switch proto detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for switch proto detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for switch proto detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for switch proto detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for switch proto detected.	<i>low</i>	Use the low level score for switch proto detected.	<i>medium</i>	Use the medium level score for switch proto detected.	<i>high</i>	Use the high level score for switch proto detected.	<i>critical</i>	Use the critical level score for switch proto detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for switch proto detected.															
<i>low</i>	Use the low level score for switch proto detected.															
<i>medium</i>	Use the medium level score for switch proto detected.															
<i>high</i>	Use the high level score for switch proto detected.															
<i>critical</i>	Use the critical level score for switch proto detected.															
mimefragmented	Threat weight score for mimefragmented detected.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for mimefragmented detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.											
Option	Description															
<i>disable</i>	Disable threat weight scoring for mimefragmented detected.															

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Use the low level score for mimefragmented detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for mimefragmented detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for mimefragmented detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for mimefragmented detected.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Use the low level score for mimefragmented detected.	<i>medium</i>	Use the medium level score for mimefragmented detected.	<i>high</i>	Use the high level score for mimefragmented detected.	<i>critical</i>	Use the critical level score for mimefragmented detected.					
Option	Description															
<i>low</i>	Use the low level score for mimefragmented detected.															
<i>medium</i>	Use the medium level score for mimefragmented detected.															
<i>high</i>	Use the high level score for mimefragmented detected.															
<i>critical</i>	Use the critical level score for mimefragmented detected.															
virus-file-type-executable	Threat weight score for virus (filetype executable) detected.	option	-	medium												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for virus (filetype executable) detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for virus (filetype executable) detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for virus (filetype executable) detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for virus (filetype executable) detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for virus (filetype executable) detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.	<i>low</i>	Use the low level score for virus (filetype executable) detected.	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.	<i>high</i>	Use the high level score for virus (filetype executable) detected.	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.															
<i>low</i>	Use the low level score for virus (filetype executable) detected.															
<i>medium</i>	Use the medium level score for virus (filetype executable) detected.															
<i>high</i>	Use the high level score for virus (filetype executable) detected.															
<i>critical</i>	Use the critical level score for virus (filetype executable) detected.															
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-	critical												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for virus (outbreak prevention) event.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for virus (outbreak prevention) event.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for virus (outbreak prevention) event.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for virus (outbreak prevention) event.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for virus (outbreak prevention) event.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.	<i>low</i>	Use the low level score for virus (outbreak prevention) event.	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.	<i>high</i>	Use the high level score for virus (outbreak prevention) event.	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.															
<i>low</i>	Use the low level score for virus (outbreak prevention) event.															
<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.															
<i>high</i>	Use the high level score for virus (outbreak prevention) event.															
<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.															
content-disarm	Threat weight score for virus (content disarm) detected.	option	-	medium												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for virus (content disarm) detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for virus (content disarm) detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for virus (content disarm) detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for virus (content disarm) detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for virus (content disarm) detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.	<i>low</i>	Use the low level score for virus (content disarm) detected.	<i>medium</i>	Use the medium level score for virus (content disarm) detected.	<i>high</i>	Use the high level score for virus (content disarm) detected.	<i>critical</i>	Use the critical level score for virus (content disarm) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.															
<i>low</i>	Use the low level score for virus (content disarm) detected.															
<i>medium</i>	Use the medium level score for virus (content disarm) detected.															
<i>high</i>	Use the high level score for virus (content disarm) detected.															
<i>critical</i>	Use the critical level score for virus (content disarm) detected.															
malware-list	Threat weight score for virus (malware list) detected.	option	-	medium												

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for virus (malware list) detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for virus (malware list) detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for virus (malware list) detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for virus (malware list) detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for virus (malware list) detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.	<i>low</i>	Use the low level score for virus (malware list) detected.	<i>medium</i>	Use the medium level score for virus (malware list) detected.	<i>high</i>	Use the high level score for virus (malware list) detected.	<i>critical</i>	Use the critical level score for virus (malware list) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.															
<i>low</i>	Use the low level score for virus (malware list) detected.															
<i>medium</i>	Use the medium level score for virus (malware list) detected.															
<i>high</i>	Use the high level score for virus (malware list) detected.															
<i>critical</i>	Use the critical level score for virus (malware list) detected.															
fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-	critical												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for FortiSandbox malicious malware detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for FortiSandbox malicious malware detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for FortiSandbox malicious malware detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for FortiSandbox malicious malware detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for FortiSandbox malicious malware detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.	<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.	<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.															
<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.															
<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.															
<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.															
<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.															
fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for FortiSandbox high risk malware detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for FortiSandbox high risk malware detected.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for FortiSandbox high risk malware detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for FortiSandbox high risk malware detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for FortiSandbox high risk malware detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.	<i>low</i>	Use the low level score for FortiSandbox high risk malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox high risk malware detected.	<i>high</i>	Use the high level score for FortiSandbox high risk malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox high risk malware detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.															
<i>low</i>	Use the low level score for FortiSandbox high risk malware detected.															
<i>medium</i>	Use the medium level score for FortiSandbox high risk malware detected.															
<i>high</i>	Use the high level score for FortiSandbox high risk malware detected.															
<i>critical</i>	Use the critical level score for FortiSandbox high risk malware detected.															
fsa-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-	medium												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for FortiSandbox medium risk malware detected.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for FortiSandbox medium risk malware detected.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.	<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.									
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.															
<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>medium</i></td> <td>Use the medium level score for FortiSandbox medium risk malware detected.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for FortiSandbox medium risk malware detected.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for FortiSandbox medium risk malware detected.</td> </tr> </tbody> </table>	Option	Description	<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.	<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.			
Option	Description											
<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.											
<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.											
<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.											

## config ips

Parameter	Description	Type	Size	Default												
info-severity	Threat weight score for IPS info severity events.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for IPS info severity events.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for IPS info severity events.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for IPS info severity events.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for IPS info severity events.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for IPS info severity events.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS info severity events.	<i>low</i>	Use the low level score for IPS info severity events.	<i>medium</i>	Use the medium level score for IPS info severity events.	<i>high</i>	Use the high level score for IPS info severity events.	<i>critical</i>	Use the critical level score for IPS info severity events.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for IPS info severity events.															
<i>low</i>	Use the low level score for IPS info severity events.															
<i>medium</i>	Use the medium level score for IPS info severity events.															
<i>high</i>	Use the high level score for IPS info severity events.															
<i>critical</i>	Use the critical level score for IPS info severity events.															
low-severity	Threat weight score for IPS low severity events.	option	-	low												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for IPS low severity events.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for IPS low severity events.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for IPS low severity events.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for IPS low severity events.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for IPS low severity events.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS low severity events.	<i>low</i>	Use the low level score for IPS low severity events.	<i>medium</i>	Use the medium level score for IPS low severity events.	<i>high</i>	Use the high level score for IPS low severity events.	<i>critical</i>	Use the critical level score for IPS low severity events.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for IPS low severity events.															
<i>low</i>	Use the low level score for IPS low severity events.															
<i>medium</i>	Use the medium level score for IPS low severity events.															
<i>high</i>	Use the high level score for IPS low severity events.															
<i>critical</i>	Use the critical level score for IPS low severity events.															
medium-severity	Threat weight score for IPS medium severity events.	option	-	medium												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for IPS medium severity events.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for IPS medium severity events.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for IPS medium severity events.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for IPS medium severity events.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS medium severity events.	<i>low</i>	Use the low level score for IPS medium severity events.	<i>medium</i>	Use the medium level score for IPS medium severity events.	<i>high</i>	Use the high level score for IPS medium severity events.					
Option	Description															
<i>disable</i>	Disable threat weight scoring for IPS medium severity events.															
<i>low</i>	Use the low level score for IPS medium severity events.															
<i>medium</i>	Use the medium level score for IPS medium severity events.															
<i>high</i>	Use the high level score for IPS medium severity events.															

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>critical</i></td> <td>Use the critical level score for IPS medium severity events.</td> </tr> </tbody> </table>	Option	Description	<i>critical</i>	Use the critical level score for IPS medium severity events.											
Option	Description															
<i>critical</i>	Use the critical level score for IPS medium severity events.															
high-severity	Threat weight score for IPS high severity events.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for IPS high severity events.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for IPS high severity events.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for IPS high severity events.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for IPS high severity events.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for IPS high severity events.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS high severity events.	<i>low</i>	Use the low level score for IPS high severity events.	<i>medium</i>	Use the medium level score for IPS high severity events.	<i>high</i>	Use the high level score for IPS high severity events.	<i>critical</i>	Use the critical level score for IPS high severity events.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for IPS high severity events.															
<i>low</i>	Use the low level score for IPS high severity events.															
<i>medium</i>	Use the medium level score for IPS high severity events.															
<i>high</i>	Use the high level score for IPS high severity events.															
<i>critical</i>	Use the critical level score for IPS high severity events.															
critical-severity	Threat weight score for IPS critical severity events.	option	-	critical												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for IPS critical severity events.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for IPS critical severity events.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for IPS critical severity events.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for IPS critical severity events.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for IPS critical severity events.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS critical severity events.	<i>low</i>	Use the low level score for IPS critical severity events.	<i>medium</i>	Use the medium level score for IPS critical severity events.	<i>high</i>	Use the high level score for IPS critical severity events.	<i>critical</i>	Use the critical level score for IPS critical severity events.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for IPS critical severity events.															
<i>low</i>	Use the low level score for IPS critical severity events.															
<i>medium</i>	Use the medium level score for IPS critical severity events.															
<i>high</i>	Use the high level score for IPS critical severity events.															
<i>critical</i>	Use the critical level score for IPS critical severity events.															

## config web

Parameter	Description	Type	Size	Default												
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255	0												
level	Threat weight score for web category filtering matches.	option	-	low												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable threat weight scoring for web category filtering matches.</td> </tr> <tr> <td><i>low</i></td> <td>Use the low level score for web category filtering matches.</td> </tr> <tr> <td><i>medium</i></td> <td>Use the medium level score for web category filtering matches.</td> </tr> <tr> <td><i>high</i></td> <td>Use the high level score for web category filtering matches.</td> </tr> <tr> <td><i>critical</i></td> <td>Use the critical level score for web category filtering matches.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable threat weight scoring for web category filtering matches.	<i>low</i>	Use the low level score for web category filtering matches.	<i>medium</i>	Use the medium level score for web category filtering matches.	<i>high</i>	Use the high level score for web category filtering matches.	<i>critical</i>	Use the critical level score for web category filtering matches.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for web category filtering matches.															
<i>low</i>	Use the low level score for web category filtering matches.															
<i>medium</i>	Use the medium level score for web category filtering matches.															
<i>high</i>	Use the high level score for web category filtering matches.															
<i>critical</i>	Use the critical level score for web category filtering matches.															



## config geolocation

Parameter	Description	Type	Size	Default												
country	Country code.	string	Maximum length: 2													
level	Threat weight score for Geolocation-based events.	option	-	low												
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable threat weight scoring for Geolocation-based events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for Geolocation-based events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for Geolocation-based events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for Geolocation-based events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for Geolocation-based events.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.	<i>low</i>	Use the low level score for Geolocation-based events.	<i>medium</i>	Use the medium level score for Geolocation-based events.	<i>high</i>	Use the high level score for Geolocation-based events.	<i>critical</i>	Use the critical level score for Geolocation-based events.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for Geolocation-based events.															
<i>low</i>	Use the low level score for Geolocation-based events.															
<i>medium</i>	Use the medium level score for Geolocation-based events.															
<i>high</i>	Use the high level score for Geolocation-based events.															
<i>critical</i>	Use the critical level score for Geolocation-based events.															

## config application

Parameter	Description	Type	Size	Default												
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0												
level	Threat weight score for Application events.	option	-	low												
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable threat weight scoring for Application events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for Application events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for Application events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for Application events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for Application events.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for Application events.	<i>low</i>	Use the low level score for Application events.	<i>medium</i>	Use the medium level score for Application events.	<i>high</i>	Use the high level score for Application events.	<i>critical</i>	Use the critical level score for Application events.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for Application events.															
<i>low</i>	Use the low level score for Application events.															
<i>medium</i>	Use the medium level score for Application events.															
<i>high</i>	Use the high level score for Application events.															
<i>critical</i>	Use the critical level score for Application events.															

## config log custom-field

Configure custom log fields.

```
config log custom-field
  Description: Configure custom log fields.
  edit <id>
    set name {string}
    set value {string}
  next
end
```

## config log custom-field

Parameter	Description	Type	Size	Default
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 15 characters).	string	Maximum length: 15	

## config log syslogd setting

Global settings for remote syslog server.

```
config log syslogd setting
  Description: Global settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config log syslogd setting

Parameter	Description	Type	Size	Default						
status	Enable/disable remote syslog logging.	option	-	disable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
Option	Description									
<i>enable</i>	Log to remote syslog server.									
<i>disable</i>	Do not log to remote syslog server.									

Parameter	Description	Type	Size	Default																																		
server	Address of remote syslog server.	string	Maximum length: 127																																			
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>legacy-reliable</i></td> <td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																													
Option	Description																																					
<i>udp</i>	Enable syslogging over UDP.																																					
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																																					
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																																					
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																																		
facility	Remote syslog facility.	option	-	local7																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.			
Option	Description																																					
<i>kernel</i>	Kernel messages.																																					
<i>user</i>	Random user-level messages.																																					
<i>mail</i>	Mail system.																																					
<i>daemon</i>	System daemons.																																					
<i>auth</i>	Security/authorization messages.																																					
<i>syslog</i>	Messages generated internally by syslog.																																					
<i>lpr</i>	Line printer subsystem.																																					
<i>news</i>	Network news subsystem.																																					
<i>uucp</i>	Network news subsystem.																																					
<i>cron</i>	Clock daemon.																																					
<i>authpriv</i>	Security/authorization messages (private).																																					
<i>ftp</i>	FTP daemon.																																					
<i>ntp</i>	NTP daemon.																																					
<i>audit</i>	Log audit.																																					
<i>alert</i>	Log alert.																																					
<i>clock</i>	Clock daemon.																																					

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																					
<i>local0</i>	Reserved for local use.																					
<i>local1</i>	Reserved for local use.																					
<i>local2</i>	Reserved for local use.																					
<i>local3</i>	Reserved for local use.																					
<i>local4</i>	Reserved for local use.																					
<i>local5</i>	Reserved for local use.																					
<i>local6</i>	Reserved for local use.																					
<i>local7</i>	Reserved for local use.																					
source-ip	Source IP address of syslog.	string	Maximum length: 63																			
format	Log format.	option	-	default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.											
Option	Description																					
<i>default</i>	Syslog format.																					
<i>csv</i>	CSV (Comma Separated Values) format.																					
<i>cef</i>	CEF (Common Event Format) format.																					
<i>rfc5424</i>	Syslog RFC5424 format.																					
priority	Set log transmission priority.	option	-	default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.															
Option	Description																					
<i>default</i>	Set Syslog transmission priority to default.																					
<i>low</i>	Set Syslog transmission priority to low.																					
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0																		
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.															
Option	Description																					
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																					
<i>high</i>	SSL communication with high encryption algorithms.																					

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.									
Option	Description															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd override-setting

Override settings for remote syslog server.

```
config log syslogd override-setting
  Description: Override settings for remote syslog server.
```

```

set status [enable|disable]
set server {string}
set mode [udp|legacy-reliable|...]
set port {integer}
set facility [kernel|user|...]
set source-ip {string}
set format [default|csv|...]
set priority [default|low]
set max-log-rate {integer}
set enc-algorithm [high-medium|high|...]
set ssl-min-proto-version [default|SSLv3|...]
set certificate {string}
config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
        set name {string}
        set custom {string}
    next
end
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config log syslogd override-setting

Parameter	Description	Type	Size	Default								
status	Enable/disable remote syslog logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.					
Option	Description											
<i>enable</i>	Log to remote syslog server.											
<i>disable</i>	Do not log to remote syslog server.											
server	Address of remote syslog server.	string	Maximum length: 127									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>legacy-reliable</i></td> <td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
<i>udp</i>	Enable syslogging over UDP.											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								

Parameter	Description	Type	Size	Default																																																		
facility	Remote syslog facility.	option	-	local7																																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																																																					
<i>kernel</i>	Kernel messages.																																																					
<i>user</i>	Random user-level messages.																																																					
<i>mail</i>	Mail system.																																																					
<i>daemon</i>	System daemons.																																																					
<i>auth</i>	Security/authorization messages.																																																					
<i>syslog</i>	Messages generated internally by syslog.																																																					
<i>lpr</i>	Line printer subsystem.																																																					
<i>news</i>	Network news subsystem.																																																					
<i>uucp</i>	Network news subsystem.																																																					
<i>cron</i>	Clock daemon.																																																					
<i>authpriv</i>	Security/authorization messages (private).																																																					
<i>ftp</i>	FTP daemon.																																																					
<i>ntp</i>	NTP daemon.																																																					
<i>audit</i>	Log audit.																																																					
<i>alert</i>	Log alert.																																																					
<i>clock</i>	Clock daemon.																																																					
<i>local0</i>	Reserved for local use.																																																					
<i>local1</i>	Reserved for local use.																																																					
<i>local2</i>	Reserved for local use.																																																					
<i>local3</i>	Reserved for local use.																																																					
<i>local4</i>	Reserved for local use.																																																					
<i>local5</i>	Reserved for local use.																																																					
<i>local6</i>	Reserved for local use.																																																					
<i>local7</i>	Reserved for local use.																																																					
source-ip	Source IP address of syslog.	string	Maximum length: 63																																																			
format	Log format.	option	-	default																																																		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.					
Option	Description															
<i>default</i>	Syslog format.															
<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.															
<i>rfc5424</i>	Syslog RFC5424 format.															
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													



Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd filter

Filters for remote system server.

```

config log syslogd filter
  Description: Filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end

```

### config log syslogd filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd override-filter

Override filters for remote system server.

```
config log syslogd override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log syslogd override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd2 setting

Global settings for remote syslog server.

```

config log syslogd2 setting
  Description: Global settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```

## config log syslogd2 setting

Parameter	Description	Type	Size	Default																								
status	Enable/disable remote syslog logging.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.																					
Option	Description																											
<i>enable</i>	Log to remote syslog server.																											
<i>disable</i>	Do not log to remote syslog server.																											
server	Address of remote syslog server.	string	Maximum length: 127																									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>legacy-reliable</i></td> <td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																			
Option	Description																											
<i>udp</i>	Enable syslogging over UDP.																											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																								
facility	Remote syslog facility.	option	-	local7																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).			
Option	Description																											
<i>kernel</i>	Kernel messages.																											
<i>user</i>	Random user-level messages.																											
<i>mail</i>	Mail system.																											
<i>daemon</i>	System daemons.																											
<i>auth</i>	Security/authorization messages.																											
<i>syslog</i>	Messages generated internally by syslog.																											
<i>lpr</i>	Line printer subsystem.																											
<i>news</i>	Network news subsystem.																											
<i>uucp</i>	Network news subsystem.																											
<i>cron</i>	Clock daemon.																											
<i>authpriv</i>	Security/authorization messages (private).																											

Parameter	Description	Type	Size	Default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																															
<i>ftp</i>	FTP daemon.																															
<i>ntp</i>	NTP daemon.																															
<i>audit</i>	Log audit.																															
<i>alert</i>	Log alert.																															
<i>clock</i>	Clock daemon.																															
<i>local0</i>	Reserved for local use.																															
<i>local1</i>	Reserved for local use.																															
<i>local2</i>	Reserved for local use.																															
<i>local3</i>	Reserved for local use.																															
<i>local4</i>	Reserved for local use.																															
<i>local5</i>	Reserved for local use.																															
<i>local6</i>	Reserved for local use.																															
<i>local7</i>	Reserved for local use.																															
source-ip	Source IP address of syslog.	string	Maximum length: 63																													
format	Log format.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																					
Option	Description																															
<i>default</i>	Syslog format.																															
<i>csv</i>	CSV (Comma Separated Values) format.																															
<i>cef</i>	CEF (Common Event Format) format.																															
<i>rfc5424</i>	Syslog RFC5424 format.																															
priority	Set log transmission priority.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.																									
Option	Description																															
<i>default</i>	Set Syslog transmission priority to default.																															
<i>low</i>	Set Syslog transmission priority to low.																															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0																												

Parameter	Description	Type	Size	Default												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	



## config log syslogd2 override-setting

Override settings for remote syslog server.

```
config log syslogd2 override-setting
  Description: Override settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config log syslogd2 override-setting

Parameter	Description	Type	Size	Default								
status	Enable/disable remote syslog logging.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.					
Option	Description											
<i>enable</i>	Log to remote syslog server.											
<i>disable</i>	Do not log to remote syslog server.											
server	Address of remote syslog server.	string	Maximum length: 127									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></tbody></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
<i>udp</i>	Enable syslogging over UDP.											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.
<i>local6</i>	Reserved for local use.
<i>local7</i>	Reserved for local use.

Parameter	Description	Type	Size	Default												
source-ip	Source IP address of syslog.	string	Maximum length: 63													
format	Log format.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.					
Option	Description															
<i>default</i>	Syslog format.															
<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.															
<i>rfc5424</i>	Syslog RFC5424 format.															
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

Parameter	Description	Type	Size	Default								
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

## config log syslogd2 filter

Filters for remote system server.

```

config log syslogd2 filter
  Description: Filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end

```

### config log syslogd2 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog 2 filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log syslogd2 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog 2 filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd3 setting

Global settings for remote syslog server.

```

config log syslogd3 setting
  Description: Global settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```



## config log syslogd3 setting

Parameter	Description	Type	Size	Default																								
status	Enable/disable remote syslog logging.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.																					
Option	Description																											
<i>enable</i>	Log to remote syslog server.																											
<i>disable</i>	Do not log to remote syslog server.																											
server	Address of remote syslog server.	string	Maximum length: 127																									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>legacy-reliable</i></td> <td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																			
Option	Description																											
<i>udp</i>	Enable syslogging over UDP.																											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																								
facility	Remote syslog facility.	option	-	local7																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).			
Option	Description																											
<i>kernel</i>	Kernel messages.																											
<i>user</i>	Random user-level messages.																											
<i>mail</i>	Mail system.																											
<i>daemon</i>	System daemons.																											
<i>auth</i>	Security/authorization messages.																											
<i>syslog</i>	Messages generated internally by syslog.																											
<i>lpr</i>	Line printer subsystem.																											
<i>news</i>	Network news subsystem.																											
<i>uucp</i>	Network news subsystem.																											
<i>cron</i>	Clock daemon.																											
<i>authpriv</i>	Security/authorization messages (private).																											

Parameter	Description	Type	Size	Default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																															
<i>ftp</i>	FTP daemon.																															
<i>ntp</i>	NTP daemon.																															
<i>audit</i>	Log audit.																															
<i>alert</i>	Log alert.																															
<i>clock</i>	Clock daemon.																															
<i>local0</i>	Reserved for local use.																															
<i>local1</i>	Reserved for local use.																															
<i>local2</i>	Reserved for local use.																															
<i>local3</i>	Reserved for local use.																															
<i>local4</i>	Reserved for local use.																															
<i>local5</i>	Reserved for local use.																															
<i>local6</i>	Reserved for local use.																															
<i>local7</i>	Reserved for local use.																															
source-ip	Source IP address of syslog.	string	Maximum length: 63																													
format	Log format.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																					
Option	Description																															
<i>default</i>	Syslog format.																															
<i>csv</i>	CSV (Comma Separated Values) format.																															
<i>cef</i>	CEF (Common Event Format) format.																															
<i>rfc5424</i>	Syslog RFC5424 format.																															
priority	Set log transmission priority.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.																									
Option	Description																															
<i>default</i>	Set Syslog transmission priority to default.																															
<i>low</i>	Set Syslog transmission priority to low.																															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0																												

Parameter	Description	Type	Size	Default												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

## config log syslogd3 override-setting

Override settings for remote syslog server.

```
config log syslogd3 override-setting
  Description: Override settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config log syslogd3 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	<b>Option</b>	<b>Description</b>		
	<i>udp</i>	Enable syslogging over UDP.		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.
<i>local6</i>	Reserved for local use.
<i>local7</i>	Reserved for local use.

Parameter	Description	Type	Size	Default												
source-ip	Source IP address of syslog.	string	Maximum length: 63													
format	Log format.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.					
Option	Description															
<i>default</i>	Syslog format.															
<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.															
<i>rfc5424</i>	Syslog RFC5424 format.															
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

Parameter	Description	Type	Size	Default								
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd3 filter

Filters for remote system server.

```

config log syslogd3 filter
  Description: Filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end

```

### config log syslogd3 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog 3 filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd3 override-filter

Override filters for remote system server.

```
config log syslogd3 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log syslogd3 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog 3 filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd4 setting

Global settings for remote syslog server.

```

config log syslogd4 setting
  Description: Global settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```

## config log syslogd4 setting

Parameter	Description	Type	Size	Default																								
status	Enable/disable remote syslog logging.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.																					
Option	Description																											
<i>enable</i>	Log to remote syslog server.																											
<i>disable</i>	Do not log to remote syslog server.																											
server	Address of remote syslog server.	string	Maximum length: 127																									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>Enable syslogging over UDP.</td> </tr> <tr> <td><i>legacy-reliable</i></td> <td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td> </tr> <tr> <td><i>reliable</i></td> <td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																			
Option	Description																											
<i>udp</i>	Enable syslogging over UDP.																											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																								
facility	Remote syslog facility.	option	-	local7																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslog.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).			
Option	Description																											
<i>kernel</i>	Kernel messages.																											
<i>user</i>	Random user-level messages.																											
<i>mail</i>	Mail system.																											
<i>daemon</i>	System daemons.																											
<i>auth</i>	Security/authorization messages.																											
<i>syslog</i>	Messages generated internally by syslog.																											
<i>lpr</i>	Line printer subsystem.																											
<i>news</i>	Network news subsystem.																											
<i>uucp</i>	Network news subsystem.																											
<i>cron</i>	Clock daemon.																											
<i>authpriv</i>	Security/authorization messages (private).																											

Parameter	Description	Type	Size	Default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																															
<i>ftp</i>	FTP daemon.																															
<i>ntp</i>	NTP daemon.																															
<i>audit</i>	Log audit.																															
<i>alert</i>	Log alert.																															
<i>clock</i>	Clock daemon.																															
<i>local0</i>	Reserved for local use.																															
<i>local1</i>	Reserved for local use.																															
<i>local2</i>	Reserved for local use.																															
<i>local3</i>	Reserved for local use.																															
<i>local4</i>	Reserved for local use.																															
<i>local5</i>	Reserved for local use.																															
<i>local6</i>	Reserved for local use.																															
<i>local7</i>	Reserved for local use.																															
source-ip	Source IP address of syslog.	string	Maximum length: 63																													
format	Log format.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																					
Option	Description																															
<i>default</i>	Syslog format.																															
<i>csv</i>	CSV (Comma Separated Values) format.																															
<i>cef</i>	CEF (Common Event Format) format.																															
<i>rfc5424</i>	Syslog RFC5424 format.																															
priority	Set log transmission priority.	option	-	default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.																									
Option	Description																															
<i>default</i>	Set Syslog transmission priority to default.																															
<i>low</i>	Set Syslog transmission priority to low.																															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0																												

Parameter	Description	Type	Size	Default												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

## config log syslogd4 override-setting

Override settings for remote syslog server.

```
config log syslogd4 override-setting
  Description: Override settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config log syslogd4 override-setting

Parameter	Description	Type	Size	Default								
status	Enable/disable remote syslog logging.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.					
Option	Description											
<i>enable</i>	Log to remote syslog server.											
<i>disable</i>	Do not log to remote syslog server.											
server	Address of remote syslog server.	string	Maximum length: 127									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></tbody></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
<i>udp</i>	Enable syslogging over UDP.											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.
<i>local6</i>	Reserved for local use.
<i>local7</i>	Reserved for local use.



Parameter	Description	Type	Size	Default												
source-ip	Source IP address of syslog.	string	Maximum length: 63													
format	Log format.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Syslog format.</td> </tr> <tr> <td><i>csv</i></td> <td>CSV (Comma Separated Values) format.</td> </tr> <tr> <td><i>cef</i></td> <td>CEF (Common Event Format) format.</td> </tr> <tr> <td><i>rfc5424</i></td> <td>Syslog RFC5424 format.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.					
Option	Description															
<i>default</i>	Syslog format.															
<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.															
<i>rfc5424</i>	Syslog RFC5424 format.															
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set Syslog transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set Syslog transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.									
Option	Description															
<i>default</i>	Set Syslog transmission priority to default.															
<i>low</i>	Set Syslog transmission priority to low.															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL communication.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

Parameter	Description	Type	Size	Default								
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

### config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd4 filter

Filters for remote system server.

```
config log syslogd4 filter
  Description: Filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

### config log syslogd4 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog 4 filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log syslogd4 override-filter

Override filters for remote system server.

```
config log syslogd4 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log syslogd4 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
anomaly	Enable/disable anomaly logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Syslog 4 filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
  Description: Settings for WebTrends.
  set status [enable|disable]
  set server {string}
end
```

## config log webtrends setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to WebTrends.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to WebTrends.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to WebTrends.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to WebTrends.	<i>disable</i>	Disable logging to WebTrends.			
Option	Description									
<i>enable</i>	Enable logging to WebTrends.									
<i>disable</i>	Disable logging to WebTrends.									
server	Address of the remote WebTrends server.	string	Maximum length: 63							

## config log webtrends filter

Filters for WebTrends.

```
config log webtrends filter
  Description: Filters for WebTrends.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log webtrends filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log to WebTrends.	option	-	information																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></tbody></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					

Parameter	Description	Type	Size	Default
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
filter	Webtrends log filter.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log memory global-setting

Global settings for memory logging.

```

config log memory global-setting
  Description: Global settings for memory logging.
  set max-size {integer}
  set full-first-warning-threshold {integer}
  set full-second-warning-threshold {integer}
  set full-final-warning-threshold {integer}

```



end

## config log memory global-setting

Parameter	Description	Type	Size	Default
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295	19568967 **
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100	95

\*\* Values may differ between models.

## config log memory setting

Settings for memory buffer.

```
config log memory setting
  Description: Settings for memory buffer.
  set status [enable|disable]
end
```

## config log memory setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to the FortiGate's memory.	option	-	enable **						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable logging to memory.</td></tr><tr><td><i>disable</i></td><td>Disable logging to memory.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable logging to memory.	<i>disable</i>	Disable logging to memory.			
Option	Description									
<i>enable</i>	Enable logging to memory.									
<i>disable</i>	Disable logging to memory.									

\*\* Values may differ between models.

## config log memory filter

Filters for memory buffer.

```
config log memory filter
  Description: Filters for memory buffer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log memory filter

Parameter	Description	Type	Size	Default																		
severity	Log every message above and including this severity level.	option	-	information																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></tbody></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	disable **																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.																	
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable local in or out traffic logging.					
Option	Description									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.			
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									
<i>disable</i>	Disable multicast traffic logging.									
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	Memory log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

\*\* Values may differ between models.

## config log disk setting

Settings for local disk logging.

```

config log disk setting
  Description: Settings for local disk logging.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set max-log-file-size {integer}
  set max-policy-packet-capture-size {integer}
  set roll-schedule [daily|weekly]
  set roll-day {option1}, {option2}, ...
  set roll-time {user}
  set diskfull [overwrite|nolog]
  set log-quota {integer}
  set dlp-archive-quota {integer}
  set maximum-log-age {integer}
  set upload [enable|disable]
  set upload-destination {option}
  set uploadip {ipv4-address}
  set uploadport {integer}
  set source-ip {ipv4-address}
  set uploaduser {string}
  set uploadpass {password}
  set uploaddir {string}
  set uploadtype {option1}, {option2}, ...
  set uploadsched [disable|enable]
  set uploadtime {user}
  set upload-delete-files [enable|disable]
  set upload-ssl-conn [default|high|...]
  set full-first-warning-threshold {integer}
  set full-second-warning-threshold {integer}
  set full-final-warning-threshold {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```

## config log disk setting

Parameter	Description	Type	Size	Default						
status	Enable/disable local disk logging.	option	-	disable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Log to local disk.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not log to local disk.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Log to local disk.	<i>disable</i>	Do not log to local disk.			
Option	Description									
<i>enable</i>	Log to local disk.									
<i>disable</i>	Do not log to local disk.									
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archiving.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archiving.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archiving.	<i>disable</i>	Disable IPS packet archiving.			
Option	Description									
<i>enable</i>	Enable IPS packet archiving.									
<i>disable</i>	Disable IPS packet archiving.									

Parameter	Description	Type	Size	Default
max-log-file-size	Maximum log file size before rolling .	integer	Minimum value: 1 Maximum value: 100	20
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100
roll-schedule	Frequency to check log file for rolling.	option	-	daily
	<b>Option</b>	<b>Description</b>		
	<i>daily</i>	Check the log file once a day.		
	<i>weekly</i>	Check the log file once a week.		
roll-day	Day of week on which to roll log file.	option	-	sunday
	<b>Option</b>	<b>Description</b>		
	<i>sunday</i>	Sunday		
	<i>monday</i>	Monday		
	<i>tuesday</i>	Tuesday		
	<i>wednesday</i>	Wednesday		
	<i>thursday</i>	Thursday		
	<i>friday</i>	Friday		
	<i>saturday</i>	Saturday		
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified	
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full .	option	-	overwrite
	<b>Option</b>	<b>Description</b>		
	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.		
	<i>nolog</i>	Stop logging when the log disk is full.		

Parameter	Description	Type	Size	Default
log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7
upload	Enable/disable uploading log files when they are rolled.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable uploading log files when they are rolled.		
	<i>disable</i>	Disable uploading log files when they are rolled.		
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-	ftp-server
	<b>Option</b>	<b>Description</b>		
	<i>ftp-server</i>	Upload rolled log files to an FTP server.		
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0
uploadport	TCP port to use for communicating with the FTP server .	integer	Minimum value: 0 Maximum value: 65535	21
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified	
uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default																																						
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl cifs **																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>traffic</i></td> <td>Upload traffic log.</td> </tr> <tr> <td><i>event</i></td> <td>Upload event log.</td> </tr> <tr> <td><i>virus</i></td> <td>Upload anti-virus log.</td> </tr> <tr> <td><i>webfilter</i></td> <td>Upload web filter log.</td> </tr> <tr> <td><i>IPS</i></td> <td>Upload IPS log.</td> </tr> <tr> <td><i>emailfilter</i></td> <td>Upload spam filter log.</td> </tr> <tr> <td><i>dlp-archive</i></td> <td>Upload DLP archive.</td> </tr> <tr> <td><i>anomaly</i></td> <td>Upload anomaly log.</td> </tr> <tr> <td><i>voip</i></td> <td>Upload VoIP log.</td> </tr> <tr> <td><i>dlp</i></td> <td>Upload DLP log.</td> </tr> <tr> <td><i>app-ctrl</i></td> <td>Upload application control log.</td> </tr> <tr> <td><i>waf</i></td> <td>Upload web application firewall log.</td> </tr> <tr> <td><i>dns</i></td> <td>Upload DNS log.</td> </tr> <tr> <td><i>ssh</i></td> <td>Upload SSH log.</td> </tr> <tr> <td><i>ssl</i></td> <td>Upload SSL log.</td> </tr> <tr> <td><i>cifs</i></td> <td>Upload CIFS log.</td> </tr> <tr> <td><i>file-filter</i></td> <td>Upload file-filter log.</td> </tr> <tr> <td><i>icap</i></td> <td>Upload ICAP log.</td> </tr> </tbody> </table>	Option	Description	<i>traffic</i>	Upload traffic log.	<i>event</i>	Upload event log.	<i>virus</i>	Upload anti-virus log.	<i>webfilter</i>	Upload web filter log.	<i>IPS</i>	Upload IPS log.	<i>emailfilter</i>	Upload spam filter log.	<i>dlp-archive</i>	Upload DLP archive.	<i>anomaly</i>	Upload anomaly log.	<i>voip</i>	Upload VoIP log.	<i>dlp</i>	Upload DLP log.	<i>app-ctrl</i>	Upload application control log.	<i>waf</i>	Upload web application firewall log.	<i>dns</i>	Upload DNS log.	<i>ssh</i>	Upload SSH log.	<i>ssl</i>	Upload SSL log.	<i>cifs</i>	Upload CIFS log.	<i>file-filter</i>	Upload file-filter log.	<i>icap</i>	Upload ICAP log.			
Option	Description																																									
<i>traffic</i>	Upload traffic log.																																									
<i>event</i>	Upload event log.																																									
<i>virus</i>	Upload anti-virus log.																																									
<i>webfilter</i>	Upload web filter log.																																									
<i>IPS</i>	Upload IPS log.																																									
<i>emailfilter</i>	Upload spam filter log.																																									
<i>dlp-archive</i>	Upload DLP archive.																																									
<i>anomaly</i>	Upload anomaly log.																																									
<i>voip</i>	Upload VoIP log.																																									
<i>dlp</i>	Upload DLP log.																																									
<i>app-ctrl</i>	Upload application control log.																																									
<i>waf</i>	Upload web application firewall log.																																									
<i>dns</i>	Upload DNS log.																																									
<i>ssh</i>	Upload SSH log.																																									
<i>ssl</i>	Upload SSL log.																																									
<i>cifs</i>	Upload CIFS log.																																									
<i>file-filter</i>	Upload file-filter log.																																									
<i>icap</i>	Upload ICAP log.																																									
uploadsched	Set the schedule for uploading log files to the FTP server .	option	-	disable																																						

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Upload when rolling.</td> </tr> <tr> <td><i>enable</i></td> <td>Scheduled upload.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Upload when rolling.	<i>enable</i>	Scheduled upload.							
Option	Description													
<i>disable</i>	Upload when rolling.													
<i>enable</i>	Scheduled upload.													
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified											
upload-delete-files	Delete log files after uploading .	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Delete log files after uploading.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not delete log files after uploading.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Delete log files after uploading.	<i>disable</i>	Do not delete log files after uploading.							
Option	Description													
<i>enable</i>	Delete log files after uploading.													
<i>disable</i>	Do not delete log files after uploading.													
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>FTPS with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>FTPS with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>FTPS with low encryption algorithms.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FTPS communication.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	FTPS with high and medium encryption algorithms.	<i>high</i>	FTPS with high encryption algorithms.	<i>low</i>	FTPS with low encryption algorithms.	<i>disable</i>	Disable FTPS communication.			
Option	Description													
<i>default</i>	FTPS with high and medium encryption algorithms.													
<i>high</i>	FTPS with high encryption algorithms.													
<i>low</i>	FTPS with low encryption algorithms.													
<i>disable</i>	Disable FTPS communication.													
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98	75										
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99	90										
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100	95										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.									
Option	Description													
<i>auto</i>	Set outgoing interface automatically.													



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description									
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

\*\* Values may differ between models.

## config log disk filter

Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type.

```

config log disk filter
  Description: Configure filters for local disk logging. Use these filters to determine the
              log messages to record according to severity and type.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end

```

## config log disk filter

Parameter	Description	Type	Size	Default														
severity	Log to disk every message above and including this severity level.	option	-	information														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.			
Option	Description																	
<i>emergency</i>	Emergency level.																	
<i>alert</i>	Alert level.																	
<i>critical</i>	Critical level.																	
<i>error</i>	Error level.																	
<i>warning</i>	Warning level.																	
<i>notification</i>	Notification level.																	

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description									
<i>information</i>	Information level.									
<i>debug</i>	Debug level.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.			
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									
<i>disable</i>	Disable multicast traffic logging.									
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									

Parameter	Description	Type	Size	Default
filter	Disk log filter.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log eventfilter

Configure log event filters.

```

config log eventfilter
  Description: Configure log event filters.
  set event [enable|disable]
  set system [enable|disable]
  set vpn [enable|disable]
  set user [enable|disable]
  set router [enable|disable]
  set wireless-activity [enable|disable]
  set wan-opt [enable|disable]
  set endpoint [enable|disable]
  set ha [enable|disable]
  set security-rating [enable|disable]
  set fortiextender [enable|disable]
  set connector [enable|disable]
  set sdwan [enable|disable]
  set switch-controller [enable|disable]
end

```

## config log eventfilter

Parameter	Description	Type	Size	Default
event	Enable/disable event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable event logging.		
	<i>disable</i>	Disable event logging.		
system	Enable/disable system event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable system event logging.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable system event logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable system event logging.					
Option	Description									
<i>disable</i>	Disable system event logging.									
vpn	Enable/disable VPN event logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VPN event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VPN event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VPN event logging.	<i>disable</i>	Disable VPN event logging.			
Option	Description									
<i>enable</i>	Enable VPN event logging.									
<i>disable</i>	Disable VPN event logging.									
user	Enable/disable user authentication event logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable user authentication event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable user authentication event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable user authentication event logging.	<i>disable</i>	Disable user authentication event logging.			
Option	Description									
<i>enable</i>	Enable user authentication event logging.									
<i>disable</i>	Disable user authentication event logging.									
router	Enable/disable router event logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable router event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable router event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable router event logging.	<i>disable</i>	Disable router event logging.			
Option	Description									
<i>enable</i>	Enable router event logging.									
<i>disable</i>	Disable router event logging.									
wireless-activity	Enable/disable wireless event logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable wireless event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable wireless event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable wireless event logging.	<i>disable</i>	Disable wireless event logging.			
Option	Description									
<i>enable</i>	Enable wireless event logging.									
<i>disable</i>	Disable wireless event logging.									
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WAN optimization event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WAN optimization event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WAN optimization event logging.	<i>disable</i>	Disable WAN optimization event logging.			
Option	Description									
<i>enable</i>	Enable WAN optimization event logging.									
<i>disable</i>	Disable WAN optimization event logging.									
endpoint	Enable/disable endpoint event logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable endpoint event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable endpoint event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable endpoint event logging.	<i>disable</i>	Disable endpoint event logging.			
Option	Description									
<i>enable</i>	Enable endpoint event logging.									
<i>disable</i>	Disable endpoint event logging.									

Parameter	Description	Type	Size	Default
ha	Enable/disable ha event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ha event logging.		
	<i>disable</i>	Disable ha event logging.		
security-rating	Enable/disable Security Rating result logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Security Fabric audit result logging.		
	<i>disable</i>	Disable Security Fabric audit result logging.		
fortiextender	Enable/disable FortiExtender logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Forti-Extender logging.		
	<i>disable</i>	Disable Forti-Extender logging.		
connector	Enable/disable SDN connector logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SDN connector logging.		
	<i>disable</i>	Disable SDN connector logging.		
sdwan	Enable/disable SD-WAN logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SD-WAN logging.		
	<i>disable</i>	Disable SD-WAN logging.		
switch-controller	Enable/disable Switch-Controller logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		

## config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
  Description: Configure logging to FortiCloud.
```

```

set status [enable|disable]
set upload-option [store-and-upload|realtime|...]
set upload-interval [daily|weekly|...]
set upload-day {user}
set upload-time {user}
set priority [default|low]
set max-log-rate {integer}
set enc-algorithm [high-medium|high|...]
set ssl-min-proto-version [default|SSLv3|...]
set conn-timeout {integer}
set source-ip {ipv4-address}
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config log fortiguard setting

Parameter	Description	Type	Size	Default										
status	Enable/disable logging to FortiCloud.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiCloud.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiCloud.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiCloud.	<i>disable</i>	Disable logging to FortiCloud.							
Option	Description													
<i>enable</i>	Enable logging to FortiCloud.													
<i>disable</i>	Disable logging to FortiCloud.													
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to the hard disk and then upload logs to FortiCloud.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiCloud in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiCloud at 1-minute intervals.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiCloud at 5-minute intervals.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.	<i>realtime</i>	Log directly to FortiCloud in real time.	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.			
Option	Description													
<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.													
<i>realtime</i>	Log directly to FortiCloud in real time.													
<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.													
<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.													
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiCloud once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiCloud once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiCloud once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiCloud once a day.	<i>weekly</i>	Upload log files to FortiCloud once a week.	<i>monthly</i>	Upload log files to FortiCloud once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiCloud once a day.													
<i>weekly</i>	Upload log files to FortiCloud once a week.													
<i>monthly</i>	Upload log files to FortiCloud once a month.													
upload-day	Day of week to roll logs.	user	Not Specified											
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified											

Parameter	Description	Type	Size	Default												
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiCloud log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiCloud log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiCloud log transmission priority to default.	<i>low</i>	Set FortiCloud log transmission priority to low.									
Option	Description															
<i>default</i>	Set FortiCloud log transmission priority to default.															
<i>low</i>	Set FortiCloud log transmission priority to low.															
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using low encryption.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption.	<i>high</i>	Encrypt logs using high encryption.	<i>low</i>	Encrypt logs using low encryption.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption.															
<i>high</i>	Encrypt logs using high encryption.															
<i>low</i>	Encrypt logs using low encryption.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiGate Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600	10												
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified	0.0.0.0												
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortiguard override-setting

Override global FortiCloud logging settings for this VDOM.

```
config log fortiguard override-setting
  Description: Override global FortiCloud logging settings for this VDOM.
  set override [enable|disable]
  set status [enable|disable]
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set priority [default|low]
  set max-log-rate {integer}
end
```

## config log fortiguard override-setting

Parameter	Description	Type	Size	Default						
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override FortiCloud logging settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use global FortiCloud logging settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override FortiCloud logging settings.	<i>disable</i>	Use global FortiCloud logging settings.			
Option	Description									
<i>enable</i>	Override FortiCloud logging settings.									
<i>disable</i>	Use global FortiCloud logging settings.									
status	Enable/disable logging to FortiCloud.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiCloud.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiCloud.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiCloud.	<i>disable</i>	Disable logging to FortiCloud.			
Option	Description									
<i>enable</i>	Enable logging to FortiCloud.									
<i>disable</i>	Disable logging to FortiCloud.									
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute						



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to the hard disk and then upload logs to FortiCloud.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiCloud in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiCloud at 1-minute intervals.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiCloud at 5-minute intervals.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.	<i>realtime</i>	Log directly to FortiCloud in real time.	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.			
Option	Description													
<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.													
<i>realtime</i>	Log directly to FortiCloud in real time.													
<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.													
<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.													
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiCloud once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiCloud once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiCloud once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiCloud once a day.	<i>weekly</i>	Upload log files to FortiCloud once a week.	<i>monthly</i>	Upload log files to FortiCloud once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiCloud once a day.													
<i>weekly</i>	Upload log files to FortiCloud once a week.													
<i>monthly</i>	Upload log files to FortiCloud once a month.													
upload-day	Day of week to roll logs.	user	Not Specified											
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified											
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiCloud log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiCloud log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiCloud log transmission priority to default.	<i>low</i>	Set FortiCloud log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiCloud log transmission priority to default.													
<i>low</i>	Set FortiCloud log transmission priority to low.													
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0										

## config log fortiguard filter

Filters for FortiCloud.

```
config log fortiguard filter
  Description: Filters for FortiCloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
```

```

set filter {string}
set filter-type [include|exclude]
end

```

## config log fortiguard filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	FortiCloud log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortiguard override-filter

Override filters for FortiCloud.

```

config log fortiguard override-filter
  Description: Override filters for FortiCloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end

```

## config log fortiguard override-filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
filter	FortiCloud log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log null-device setting

Settings for null device logging.

```
config log null-device setting
  Description: Settings for null device logging.
  set status [enable|disable]
end
```

## config log null-device setting

Parameter	Description	Type	Size	Default						
status	Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	<i>disable</i>	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).			
Option	Description									
<i>enable</i>	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).									
<i>disable</i>	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).									

## config log null-device filter

Filters for null device logging.

```

config log null-device filter
  Description: Filters for null device logging.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
  
```

## config log null-device filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					

Parameter	Description	Type	Size	Default
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
filter	Null-device log filter.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log setting

Configure general log settings.

```
config log setting
  Description: Configure general log settings.
  set resolve-ip [enable|disable]
  set resolve-port [enable|disable]
  set log-user-in-upper [enable|disable]
  set fwpolicy-implicit-log [enable|disable]
```

```

set fwpolicy6-implicit-log [enable|disable]
set log-invalid-packet [enable|disable]
set local-in-allow [enable|disable]
set local-in-deny-unicast [enable|disable]
set local-in-deny-broadcast [enable|disable]
set local-out [enable|disable]
set daemon-log [enable|disable]
set neighbor-event [enable|disable]
set brief-traffic-format [enable|disable]
set user-anonymize [enable|disable]
set expolicy-implicit-log [enable|disable]
set log-policy-comment [enable|disable]
set faz-override [enable|disable]
set syslog-override [enable|disable]
set custom-log-fields <field-id1>, <field-id2>, ...
end

```

## config log setting

Parameter	Description	Type	Size	Default						
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding resolved domain names to traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding resolved domain names to traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding resolved domain names to traffic logs.	<i>disable</i>	Disable adding resolved domain names to traffic logs.			
Option	Description									
<i>enable</i>	Enable adding resolved domain names to traffic logs.									
<i>disable</i>	Disable adding resolved domain names to traffic logs.									
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding resolved service names to traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding resolved service names to traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding resolved service names to traffic logs.	<i>disable</i>	Disable adding resolved service names to traffic logs.			
Option	Description									
<i>enable</i>	Enable adding resolved service names to traffic logs.									
<i>disable</i>	Disable adding resolved service names to traffic logs.									
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logs with user-in-upper.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logs with user-in-upper.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logs with user-in-upper.	<i>disable</i>	Disable logs with user-in-upper.			
Option	Description									
<i>enable</i>	Enable logs with user-in-upper.									
<i>disable</i>	Disable logs with user-in-upper.									
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable implicit firewall policy logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable implicit firewall policy logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable implicit firewall policy logging.	<i>disable</i>	Disable implicit firewall policy logging.			
Option	Description									
<i>enable</i>	Enable implicit firewall policy logging.									
<i>disable</i>	Disable implicit firewall policy logging.									
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable implicit firewall policy6 logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable implicit firewall policy6 logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable implicit firewall policy6 logging.	<i>disable</i>	Disable implicit firewall policy6 logging.			
Option	Description									
<i>enable</i>	Enable implicit firewall policy6 logging.									
<i>disable</i>	Disable implicit firewall policy6 logging.									
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable invalid packet traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable invalid packet traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable invalid packet traffic logging.	<i>disable</i>	Disable invalid packet traffic logging.			
Option	Description									
<i>enable</i>	Enable invalid packet traffic logging.									
<i>disable</i>	Disable invalid packet traffic logging.									
local-in-allow	Enable/disable local-in-allow logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local-in-allow logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local-in-allow logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local-in-allow logging.	<i>disable</i>	Disable local-in-allow logging.			
Option	Description									
<i>enable</i>	Enable local-in-allow logging.									
<i>disable</i>	Disable local-in-allow logging.									
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local-in-deny-unicast logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local-in-deny-unicast logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local-in-deny-unicast logging.	<i>disable</i>	Disable local-in-deny-unicast logging.			
Option	Description									
<i>enable</i>	Enable local-in-deny-unicast logging.									
<i>disable</i>	Disable local-in-deny-unicast logging.									
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local-in-deny-broadcast logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local-in-deny-broadcast logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local-in-deny-broadcast logging.	<i>disable</i>	Disable local-in-deny-broadcast logging.			
Option	Description									
<i>enable</i>	Enable local-in-deny-broadcast logging.									
<i>disable</i>	Disable local-in-deny-broadcast logging.									
local-out	Enable/disable local-out logging.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local-out logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local-out logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local-out logging.	<i>disable</i>	Disable local-out logging.			
Option	Description									
<i>enable</i>	Enable local-out logging.									
<i>disable</i>	Disable local-out logging.									
daemon-log	Enable/disable daemon logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable daemon logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable daemon logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable daemon logging.	<i>disable</i>	Disable daemon logging.			
Option	Description									
<i>enable</i>	Enable daemon logging.									
<i>disable</i>	Disable daemon logging.									
neighbor-event	Enable/disable neighbor event logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable neighbor event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable neighbor event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable neighbor event logging.	<i>disable</i>	Disable neighbor event logging.			
Option	Description									
<i>enable</i>	Enable neighbor event logging.									
<i>disable</i>	Disable neighbor event logging.									
brief-traffic-format	Enable/disable brief format traffic logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable brief format traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable brief format traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable brief format traffic logging.	<i>disable</i>	Disable brief format traffic logging.			
Option	Description									
<i>enable</i>	Enable brief format traffic logging.									
<i>disable</i>	Disable brief format traffic logging.									
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anonymizing user names in log messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anonymizing user names in log messages.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anonymizing user names in log messages.	<i>disable</i>	Disable anonymizing user names in log messages.			
Option	Description									
<i>enable</i>	Enable anonymizing user names in log messages.									
<i>disable</i>	Disable anonymizing user names in log messages.									
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable explicit proxy firewall implicit policy logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable explicit proxy firewall implicit policy logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable explicit proxy firewall implicit policy logging.	<i>disable</i>	Disable explicit proxy firewall implicit policy logging.			
Option	Description									
<i>enable</i>	Enable explicit proxy firewall implicit policy logging.									
<i>disable</i>	Disable explicit proxy firewall implicit policy logging.									
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inserting policy comments into traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inserting policy comments into traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inserting policy comments into traffic logs.	<i>disable</i>	Disable inserting policy comments into traffic logs.			
Option	Description									
<i>enable</i>	Enable inserting policy comments into traffic logs.									
<i>disable</i>	Disable inserting policy comments into traffic logs.									
faz-override	Enable/disable override FortiAnalyzer settings.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable override FortiAnalyzer settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable override FortiAnalyzer settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable override FortiAnalyzer settings.	<i>disable</i>	Disable override FortiAnalyzer settings.			
Option	Description									
<i>enable</i>	Enable override FortiAnalyzer settings.									
<i>disable</i>	Disable override FortiAnalyzer settings.									
syslog-override	Enable/disable override Syslog settings.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable override Syslog settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable override Syslog settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable override Syslog settings.	<i>disable</i>	Disable override Syslog settings.			
Option	Description									
<i>enable</i>	Enable override Syslog settings.									
<i>disable</i>	Disable override Syslog settings.									
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35							

## config log gui-display

Configure how log messages are displayed on the GUI.

```
config log gui-display
  Description: Configure how log messages are displayed on the GUI.
  set resolve-hosts [enable|disable]
  set resolve-apps [enable|disable]
  set fortiview-unscanned-apps [enable|disable]
end
```

## config log gui-display

Parameter	Description	Type	Size	Default						
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable resolving IP addresses to hostnames.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable resolving IP addresses to hostnames.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable resolving IP addresses to hostnames.	<i>disable</i>	Disable resolving IP addresses to hostnames.			
Option	Description									
<i>enable</i>	Enable resolving IP addresses to hostnames.									
<i>disable</i>	Disable resolving IP addresses to hostnames.									

Parameter	Description	Type	Size	Default						
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable unknown applications on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable unknown applications on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable unknown applications on the GUI.	<i>disable</i>	Disable unknown applications on the GUI.			
Option	Description									
<i>enable</i>	Enable unknown applications on the GUI.									
<i>disable</i>	Disable unknown applications on the GUI.									
fortiview- unscanned- apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable showing unscanned traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable showing unscanned traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable showing unscanned traffic.	<i>disable</i>	Disable showing unscanned traffic.			
Option	Description									
<i>enable</i>	Enable showing unscanned traffic.									
<i>disable</i>	Disable showing unscanned traffic.									

## config log fortianalyzer setting

Global FortiAnalyzer settings.

```

config log fortianalyzer setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```

## config log fortianalyzer setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identity verification of FortiAnalyzer by use of certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identity verification of FortiAnalyzer by use of certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.			
Option	Description									
<i>sha256</i>	Use SHA256 as HMAC algorithm.									
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.															
<i>high</i>	Encrypt logs using high encryption algorithms.															
<i>low</i>	Encrypt logs using all encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5												
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.											
Option	Description															
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description											
<i>realtime</i>	Log directly to FortiAnalyzer in real time.											
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.											
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.			
Option	Description											
<i>daily</i>	Upload log files to FortiAnalyzer once a day.											
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.											
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.											
upload-day	Day of week (month) to upload logs.	user	Not Specified									
upload-time	Time to upload logs (hh:mm).	user	Not Specified									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reliable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reliable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.					
Option	Description											
<i>enable</i>	Enable reliable logging to FortiAnalyzer.											
<i>disable</i>	Disable reliable logging to FortiAnalyzer.											
priority	Set log transmission priority.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.					
Option	Description											
<i>default</i>	Set FortiAnalyzer log transmission priority to default.											
<i>low</i>	Set FortiAnalyzer log transmission priority to low.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
  Description: Override FortiAnalyzer settings.
  set use-management-vdom [enable|disable]
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config log fortianalyzer override-setting

Parameter	Description	Type	Size	Default
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identity verification of FortiAnalyzer by use of certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identity verification of FortiAnalyzer by use of certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
Option	Description															
<i>sha256</i>	Use SHA256 as HMAC algorithm.															
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.															
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.															
<i>high</i>	Encrypt logs using high encryption algorithms.															
<i>low</i>	Encrypt logs using all encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5												
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reliable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reliable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer filter

Filters for FortiAnalyzer.

```
config log fortianalyzer filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DLP archive logging.					
Option	Description									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer override-filter

Parameter	Description	Type	Size	Default												
severity	Lowest severity level to log.	option	-	information												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.			
Option	Description															
<i>emergency</i>	Emergency level.															
<i>alert</i>	Alert level.															
<i>critical</i>	Critical level.															
<i>error</i>	Error level.															
<i>warning</i>	Warning level.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description											
<i>notification</i>	Notification level.											
<i>information</i>	Information level.											
<i>debug</i>	Debug level.											
forward-traffic	Enable/disable forward traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.					
Option	Description											
<i>enable</i>	Enable forward traffic logging.											
<i>disable</i>	Disable forward traffic logging.											
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.					
Option	Description											
<i>enable</i>	Enable local in or out traffic logging.											
<i>disable</i>	Disable local in or out traffic logging.											
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.					
Option	Description											
<i>enable</i>	Enable multicast traffic logging.											
<i>disable</i>	Disable multicast traffic logging.											
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.					
Option	Description											
<i>enable</i>	Enable sniffer traffic logging.											
<i>disable</i>	Disable sniffer traffic logging.											
anomaly	Enable/disable anomaly logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.					
Option	Description											
<i>enable</i>	Enable anomaly logging.											
<i>disable</i>	Disable anomaly logging.											
voip	Enable/disable VoIP logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.							
Option	Description											
<i>enable</i>	Enable VoIP logging.											

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable VoIP logging.					
Option	Description									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DLP archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```

config log fortianalyzer2 setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```



## config log fortianalyzer2 setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identity verification of FortiAnalyzer by use of certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identity verification of FortiAnalyzer by use of certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.			
Option	Description									
<i>sha256</i>	Use SHA256 as HMAC algorithm.									
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.															
<i>high</i>	Encrypt logs using high encryption algorithms.															
<i>low</i>	Encrypt logs using all encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5												
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.											
Option	Description															
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description											
<i>realtime</i>	Log directly to FortiAnalyzer in real time.											
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.											
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.			
Option	Description											
<i>daily</i>	Upload log files to FortiAnalyzer once a day.											
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.											
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.											
upload-day	Day of week (month) to upload logs.	user	Not Specified									
upload-time	Time to upload logs (hh:mm).	user	Not Specified									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reliable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reliable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.					
Option	Description											
<i>enable</i>	Enable reliable logging to FortiAnalyzer.											
<i>disable</i>	Disable reliable logging to FortiAnalyzer.											
priority	Set log transmission priority.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.					
Option	Description											
<i>default</i>	Set FortiAnalyzer log transmission priority to default.											
<i>low</i>	Set FortiAnalyzer log transmission priority to low.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.

```

config log fortianalyzer2 override-setting
  Description: Override FortiAnalyzer settings.
  set use-management-vdom [enable|disable]
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```

## config log fortianalyzer2 override-setting

Parameter	Description	Type	Size	Default
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identity verification of FortiAnalyzer by use of certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identity verification of FortiAnalyzer by use of certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
Option	Description															
<i>sha256</i>	Use SHA256 as HMAC algorithm.															
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.															
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.															
<i>high</i>	Encrypt logs using high encryption algorithms.															
<i>low</i>	Encrypt logs using all encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5												
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reliable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reliable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer2 filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer2 filter

Parameter	Description	Type	Size	Default																
severity	Log every message above and including this severity level.	option	-	information																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.			
Option	Description																			
<i>emergency</i>	Emergency level.																			
<i>alert</i>	Alert level.																			
<i>critical</i>	Critical level.																			
<i>error</i>	Error level.																			
<i>warning</i>	Warning level.																			
<i>notification</i>	Notification level.																			
<i>information</i>	Information level.																			



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>debug</i>	Debug level.					
Option	Description									
<i>debug</i>	Debug level.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.			
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									
<i>disable</i>	Disable multicast traffic logging.									
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									

Parameter	Description	Type	Size	Default						
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DLP archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer 2 log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer2 override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer2 override-filter

Parameter	Description	Type	Size	Default						
severity	Log every message above and including this severity level.	option	-	information						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.			
Option	Description									
<i>emergency</i>	Emergency level.									
<i>alert</i>	Alert level.									

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																	
<i>critical</i>	Critical level.																	
<i>error</i>	Error level.																	
<i>warning</i>	Warning level.																	
<i>notification</i>	Notification level.																	
<i>information</i>	Information level.																	
<i>debug</i>	Debug level.																	
forward-traffic	Enable/disable forward traffic logging.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.											
Option	Description																	
<i>enable</i>	Enable forward traffic logging.																	
<i>disable</i>	Disable forward traffic logging.																	
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.											
Option	Description																	
<i>enable</i>	Enable local in or out traffic logging.																	
<i>disable</i>	Disable local in or out traffic logging.																	
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.											
Option	Description																	
<i>enable</i>	Enable multicast traffic logging.																	
<i>disable</i>	Disable multicast traffic logging.																	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.											
Option	Description																	
<i>enable</i>	Enable sniffer traffic logging.																	
<i>disable</i>	Disable sniffer traffic logging.																	
anomaly	Enable/disable anomaly logging.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.											
Option	Description																	
<i>enable</i>	Enable anomaly logging.																	
<i>disable</i>	Disable anomaly logging.																	

Parameter	Description	Type	Size	Default						
voip	Enable/disable VoIP logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DLP archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer 2 log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```

config log fortianalyzer3 setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}

```

```

set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config log fortianalyzer3 setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identity verification of FortiAnalyzer by use of certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identity verification of FortiAnalyzer by use of certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.					
Option	Description									
<i>sha256</i>	Use SHA256 as HMAC algorithm.									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
Option	Description															
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.															
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.															
<i>high</i>	Encrypt logs using high encryption algorithms.															
<i>low</i>	Encrypt logs using all encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5												
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reliable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reliable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer3 override-setting
  Description: Override FortiAnalyzer settings.
  set use-management-vdom [enable|disable]
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config log fortianalyzer3 override-setting

Parameter	Description	Type	Size	Default
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identity verification of FortiAnalyzer by use of certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identity verification of FortiAnalyzer by use of certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
Option	Description															
<i>sha256</i>	Use SHA256 as HMAC algorithm.															
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.															
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.															
<i>high</i>	Encrypt logs using high encryption algorithms.															
<i>low</i>	Encrypt logs using all encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5												
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reliable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reliable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer3 filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer3 filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DLP archive logging.					
Option	Description									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer 3 log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer3 override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer3 override-filter

Parameter	Description	Type	Size	Default												
severity	Lowest severity level to log.	option	-	information												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.			
Option	Description															
<i>emergency</i>	Emergency level.															
<i>alert</i>	Alert level.															
<i>critical</i>	Critical level.															
<i>error</i>	Error level.															
<i>warning</i>	Warning level.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description											
<i>notification</i>	Notification level.											
<i>information</i>	Information level.											
<i>debug</i>	Debug level.											
forward-traffic	Enable/disable forward traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.					
Option	Description											
<i>enable</i>	Enable forward traffic logging.											
<i>disable</i>	Disable forward traffic logging.											
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.					
Option	Description											
<i>enable</i>	Enable local in or out traffic logging.											
<i>disable</i>	Disable local in or out traffic logging.											
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.					
Option	Description											
<i>enable</i>	Enable multicast traffic logging.											
<i>disable</i>	Disable multicast traffic logging.											
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.					
Option	Description											
<i>enable</i>	Enable sniffer traffic logging.											
<i>disable</i>	Disable sniffer traffic logging.											
anomaly	Enable/disable anomaly logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.					
Option	Description											
<i>enable</i>	Enable anomaly logging.											
<i>disable</i>	Disable anomaly logging.											
voip	Enable/disable VoIP logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.							
Option	Description											
<i>enable</i>	Enable VoIP logging.											

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable VoIP logging.					
Option	Description									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DLP archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer 3 log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer-cloud setting

Global FortiAnalyzer Cloud settings.

```

config log fortianalyzer-cloud setting
  Description: Global FortiAnalyzer Cloud settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```



## config log fortianalyzer-cloud setting

Parameter	Description	Type	Size	Default								
status	Enable/disable logging to FortiAnalyzer.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging to FortiAnalyzer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging to FortiAnalyzer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.					
Option	Description											
<i>enable</i>	Enable logging to FortiAnalyzer.											
<i>disable</i>	Disable logging to FortiAnalyzer.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS packet archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS packet archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
Option	Description											
<i>enable</i>	Enable IPS packet archive logging.											
<i>disable</i>	Disable IPS packet archive logging.											
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAnalyzer access to configuration and data.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAnalyzer access to configuration and data.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.					
Option	Description											
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.											
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha256</i></td> <td>Use SHA256 as HMAC algorithm.</td> </tr> <tr> <td><i>sha1</i></td> <td>Step down to SHA1 as the HMAC algorithm.</td> </tr> </tbody> </table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
Option	Description											
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high-medium</i></td> <td>Encrypt logs using high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>Encrypt logs using high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>Encrypt logs using all encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
Option	Description											
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.											
<i>high</i>	Encrypt logs using high encryption algorithms.											
<i>low</i>	Encrypt logs using all encryption algorithms.											
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.							
Option	Description											
<i>default</i>	Follow system global setting.											

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description													
<i>SSLv3</i>	SSLv3.													
<i>TLSv1</i>	TLSv1.													
<i>TLSv1-1</i>	TLSv1.1.													
<i>TLSv1-2</i>	TLSv1.2.													
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10										
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5										
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35											
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63											
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td> <td>Log to hard disk and then upload to FortiAnalyzer.</td> </tr> <tr> <td><i>realtime</i></td> <td>Log directly to FortiAnalyzer in real time.</td> </tr> <tr> <td><i>1-minute</i></td> <td>Log directly to FortiAnalyzer at least every 1 minute.</td> </tr> <tr> <td><i>5-minute</i></td> <td>Log directly to FortiAnalyzer at least every 5 minutes.</td> </tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>daily</i></td> <td>Upload log files to FortiAnalyzer once a day.</td> </tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.									
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>weekly</i></td> <td>Upload log files to FortiAnalyzer once a week.</td> </tr> <tr> <td><i>monthly</i></td> <td>Upload log files to FortiAnalyzer once a month.</td> </tr> </tbody> </table>	Option	Description	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description											
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.											
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.											
upload-day	Day of week (month) to upload logs.	user	Not Specified									
upload-time	Time to upload logs (hh:mm).	user	Not Specified									
priority	Set log transmission priority.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Set FortiAnalyzer log transmission priority to default.</td> </tr> <tr> <td><i>low</i></td> <td>Set FortiAnalyzer log transmission priority to low.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.					
Option	Description											
<i>default</i>	Set FortiAnalyzer log transmission priority to default.											
<i>low</i>	Set FortiAnalyzer log transmission priority to low.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config log fortianalyzer-cloud override-setting

Override FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud override-setting
  Description: Override FortiAnalyzer Cloud settings.
  set status [enable|disable]
end
```

## config log fortianalyzer-cloud override-setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable logging to FortiAnalyzer.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									

## config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud filter
  Description: Filters for FortiAnalyzer Cloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end
```

## config log fortianalyzer-cloud filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></tbody></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DLP archive logging.					
Option	Description									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer Cloud log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```

config log fortianalyzer-cloud override-filter
  Description: Override filters for FortiAnalyzer Cloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
end

```

## config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size	Default												
severity	Lowest severity level to log.	option	-	information												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.			
Option	Description															
<i>emergency</i>	Emergency level.															
<i>alert</i>	Alert level.															
<i>critical</i>	Critical level.															
<i>error</i>	Error level.															
<i>warning</i>	Warning level.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description											
<i>notification</i>	Notification level.											
<i>information</i>	Information level.											
<i>debug</i>	Debug level.											
forward-traffic	Enable/disable forward traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forward traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forward traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.					
Option	Description											
<i>enable</i>	Enable forward traffic logging.											
<i>disable</i>	Disable forward traffic logging.											
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local in or out traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local in or out traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.					
Option	Description											
<i>enable</i>	Enable local in or out traffic logging.											
<i>disable</i>	Disable local in or out traffic logging.											
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.					
Option	Description											
<i>enable</i>	Enable multicast traffic logging.											
<i>disable</i>	Disable multicast traffic logging.											
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer traffic logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer traffic logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.					
Option	Description											
<i>enable</i>	Enable sniffer traffic logging.											
<i>disable</i>	Disable sniffer traffic logging.											
anomaly	Enable/disable anomaly logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable anomaly logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable anomaly logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.					
Option	Description											
<i>enable</i>	Enable anomaly logging.											
<i>disable</i>	Disable anomaly logging.											
voip	Enable/disable VoIP logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP logging.							
Option	Description											
<i>enable</i>	Enable VoIP logging.											

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable VoIP logging.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable VoIP logging.					
Option	Description									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DLP archive logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DLP archive logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
filter	FortiAnalyzer Cloud log filter.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include</i></td> <td>Include logs that match the filter.</td> </tr> <tr> <td><i>exclude</i></td> <td>Exclude logs that match the filter.</td> </tr> </tbody> </table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									



## mgmt-data

This section includes syntax for the following commands:

- [config mgmt-data status on page 537](#)

### config mgmt-data status

mgmt-data status.

```
config mgmt-data status
  Description: mgmt-data status.
end
```

## router

This section includes syntax for the following commands:

- [config router info6 on page 662](#)
- [config router prefix-list on page 541](#)
- [config router ripng on page 557](#)
- [config router static6 on page 569](#)
- [config router setting on page 662](#)
- [config router prefix-list6 on page 542](#)
- [config router ospf6 on page 586](#)
- [config router multicast on page 651](#)
- [config router aspath-list on page 540](#)
- [config router access-list on page 538](#)
- [config router multicast-flow on page 650](#)
- [config router bgp on page 599](#)
- [config router static on page 562](#)
- [config router route-map on page 545](#)
- [config router ospf on page 571](#)
- [config router policy6 on page 568](#)
- [config router key-chain on page 543](#)
- [config router rip on page 551](#)
- [config router access-list6 on page 539](#)
- [config router bfd on page 663](#)
- [config router community-list on page 544](#)
- [config router multicast6 on page 660](#)
- [config router info on page 661](#)
- [config router auth-path on page 662](#)
- [config router policy on page 565](#)
- [config router isis on page 638](#)
- [config router bfd6 on page 663](#)

### config router access-list

Configure access lists.

```
config router access-list
  Description: Configure access lists.
  edit <name>
    set comments {string}
  config rule
    Description: Rule.
    edit <id>
      set action [permit|deny]
      set prefix {user}
```

```

        set wildcard {user}
        set exact-match [enable|disable]
        set flags {integer}
    next
end
next
end

```

## config router access-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default						
action	Permit or deny this IP address and netmask prefix.	option	-	permit						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>permit</i></td> <td>Permit or allow this IP address and netmask prefix.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny this IP address and netmask prefix.</td> </tr> </tbody> </table>	Option	Description	<i>permit</i>	Permit or allow this IP address and netmask prefix.	<i>deny</i>	Deny this IP address and netmask prefix.			
Option	Description									
<i>permit</i>	Permit or allow this IP address and netmask prefix.									
<i>deny</i>	Deny this IP address and netmask prefix.									
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified							
wildcard	Wildcard to define Cisco-style wildcard filter criteria.	user	Not Specified							
exact-match	Enable/disable exact match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable exact match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable exact match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable exact match.	<i>disable</i>	Disable exact match.			
Option	Description									
<i>enable</i>	Enable exact match.									
<i>disable</i>	Disable exact match.									
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config router access-list6

Configure IPv6 access lists.

```

config router access-list6
    Description: Configure IPv6 access lists.
    edit <name>

```

```

set comments {string}
config rule
  Description: Rule.
  edit <id>
    set action [permit|deny]
    set prefix6 {user}
    set exact-match [enable|disable]
    set flags {integer}
  next
end
next
end

```

## config router access-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default						
action	Permit or deny this IP address and netmask prefix.	option	-	permit						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>permit</i></td> <td>Permit or allow this IP address and netmask prefix.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny this IP address and netmask prefix.</td> </tr> </tbody> </table>	Option	Description	<i>permit</i>	Permit or allow this IP address and netmask prefix.	<i>deny</i>	Deny this IP address and netmask prefix.			
Option	Description									
<i>permit</i>	Permit or allow this IP address and netmask prefix.									
<i>deny</i>	Deny this IP address and netmask prefix.									
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified							
exact-match	Enable/disable exact prefix match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable exact match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable exact match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable exact match.	<i>disable</i>	Disable exact match.			
Option	Description									
<i>enable</i>	Enable exact match.									
<i>disable</i>	Disable exact match.									
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config router aspath-list

Configure Autonomous System (AS) path lists.

```

config router aspath-list
  Description: Configure Autonomous System (AS) path lists.
  edit <name>
    config rule
      Description: AS path list rule.
      edit <id>
        set action [deny|permit]
        set regexp {string}
      next
    end
  next
end

```

### config rule

Parameter	Description	Type	Size	Default						
action	Permit or deny route-based operations, based on the route's AS_PATH attribute.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>deny</i></td> <td>Deny route-based operations.</td> </tr> <tr> <td><i>permit</i></td> <td>Permit route-based operations.</td> </tr> </tbody> </table>	Option	Description	<i>deny</i>	Deny route-based operations.	<i>permit</i>	Permit route-based operations.			
Option	Description									
<i>deny</i>	Deny route-based operations.									
<i>permit</i>	Permit route-based operations.									
regexp	Regular-expression to match the Border Gateway Protocol (BGP) AS paths.	string	Maximum length: 63							

### config router prefix-list

Configure IPv4 prefix lists.

```

config router prefix-list
  Description: Configure IPv4 prefix lists.
  edit <name>
    set comments {string}
    config rule
      Description: IPv4 prefix list rule.
      edit <id>
        set action [permit|deny]
        set prefix {user}
        set ge {integer}
        set le {integer}
        set flags {integer}
      next
    end
  next
end

```

## config router prefix-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default						
action	Permit or deny this IP address and netmask prefix.	option	-	permit						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>permit</i></td><td>Allow or permit packets that match this rule.</td></tr><tr><td><i>deny</i></td><td>Deny packets that match this rule.</td></tr></tbody></table>	Option	Description	<i>permit</i>	Allow or permit packets that match this rule.	<i>deny</i>	Deny packets that match this rule.			
Option	Description									
<i>permit</i>	Allow or permit packets that match this rule.									
<i>deny</i>	Deny packets that match this rule.									
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	0.0.0.0 0.0.0.0						
ge	Minimum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 32							
le	Maximum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 32							
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config router prefix-list6

Configure IPv6 prefix lists.

```
config router prefix-list6
  Description: Configure IPv6 prefix lists.
  edit <name>
    set comments {string}
    config rule
      Description: IPv6 prefix list rule.
      edit <id>
        set action [permit|deny]
        set prefix6 {user}
        set ge {integer}
        set le {integer}
```

```

        set flags {integer}
    next
end
next
end

```

## config router prefix-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default						
action	Permit or deny packets that match this rule.	option	-	permit						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>permit</i></td> <td>Allow or permit packets that match this rule.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny packets that match this rule.</td> </tr> </tbody> </table>	Option	Description	<i>permit</i>	Allow or permit packets that match this rule.	<i>deny</i>	Deny packets that match this rule.			
Option	Description									
<i>permit</i>	Allow or permit packets that match this rule.									
<i>deny</i>	Deny packets that match this rule.									
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified							
ge	Minimum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 128							
le	Maximum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 128							
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config router key-chain

Configure key-chain.

```

config router key-chain
  Description: Configure key-chain.
  edit <name>
    config key
      Description: Configuration method to edit key settings.
    
```

```

    edit <id>
      set accept-lifetime {user}
      set send-lifetime {user}
      set key-string {string}
    next
  end
next
end

```

## config key

Parameter	Description	Type	Size	Default
accept-lifetime	Lifetime of received authentication key (format: hh:mm:ss day month year).	user	Not Specified	
send-lifetime	Lifetime of sent authentication key (format: hh:mm:ss day month year).	user	Not Specified	
key-string	Password for the key (max. = 35 characters).	string	Maximum length: 35	

## config router community-list

Configure community lists.

```

config router community-list
  Description: Configure community lists.
  edit <name>
    set type [standard|expanded]
    config rule
      Description: Community list rule.
      edit <id>
        set action [deny|permit]
        set regexp {string}
        set match {string}
      next
    end
  next
end

```

## config router community-list

Parameter	Description	Type	Size	Default
type	Community list type (standard or expanded).	option	-	standard
	<b>Option</b>	<b>Description</b>		
	<i>standard</i>	Standard community list type.		
	<i>expanded</i>	Expanded community list type.		



## config rule

Parameter	Description	Type	Size	Default						
action	Permit or deny route-based operations, based on the route's COMMUNITY attribute.	option	-							
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>deny</i></td><td>Deny route-based operations.</td></tr><tr><td><i>permit</i></td><td>Permit or allow route-based operations.</td></tr></tbody></table>	Option	Description	<i>deny</i>	Deny route-based operations.	<i>permit</i>	Permit or allow route-based operations.			
Option	Description									
<i>deny</i>	Deny route-based operations.									
<i>permit</i>	Permit or allow route-based operations.									
regexp	Ordered list of COMMUNITY attributes as a regular expression.	string	Maximum length: 255							
match	Community specifications for matching a reserved community.	string	Maximum length: 255							

## config router route-map

Configure route maps.

```
config router route-map
  Description: Configure route maps.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set match-as-path {string}
        set match-community {string}
        set match-community-exact [enable|disable]
        set match-origin [none|egp|...]
        set match-interface {string}
        set match-ip-address {string}
        set match-ip6-address {string}
        set match-ip-nexthop {string}
        set match-ip6-nexthop {string}
        set match-metric {integer}
        set match-route-type [1|2|...]
        set match-tag {integer}
        set match-vrf {integer}
        set set-aggregator-as {integer}
        set set-aggregator-ip {ipv4-address-any}
        set set-aspath-action [prepend|replace]
        set set-aspath <as1>, <as2>, ...
        set set-atomic-aggregate [enable|disable]
        set set-community-delete {string}
        set set-community <community1>, <community2>, ...
        set set-community-additive [enable|disable]
        set set-dampening-reachability-half-life {integer}
        set set-dampening-reuse {integer}
        set set-dampening-suppress {integer}
```

```

set set-dampening-max-suppress {integer}
set set-dampening-unreachability-half-life {integer}
set set-extcommunity-rt <community1>, <community2>, ...
set set-extcommunity-soo <community1>, <community2>, ...
set set-ip-nexthop {ipv4-address}
set set-ip6-nexthop {ipv6-address}
set set-ip6-nexthop-local {ipv6-address}
set set-local-preference {integer}
set set-metric {integer}
set set-metric-type [1|2|...]
set set-originator-id {ipv4-address-any}
set set-origin [none|egp|...]
set set-tag {integer}
set set-weight {integer}
set set-flags {integer}
set match-flags {integer}
set set-route-tag {integer}
next
end
next
end

```

## config router route-map

Parameter	Description	Type	Size	Default
comments	Optional comments.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default						
action	Action.	option	-	permit						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>permit</i></td> <td>Permit.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny.</td> </tr> </tbody> </table>	Option	Description	<i>permit</i>	Permit.	<i>deny</i>	Deny.			
Option	Description									
<i>permit</i>	Permit.									
<i>deny</i>	Deny.									
match-as-path	Match BGP AS path list.	string	Maximum length: 35							
match-community	Match BGP community list.	string	Maximum length: 35							
match-community-exact	Enable/disable exact matching of communities.	option	-	disable						

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable exact matching of communities.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable exact matching of communities.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable exact matching of communities.	<i>disable</i>	Disable exact matching of communities.							
Option	Description													
<i>enable</i>	Enable exact matching of communities.													
<i>disable</i>	Disable exact matching of communities.													
match-origin	Match BGP origin code.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>egp</i></td> <td>Remote EGP.</td> </tr> <tr> <td><i>igp</i></td> <td>Local IGP.</td> </tr> <tr> <td><i>incomplete</i></td> <td>Unknown heritage.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>egp</i>	Remote EGP.	<i>igp</i>	Local IGP.	<i>incomplete</i>	Unknown heritage.			
Option	Description													
<i>none</i>	None.													
<i>egp</i>	Remote EGP.													
<i>igp</i>	Local IGP.													
<i>incomplete</i>	Unknown heritage.													
match-interface	Match interface configuration.	string	Maximum length: 15											
match-ip-address	Match IP address permitted by access-list or prefix-list.	string	Maximum length: 35											
match-ip6-address	Match IPv6 address permitted by access-list6 or prefix-list6.	string	Maximum length: 35											
match-ip-nexthop	Match next hop IP address passed by access-list or prefix-list.	string	Maximum length: 35											
match-ip6-nexthop	Match next hop IPv6 address passed by access-list6 or prefix-list6.	string	Maximum length: 35											
match-metric	Match metric for redistribute routes.	integer	Minimum value: 0 Maximum value: 4294967295											
match-route-type	Match route type.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>External type 1.</td> </tr> <tr> <td><i>2</i></td> <td>External type 2.</td> </tr> <tr> <td><i>none</i></td> <td>No type specified.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	External type 1.	<i>2</i>	External type 2.	<i>none</i>	No type specified.					
Option	Description													
<i>1</i>	External type 1.													
<i>2</i>	External type 2.													
<i>none</i>	No type specified.													

Parameter	Description	Type	Size	Default						
match-tag	Match tag.	integer	Minimum value: 0 Maximum value: 4294967295							
match-vrf	Match VRF ID.	integer	Minimum value: 0 Maximum value: 31							
set-aggregator-as	BGP aggregator AS.	integer	Minimum value: 0 Maximum value: 4294967295	0						
set-aggregator-ip	BGP aggregator IP.	ipv4-address-any	Not Specified	0.0.0.0						
set-aspaction	Specify preferred action of set-aspaction.	option	-	prepend						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>prepend</i></td> <td>Prepend.</td> </tr> <tr> <td><i>replace</i></td> <td>Replace.</td> </tr> </tbody> </table>	Option	Description	<i>prepend</i>	Prepend.	<i>replace</i>	Replace.			
Option	Description									
<i>prepend</i>	Prepend.									
<i>replace</i>	Replace.									
set-aspaction <as>	Prepend BGP AS path attribute. AS number (0 - 42949672). NOTE: Use quotes for repeating numbers, e.g.: "1 1 2"	string	Maximum length: 79							
set-atomic-aggregate	Enable/disable BGP atomic aggregate attribute.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable BGP atomic aggregate attribute.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable BGP atomic aggregate attribute.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable BGP atomic aggregate attribute.	<i>disable</i>	Disable BGP atomic aggregate attribute.			
Option	Description									
<i>enable</i>	Enable BGP atomic aggregate attribute.									
<i>disable</i>	Disable BGP atomic aggregate attribute.									
set-community-delete	Delete communities matching community list.	string	Maximum length: 35							
set-community <community>	BGP community attribute. Attribute: AA AA:NN internet local-AS no-advertise no-export.	string	Maximum length: 79							
set-community-additive	Enable/disable adding set-community to existing community.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding set-community to existing community.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding set-community to existing community.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding set-community to existing community.	<i>disable</i>	Disable adding set-community to existing community.			
Option	Description									
<i>enable</i>	Enable adding set-community to existing community.									
<i>disable</i>	Disable adding set-community to existing community.									
set-dampening-reachability-half-life	Reachability half-life time for the penalty .	integer	Minimum value: 0 Maximum value: 45	0						
set-dampening-reuse	Value to start reusing a route .	integer	Minimum value: 0 Maximum value: 20000	0						
set-dampening-suppress	Value to start suppressing a route .	integer	Minimum value: 0 Maximum value: 20000	0						
set-dampening-max-suppress	Maximum duration to suppress a route .	integer	Minimum value: 0 Maximum value: 255	0						
set-dampening-unreachability-half-life	Unreachability Half-life time for the penalty	integer	Minimum value: 0 Maximum value: 45	0						
set-extcommunity-rt <community>	Route Target extended community. AA:NN.	string	Maximum length: 79							
set-extcommunity-soo <community>	Site-of-Origin extended community. AA:NN	string	Maximum length: 79							
set-ip-nexthop	IP address of next hop.	ipv4-address	Not Specified							
set-ip6-nexthop	IPv6 global address of next hop.	ipv6-address	Not Specified							
set-ip6-nexthop-local	IPv6 local address of next hop.	ipv6-address	Not Specified							

Parameter	Description	Type	Size	Default										
set-local-preference	BGP local preference path attribute.	integer	Minimum value: 0 Maximum value: 4294967295											
set-metric	Metric value.	integer	Minimum value: 0 Maximum value: 4294967295											
set-metric-type	Metric type.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>External type 1.</td> </tr> <tr> <td>2</td> <td>External type 2.</td> </tr> <tr> <td>none</td> <td>No type specified.</td> </tr> </tbody> </table>	Option	Description	1	External type 1.	2	External type 2.	none	No type specified.					
Option	Description													
1	External type 1.													
2	External type 2.													
none	No type specified.													
set-originator-id	BGP originator ID attribute.	ipv4-address-any	Not Specified											
set-origin	BGP origin code.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>none</td> <td>None.</td> </tr> <tr> <td>egp</td> <td>Remote EGP.</td> </tr> <tr> <td>igp</td> <td>Local IGP.</td> </tr> <tr> <td>incomplete</td> <td>Unknown heritage.</td> </tr> </tbody> </table>	Option	Description	none	None.	egp	Remote EGP.	igp	Local IGP.	incomplete	Unknown heritage.			
Option	Description													
none	None.													
egp	Remote EGP.													
igp	Local IGP.													
incomplete	Unknown heritage.													
set-tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295											
set-weight	BGP weight for routing table.	integer	Minimum value: 0 Maximum value: 4294967295											

Parameter	Description	Type	Size	Default
set-flags	BGP flags value	integer	Minimum value: 0 Maximum value: 65535	0
match-flags	BGP flag value to match	integer	Minimum value: 0 Maximum value: 65535	0
set-route-tag	Route tag for routing table.	integer	Minimum value: 0 Maximum value: 4294967295	

## config router rip

Configure RIP.

```

config router rip
  Description: Configure RIP.
  set default-information-originate [enable|disable]
  set default-metric {integer}
  set max-out-metric {integer}
  set recv-buffer-size {integer}
  config distance
    Description: distance
    edit <id>
      set prefix {ipv4-classnet-any}
      set distance {integer}
      set access-list {string}
    next
  end
  config distribute-list
    Description: Distribute list.
    edit <id>
      set status [enable|disable]
      set direction [in|out]
      set listname {string}
      set interface {string}
    next
  end
  config neighbor
    Description: neighbor
    edit <id>
      set ip {ipv4-address}
    next
  end
  config network
    Description: network
    edit <id>
      set prefix {ipv4-classnet}

```

```

    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set status [enable|disable]
        set direction [in|out]
        set access-list {string}
        set offset {integer}
        set interface {string}
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
    next
end
set update-timer {integer}
set timeout-timer {integer}
set garbage-timer {integer}
set version [1|2]
config interface
    Description: RIP interface configuration.
    edit <name>
        set auth-keychain {string}
        set auth-mode [none|text|...]
        set auth-string {password}
        set receive-version {option1}, {option2}, ...
        set send-version {option1}, {option2}, ...
        set send-version2-broadcast [disable|enable]
        set split-horizon-status [enable|disable]
        set split-horizon [poisoned|regular]
        set flags {integer}
    next
end
end
end

```

## config router rip

Parameter	Description	Type	Size	Default						
default-information-originate	Enable/disable generation of default route.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									



Parameter	Description	Type	Size	Default						
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1						
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0						
recv-buffer-size	Receiving buffer size.	integer	Minimum value: 8129 Maximum value: 2147483647	65536 **						
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							
update-timer	Update timer in seconds.	integer	Minimum value: 1 Maximum value: 2147483647	30						
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	180						
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	120						
version	RIP version.	option	-	2						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Version 1.</td> </tr> <tr> <td>2</td> <td>Version 2.</td> </tr> </tbody> </table>	Option	Description	1	Version 1.	2	Version 2.			
Option	Description									
1	Version 1.									
2	Version 2.									

\*\* Values may differ between models.

## config distance

Parameter	Description	Type	Size	Default
prefix	Distance prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
distance	Distance .	integer	Minimum value: 1 Maximum value: 255	0
access-list	Access list for route destination.	string	Maximum length: 35	

## config distribute-list

Parameter	Description	Type	Size	Default						
status	status	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
direction	Distribute list direction.	option	-	out						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></tbody></table>	Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.			
Option	Description									
<i>in</i>	Filter incoming packets.									
<i>out</i>	Filter outgoing packets.									
listname	Distribute access/prefix list name.	string	Maximum length: 35							
interface	Distribute list interface name.	string	Maximum length: 15							

## config neighbor

Parameter	Description	Type	Size	Default
ip	IP address.	ipv4-address	Not Specified	0.0.0.0

## config network

Parameter	Description	Type	Size	Default
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config offset-list

Parameter	Description	Type	Size	Default						
status	status	option	-	enable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
direction	Offset list direction.	option	-	out						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></tbody></table>	Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.			
Option	Description									
<i>in</i>	Filter incoming packets.									
<i>out</i>	Filter outgoing packets.									
access-list	Access list name.	string	Maximum length: 35							
offset	offset	integer	Minimum value: 1 Maximum value: 16	0						
interface	Interface name.	string	Maximum length: 15							

## config redistribute

Parameter	Description	Type	Size	Default						
status	status	option	-	disable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
routemap	Route map name.	string	Maximum length: 35	

## config interface

Parameter	Description	Type	Size	Default								
auth-keychain	Authentication key-chain name.	string	Maximum length: 35									
auth-mode	Authentication mode.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>text</i></td> <td>Text.</td> </tr> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>md5</i>	MD5.			
Option	Description											
<i>none</i>	None.											
<i>text</i>	Text.											
<i>md5</i>	MD5.											
auth-string	Authentication string/password.	password	Not Specified									
receive-version	Receive version.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>Version 1.</td> </tr> <tr> <td><i>2</i></td> <td>Version 2.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	Version 1.	<i>2</i>	Version 2.					
Option	Description											
<i>1</i>	Version 1.											
<i>2</i>	Version 2.											
send-version	Send version.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>Version 1.</td> </tr> <tr> <td><i>2</i></td> <td>Version 2.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	Version 1.	<i>2</i>	Version 2.					
Option	Description											
<i>1</i>	Version 1.											
<i>2</i>	Version 2.											
send-version2-broadcast	Enable/disable broadcast version 1 compatible packets.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable broadcasting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable broadcasting.							
Option	Description											
<i>disable</i>	Disable broadcasting.											

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable broadcasting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable broadcasting.					
Option	Description									
<i>enable</i>	Enable broadcasting.									
split-horizon-status	Enable/disable split horizon.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
split-horizon	Enable/disable split horizon.	option	-	poisoned						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>poisoned</i></td> <td>Poisoned.</td> </tr> <tr> <td><i>regular</i></td> <td>Regular.</td> </tr> </tbody> </table>	Option	Description	<i>poisoned</i>	Poisoned.	<i>regular</i>	Regular.			
Option	Description									
<i>poisoned</i>	Poisoned.									
<i>regular</i>	Regular.									
flags	flags	integer	Minimum value: 0 Maximum value: 255	8						

## config router ripng

Configure RIPng.

```

config router ripng
  Description: Configure RIPng.
  set default-information-originate [enable|disable]
  set default-metric {integer}
  set max-out-metric {integer}
  config distance
    Description: distance
    edit <id>
      set distance {integer}
      set prefix6 {ipv6-prefix}
      set access-list6 {string}
    next
  end
  config distribute-list
    Description: Distribute list.
    edit <id>
      set status [enable|disable]
      set direction [in|out]
      set listname {string}
      set interface {string}
    next
  end
config neighbor

```

```

Description: neighbor
edit <id>
    set ip6 {ipv6-address}
    set interface {string}
next
end
config network
Description: Network.
edit <id>
    set prefix {ipv6-prefix}
next
end
config aggregate-address
Description: Aggregate address.
edit <id>
    set prefix6 {ipv6-prefix}
next
end
config offset-list
Description: Offset list.
edit <id>
    set status [enable|disable]
    set direction [in|out]
    set access-list6 {string}
    set offset {integer}
    set interface {string}
next
end
set passive-interface <name1>, <name2>, ...
config redistribute
Description: Redistribute configuration.
edit <name>
    set status [enable|disable]
    set metric {integer}
    set routemap {string}
next
end
set update-timer {integer}
set timeout-timer {integer}
set garbage-timer {integer}
config interface
Description: RIPng interface configuration.
edit <name>
    set split-horizon-status [enable|disable]
    set split-horizon [poisoned|regular]
    set flags {integer}
next
end
end

```

## config router ripng

Parameter	Description	Type	Size	Default						
default-information-originate	Enable/disable generation of default route.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1						
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0						
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							
update-timer	Update timer.	integer	Minimum value: 5 Maximum value: 2147483647	30						
timeout-timer	Timeout timer.	integer	Minimum value: 5 Maximum value: 2147483647	180						
garbage-timer	Garbage timer.	integer	Minimum value: 5 Maximum value: 2147483647	120						

## config distance

Parameter	Description	Type	Size	Default
distance	Distance .	integer	Minimum value: 1 Maximum value: 255	0
prefix6	Distance prefix6.	ipv6-prefix	Not Specified	::/0
access-list6	Access list for route destination.	string	Maximum length: 35	

## config distribute-list

Parameter	Description	Type	Size	Default						
status	status	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
direction	Distribute list direction.	option	-	out						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></tbody></table>	Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.			
Option	Description									
<i>in</i>	Filter incoming packets.									
<i>out</i>	Filter outgoing packets.									
listname	Distribute access/prefix list name.	string	Maximum length: 35							
interface	Distribute list interface name.	string	Maximum length: 15							

## config neighbor

Parameter	Description	Type	Size	Default
ip6	IPv6 link-local address.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	



## config network

Parameter	Description	Type	Size	Default
prefix	Network IPv6 link-local prefix.	ipv6-prefix	Not Specified	::/0

## config aggregate-address

Parameter	Description	Type	Size	Default
prefix6	Aggregate address prefix.	ipv6-prefix	Not Specified	::/0

## config offset-list

Parameter	Description	Type	Size	Default						
status	status	option	-	enable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
direction	Offset list direction.	option	-	out						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></tbody></table>	Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.			
Option	Description									
<i>in</i>	Filter incoming packets.									
<i>out</i>	Filter outgoing packets.									
access-list6	IPv6 access list name.	string	Maximum length: 35							
offset	offset	integer	Minimum value: 1 Maximum value: 16	0						
interface	Interface name.	string	Maximum length: 15							

## config redistribute

Parameter	Description	Type	Size	Default
status	status	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0						
routemap	Route map name.	string	Maximum length: 35							

### config interface

Parameter	Description	Type	Size	Default						
split-horizon-status	Enable/disable split horizon.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
split-horizon	Enable/disable split horizon.	option	-	poisoned						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>poisoned</i></td> <td>Poisoned.</td> </tr> <tr> <td><i>regular</i></td> <td>Regular.</td> </tr> </tbody> </table>	Option	Description	<i>poisoned</i>	Poisoned.	<i>regular</i>	Regular.			
Option	Description									
<i>poisoned</i>	Poisoned.									
<i>regular</i>	Regular.									
flags	Flags.	integer	Minimum value: 0 Maximum value: 255	8						

### config router static

Configure IPv4 static routing tables.

```

config router static
  Description: Configure IPv4 static routing tables.
  edit <seq-num>
    set status [enable|disable]
    set dst {ipv4-classnet}
    set src {ipv4-classnet}
    set gateway {ipv4-address}
    set distance {integer}

```

```

set weight {integer}
set priority {integer}
set device {string}
set comment {var-string}
set blackhole [enable|disable]
set dynamic-gateway [enable|disable]
set sdwan [enable|disable]
set dstaddr {string}
set internet-service {integer}
set internet-service-custom {string}
set link-monitor-exempt [enable|disable]
set vrf {integer}
set bfd [enable|disable]
next
end

```

## config router static

Parameter	Description	Type	Size	Default						
status	Enable/disable this static route.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable static route.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable static route.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable static route.	<i>disable</i>	Disable static route.			
Option	Description									
<i>enable</i>	Enable static route.									
<i>disable</i>	Disable static route.									
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
src	Source prefix for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0						
distance	Administrative distance .	integer	Minimum value: 1 Maximum value: 255	10						
weight	Administrative weight .	integer	Minimum value: 0 Maximum value: 255	0						
priority	Administrative priority .	integer	Minimum value: 0 Maximum value: 65535	0						
device	Gateway out interface or tunnel.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
blackhole	Enable/disable black hole.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable black hole.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable black hole.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.			
Option	Description									
<i>enable</i>	Enable black hole.									
<i>disable</i>	Disable black hole.									
dynamic-gateway	Enable use of dynamic gateway retrieved from a DHCP or PPP server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dynamic gateway.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dynamic gateway.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dynamic gateway.	<i>disable</i>	Disable dynamic gateway.			
Option	Description									
<i>enable</i>	Enable dynamic gateway.									
<i>disable</i>	Disable dynamic gateway.									
sdwan	Enable/disable egress through SD-WAN.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SD-WAN access.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SD-WAN access.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SD-WAN access.	<i>disable</i>	Disable SD-WAN access.			
Option	Description									
<i>enable</i>	Enable SD-WAN access.									
<i>disable</i>	Disable SD-WAN access.									
dstaddr	Name of firewall address or address group.	string	Maximum length: 79							
internet-service	Application ID in the Internet service database.	integer	Minimum value: 0 Maximum value: 4294967295	0						
internet-service-custom	Application name in the Internet service custom database.	string	Maximum length: 64							
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Keep this static route when link monitor or health check is down.</td> </tr> <tr> <td><i>disable</i></td> <td>Withdraw this static route when link monitor or health check is down. (default)</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Keep this static route when link monitor or health check is down.	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)			
Option	Description									
<i>enable</i>	Keep this static route when link monitor or health check is down.									
<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)									

Parameter	Description	Type	Size	Default
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable

Option	Description
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).

## config router policy

Configure IPv4 routing policies.

```

config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set input-device <name1>, <name2>, ...
    set input-device-negate [enable|disable]
    set src <subnet1>, <subnet2>, ...
    set srcaddr <name1>, <name2>, ...
    set src-negate [enable|disable]
    set dst <subnet1>, <subnet2>, ...
    set dstaddr <name1>, <name2>, ...
    set dst-negate [enable|disable]
    set action [deny|permit]
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set start-source-port {integer}
    set end-source-port {integer}
    set gateway {ipv4-address}
    set output-device {string}
    set tos {user}
    set tos-mask {user}
    set status [enable|disable]
    set comments {var-string}
    set internet-service-id <id1>, <id2>, ...
    set internet-service-custom <name1>, <name2>, ...
  next
end

```

## config router policy

Parameter	Description	Type	Size	Default
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	
input-device- negate	Enable/disable negation of input device match.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable negation of input device match.		
	<i>disable</i>	Disable negation of input device match.		
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
srcaddr <name>	Source address name. Address/group name.	string	Maximum length: 79	
src-negate	Enable/disable negating source address match.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable source address negation.		
	<i>disable</i>	Disable source address negation.		
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
dstaddr <name>	Destination address name. Address/group name.	string	Maximum length: 79	
dst-negate	Enable/disable negating destination address match.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable destination address negation.		
	<i>disable</i>	Disable destination address negation.		
action	Action of the policy route.	option	-	permit
	<b>Option</b>	<b>Description</b>		
	<i>deny</i>	Do not search policy route table.		
	<i>permit</i>	Use this policy route for forwarding.		

Parameter	Description	Type	Size	Default						
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255	0						
start-port	Start destination port number .	integer	Minimum value: 0 Maximum value: 65535	0						
end-port	End destination port number .	integer	Minimum value: 0 Maximum value: 65535	65535						
start-source-port	Start source port number .	integer	Minimum value: 0 Maximum value: 65535	0						
end-source-port	End source port number .	integer	Minimum value: 0 Maximum value: 65535	65535						
gateway	IP address of the gateway.	ipv4-address	Not Specified	0.0.0.0						
output-device	Outgoing interface name.	string	Maximum length: 35							
tos	Type of service bit pattern.	user	Not Specified							
tos-mask	Type of service evaluated bits.	user	Not Specified							
status	Enable/disable this policy route.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy route.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy route.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.		
Option	Description									
<i>enable</i>	Enable this policy route.									
<i>disable</i>	Disable this policy route.									
comments	Optional comments.	var-string	Maximum length: 255							
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295							

Parameter	Description	Type	Size	Default
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79	

## config router policy6

Configure IPv6 routing policies.

```
config router policy6
  Description: Configure IPv6 routing policies.
  edit <seq-num>
    set input-device <name1>, <name2>, ...
    set src {ipv6-network}
    set dst {ipv6-network}
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set gateway {ipv6-address}
    set output-device {string}
    set tos {user}
    set tos-mask {user}
    set status [enable|disable]
    set comments {var-string}
  next
end
```

## config router policy6

Parameter	Description	Type	Size	Default
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	
src	Source IPv6 prefix.	ipv6-network	Not Specified	::/0
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255	0



Parameter	Description	Type	Size	Default						
start-port	Start destination port number .	integer	Minimum value: 1 Maximum value: 65535	1						
end-port	End destination port number .	integer	Minimum value: 1 Maximum value: 65535	65535						
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
output-device	Outgoing interface name.	string	Maximum length: 35							
tos	Type of service bit pattern.	user	Not Specified							
tos-mask	Type of service evaluated bits.	user	Not Specified							
status	Enable/disable this policy route.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this policy route.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this policy route.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.			
Option	Description									
<i>enable</i>	Enable this policy route.									
<i>disable</i>	Disable this policy route.									
comments	Optional comments.	var-string	Maximum length: 255							

## config router static6

Configure IPv6 static routing tables.

```

config router static6
  Description: Configure IPv6 static routing tables.
  edit <seq-num>
    set status [enable|disable]
    set dst {ipv6-network}
    set gateway {ipv6-address}
    set device {string}
    set devindex {integer}
    set distance {integer}
    set priority {integer}
    set comment {var-string}
    set blackhole [enable|disable]
    set sdwan [enable|disable]
    set link-monitor-exempt [enable|disable]
  
```

```

    set bfd [enable|disable]
  next
end

```

## config router static6

Parameter	Description	Type	Size	Default						
status	Enable/disable this static route.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable static route.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable static route.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable static route.	<i>disable</i>	Disable static route.			
Option	Description									
<i>enable</i>	Enable static route.									
<i>disable</i>	Disable static route.									
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0						
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
device	Gateway out interface or tunnel.	string	Maximum length: 35							
devindex	Device index .	integer	Minimum value: 0 Maximum value: 4294967295	0						
distance	Administrative distance .	integer	Minimum value: 1 Maximum value: 255	10						
priority	Administrative priority .	integer	Minimum value: 1 Maximum value: 65535	1024						
comment	Optional comments.	var-string	Maximum length: 255							
blackhole	Enable/disable black hole.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable black hole.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable black hole.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.			
Option	Description									
<i>enable</i>	Enable black hole.									
<i>disable</i>	Disable black hole.									
sdwan	Enable/disable egress through the SD-WAN.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Keep this static route when link monitor or health check is down.</td> </tr> <tr> <td><i>disable</i></td> <td>Withdraw this static route when link monitor or health check is down. (default)</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Keep this static route when link monitor or health check is down.	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)			
Option	Description									
<i>enable</i>	Keep this static route when link monitor or health check is down.									
<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)									
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Bidirectional Forwarding Detection (BFD).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Bidirectional Forwarding Detection (BFD).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).									

## config router ospf

Configure OSPF.

```

config router ospf
  Description: Configure OSPF.
  set abr-type [cisco|ibm|...]
  set auto-cost-ref-bandwidth {integer}
  set distance-external {integer}
  set distance-inter-area {integer}
  set distance-intra-area {integer}
  set database-overflow [enable|disable]
  set database-overflow-max-lsas {integer}
  set database-overflow-time-to-recover {integer}
  set default-information-originate [enable|always|...]
  set default-information-metric {integer}
  set default-information-metric-type [1|2]
  set default-information-route-map {string}
  set default-metric {integer}
  set distance {integer}
  set rfc1583-compatible [enable|disable]
  set router-id {ipv4-address-any}
  set spf-timers {user}
  set bfd [enable|disable]
  set log-neighbour-changes [enable|disable]
  set distribute-list-in {string}
  set distribute-route-map-in {string}
  set restart-mode [none|lls|...]
  set restart-period {integer}

```

```

config area
  Description: OSPF area configuration.
  edit <id>
    set shortcut [disable|enable|...]
    set authentication [none|text|...]
    set default-cost {integer}
    set nssa-translator-role [candidate|never|...]
    set stub-type [no-summary|summary]
    set type [regular|nssa|...]
    set nssa-default-information-originate [enable|always|...]
    set nssa-default-information-originate-metric {integer}
    set nssa-default-information-originate-metric-type [1|2]
    set nssa-redistribution [enable|disable]
  config range
    Description: OSPF area range configuration.
    edit <id>
      set prefix {ipv4-classnet-any}
      set advertise [disable|enable]
      set substitute {ipv4-classnet-any}
      set substitute-status [enable|disable]
    next
  end
  config virtual-link
    Description: OSPF virtual link configuration.
    edit <name>
      set authentication [none|text|...]
      set authentication-key {password}
      set md5-keychain {string}
      set dead-interval {integer}
      set hello-interval {integer}
      set retransmit-interval {integer}
      set transmit-delay {integer}
      set peer {ipv4-address-any}
    config md5-keys
      Description: MD5 key.
      edit <id>
        set key-string {password}
      next
    end
  next
end
  config filter-list
    Description: OSPF area filter-list configuration.
    edit <id>
      set list {string}
      set direction [in|out]
    next
  end
end
  config ospf-interface
    Description: OSPF interface configuration.
    edit <name>
      set interface {string}
      set ip {ipv4-address}
      set authentication [none|text|...]
      set authentication-key {password}

```

```

    set md5-keychain {string}
    set prefix-length {integer}
    set retransmit-interval {integer}
    set transmit-delay {integer}
    set cost {integer}
    set priority {integer}
    set dead-interval {integer}
    set hello-interval {integer}
    set hello-multiplier {integer}
    set database-filter-out [enable|disable]
    set mtu {integer}
    set mtu-ignore [enable|disable]
    set network-type [broadcast|non-broadcast|...]
    set bfd [global|enable|...]
    set status [disable|enable]
    set resync-timeout {integer}
    config md5-keys
        Description: MD5 key.
        edit <id>
            set key-string {password}
        next
    end
next
end
config network
    Description: OSPF network configuration.
    edit <id>
        set prefix {ipv4-classnet}
        set area {ipv4-address-any}
    next
end
config neighbor
    Description: OSPF neighbor configuration are used when OSPF runs on non-broadcast
        media
    edit <id>
        set ip {ipv4-address}
        set poll-interval {integer}
        set cost {integer}
        set priority {integer}
    next
end
set passive-interface <name1>, <name2>, ...
config summary-address
    Description: IP address summary configuration.
    edit <id>
        set prefix {ipv4-classnet}
        set tag {integer}
        set advertise [disable|enable]
    next
end
config distribute-list
    Description: Distribute list configuration.
    edit <id>
        set access-list {string}
        set protocol [connected|static|...]
    next
end

```

```

config redistribute
  Description: Redistribute configuration.
  edit <name>
    set status [enable|disable]
    set metric {integer}
    set routemap {string}
    set metric-type [1|2]
    set tag {integer}
  next
end
end

```

## config router ospf

Parameter	Description	Type	Size	Default										
abr-type	Area border router type.	option	-	standard										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>cisco</i></td> <td>Cisco.</td> </tr> <tr> <td><i>ibm</i></td> <td>IBM.</td> </tr> <tr> <td><i>shortcut</i></td> <td>Shortcut.</td> </tr> <tr> <td><i>standard</i></td> <td>Standard.</td> </tr> </tbody> </table>	Option	Description	<i>cisco</i>	Cisco.	<i>ibm</i>	IBM.	<i>shortcut</i>	Shortcut.	<i>standard</i>	Standard.			
Option	Description													
<i>cisco</i>	Cisco.													
<i>ibm</i>	IBM.													
<i>shortcut</i>	Shortcut.													
<i>standard</i>	Standard.													
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000										
distance-external	Administrative external distance.	integer	Minimum value: 1 Maximum value: 255	110										
distance-inter-area	Administrative inter-area distance.	integer	Minimum value: 1 Maximum value: 255	110										
distance-intra-area	Administrative intra-area distance.	integer	Minimum value: 1 Maximum value: 255	110										
database-overflow	Enable/disable database overflow.	option	-	disable										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
database-overflow-max-lsas	Database overflow maximum LSAs.	integer	Minimum value: 0 Maximum value: 4294967295	10000								
database-overflow-time-to-recover	Database overflow time to recover (sec).	integer	Minimum value: 0 Maximum value: 65535	300								
default-information-originate	Enable/disable generation of default route.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>always</i></td> <td>Always advertise the default router.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>always</i>	Always advertise the default router.	<i>disable</i>	Disable setting.			
Option	Description											
<i>enable</i>	Enable setting.											
<i>always</i>	Always advertise the default router.											
<i>disable</i>	Disable setting.											
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10								
default-information-metric-type	Default information metric type.	option	-	2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>Type 1.</td> </tr> <tr> <td><i>2</i></td> <td>Type 2.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	Type 1.	<i>2</i>	Type 2.					
Option	Description											
<i>1</i>	Type 1.											
<i>2</i>	Type 2.											
default-information-route-map	Default information route map.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10						
distance	Distance of the route.	integer	Minimum value: 1 Maximum value: 255	110						
rfc1583-compatible	Enable/disable RFC1583 compatibility.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
router-id	Router ID.	ipv4-address-any	Not Specified	0.0.0.0						
spf-timers	SPF calculation frequency.	user	Not Specified							
bfd	Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
log-neighbour-changes	Enable logging of OSPF neighbour's changes	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
distribute-list-in	Filter incoming routes.	string	Maximum length: 35							
distribute-route-map-in	Filter incoming external routes by route-map.	string	Maximum length: 35							
restart-mode	OSPF restart mode (graceful or LLS).	option	-	none						



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Hitless restart disabled.</td> </tr> <tr> <td><i>lls</i></td> <td>LLS mode.</td> </tr> <tr> <td><i>graceful-restart</i></td> <td>Graceful Restart Mode.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Hitless restart disabled.	<i>lls</i>	LLS mode.	<i>graceful-restart</i>	Graceful Restart Mode.			
Option	Description											
<i>none</i>	Hitless restart disabled.											
<i>lls</i>	LLS mode.											
<i>graceful-restart</i>	Graceful Restart Mode.											
restart-period	Graceful restart period.	integer	Minimum value: 1 Maximum value: 3600	120								
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79									

### config area

Parameter	Description	Type	Size	Default								
shortcut	Enable/disable shortcut option.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable shortcut option.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable shortcut option.</td> </tr> <tr> <td><i>default</i></td> <td>Default shortcut option.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable shortcut option.	<i>enable</i>	Enable shortcut option.	<i>default</i>	Default shortcut option.			
Option	Description											
<i>disable</i>	Disable shortcut option.											
<i>enable</i>	Enable shortcut option.											
<i>default</i>	Default shortcut option.											
authentication	Authentication type.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>text</i></td> <td>Text.</td> </tr> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>md5</i>	MD5.			
Option	Description											
<i>none</i>	None.											
<i>text</i>	Text.											
<i>md5</i>	MD5.											
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 4294967295	10								
nssa-translator-role	NSSA translator role type.	option	-	candidate								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>candidate</i></td> <td>Candidate.</td> </tr> <tr> <td><i>never</i></td> <td>Never.</td> </tr> <tr> <td><i>always</i></td> <td>Always.</td> </tr> </tbody> </table>	Option	Description	<i>candidate</i>	Candidate.	<i>never</i>	Never.	<i>always</i>	Always.			
Option	Description											
<i>candidate</i>	Candidate.											
<i>never</i>	Never.											
<i>always</i>	Always.											
stub-type	Stub summary setting.	option	-	summary								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-summary</i></td> <td>No summary.</td> </tr> <tr> <td><i>summary</i></td> <td>Summary.</td> </tr> </tbody> </table>	Option	Description	<i>no-summary</i>	No summary.	<i>summary</i>	Summary.					
Option	Description											
<i>no-summary</i>	No summary.											
<i>summary</i>	Summary.											
type	Area type setting.	option	-	regular								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>Regular.</td> </tr> <tr> <td><i>nssa</i></td> <td>NSSA.</td> </tr> <tr> <td><i>stub</i></td> <td>Stub.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	Regular.	<i>nssa</i>	NSSA.	<i>stub</i>	Stub.			
Option	Description											
<i>regular</i>	Regular.											
<i>nssa</i>	NSSA.											
<i>stub</i>	Stub.											
nssa-default-information-originate	Redistribute, advertise, or do not originate Type-7 default route into NSSA area.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Redistribute Type-7 default route from routing table.</td> </tr> <tr> <td><i>always</i></td> <td>Advertise a self-originated Type-7 default route.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not advertise Type-7 default route.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Redistribute Type-7 default route from routing table.	<i>always</i>	Advertise a self-originated Type-7 default route.	<i>disable</i>	Do not advertise Type-7 default route.			
Option	Description											
<i>enable</i>	Redistribute Type-7 default route from routing table.											
<i>always</i>	Advertise a self-originated Type-7 default route.											
<i>disable</i>	Do not advertise Type-7 default route.											
nssa-default-information-originate-metric	OSPF default metric.	integer	Minimum value: 0 Maximum value: 16777214	10								
nssa-default-information-originate-metric-type	OSPF metric type for default routes.	option	-	2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Type 1.</td> </tr> <tr> <td>2</td> <td>Type 2.</td> </tr> </tbody> </table>	Option	Description	1	Type 1.	2	Type 2.					
Option	Description											
1	Type 1.											
2	Type 2.											

Parameter	Description	Type	Size	Default
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable redistribute into NSSA area.		
	<i>disable</i>	Disable redistribute into NSSA area.		

### config range

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
advertise	Enable/disable advertise status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertise status.		
	<i>enable</i>	Enable advertise status.		
substitute	Substitute prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
substitute-status	Enable/disable substitute status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable substitute status.		
	<i>disable</i>	Disable substitute status.		

### config virtual-link

Parameter	Description	Type	Size	Default
authentication	Authentication type.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>text</i>	Text.		
	<i>md5</i>	MD5.		

Parameter	Description	Type	Size	Default
authentication-key	Authentication key.	password	Not Specified	
md5-keychain	Authentication MD5 key-chain name.	string	Maximum length: 35	
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1
peer	Peer IP.	ipv4-address-any	Not Specified	0.0.0.0

### config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

### config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

## config filter-list

Parameter	Description	Type	Size	Default						
list	Access-list or prefix-list name.	string	Maximum length: 35							
direction	Direction.	option	-	out						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>in</i></td><td>In.</td></tr><tr><td><i>out</i></td><td>Out.</td></tr></tbody></table>	Option	Description	<i>in</i>	In.	<i>out</i>	Out.			
Option	Description									
<i>in</i>	In.									
<i>out</i>	Out.									

## config ospf-interface

Parameter	Description	Type	Size	Default								
interface	Configuration interface name.	string	Maximum length: 15									
ip	IP address.	ipv4-address	Not Specified	0.0.0.0								
authentication	Authentication type.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>md5</i></td><td>MD5.</td></tr></tbody></table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>md5</i>	MD5.			
Option	Description											
<i>none</i>	None.											
<i>text</i>	Text.											
<i>md5</i>	MD5.											
authentication-key	Authentication key.	password	Not Specified									
md5-keychain	Authentication MD5 key-chain name.	string	Maximum length: 35									
prefix-length	Prefix length.	integer	Minimum value: 0 Maximum value: 32	0								
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5								

Parameter	Description	Type	Size	Default						
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1						
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0						
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1						
dead-interval	Dead interval.	integer	Minimum value: 0 Maximum value: 65535	0						
hello-interval	Hello interval.	integer	Minimum value: 0 Maximum value: 65535	0						
hello-multiplier	Number of hello packets within dead interval.	integer	Minimum value: 3 Maximum value: 10	0						
database-filter-out	Enable/disable control of flooding out LSAs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
mtu	MTU for database description packets.	integer	Minimum value: 576 Maximum value: 65535	0						
mtu-ignore	Enable/disable ignore MTU.	option	-	disable						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
network-type	Network type.	option	-	broadcast												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>broadcast</i></td> <td>Broadcast.</td> </tr> <tr> <td><i>non-broadcast</i></td> <td>Non-broadcast.</td> </tr> <tr> <td><i>point-to-point</i></td> <td>Point-to-point.</td> </tr> <tr> <td><i>point-to-multipoint</i></td> <td>Point-to-multipoint.</td> </tr> <tr> <td><i>point-to-multipoint-non-broadcast</i></td> <td>Point-to-multipoint and non-broadcast.</td> </tr> </tbody> </table>	Option	Description	<i>broadcast</i>	Broadcast.	<i>non-broadcast</i>	Non-broadcast.	<i>point-to-point</i>	Point-to-point.	<i>point-to-multipoint</i>	Point-to-multipoint.	<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.			
Option	Description															
<i>broadcast</i>	Broadcast.															
<i>non-broadcast</i>	Non-broadcast.															
<i>point-to-point</i>	Point-to-point.															
<i>point-to-multipoint</i>	Point-to-multipoint.															
<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.															
bfd	Bidirectional Forwarding Detection (BFD).	option	-	global												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Follow global configuration.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable BFD on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable BFD on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Follow global configuration.	<i>enable</i>	Enable BFD on this interface.	<i>disable</i>	Disable BFD on this interface.							
Option	Description															
<i>global</i>	Follow global configuration.															
<i>enable</i>	Enable BFD on this interface.															
<i>disable</i>	Disable BFD on this interface.															
status	Enable/disable status.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.									
Option	Description															
<i>disable</i>	Disable status.															
<i>enable</i>	Enable status.															
resync-timeout	Graceful restart neighbor resynchronization timeout.	integer	Minimum value: 1 Maximum value: 3600	40												

### config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

### config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

### config network

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
area	Attach the network to area.	ipv4-address-any	Not Specified	0.0.0.0

### config neighbor

Parameter	Description	Type	Size	Default
ip	Interface IP address of the neighbor.	ipv4-address	Not Specified	0.0.0.0
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

### config summary-address

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0



Parameter	Description	Type	Size	Default
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0
advertise	Enable/disable advertise status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertise status.		
	<i>enable</i>	Enable advertise status.		

### config distribute-list

Parameter	Description	Type	Size	Default
access-list	Access list name.	string	Maximum length: 35	
protocol	Protocol type.	option	-	connected
	<b>Option</b>	<b>Description</b>		
	<i>connected</i>	Connected type.		
	<i>static</i>	Static type.		
	<i>rip</i>	RIP type.		

### config redistribute

Parameter	Description	Type	Size	Default
status	status	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0
routemap	Route map name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
metric-type	Metric type.	option	-	2						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Type 1.</td> </tr> <tr> <td>2</td> <td>Type 2.</td> </tr> </tbody> </table>	Option	Description	1	Type 1.	2	Type 2.			
Option	Description									
1	Type 1.									
2	Type 2.									
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config router ospf6

Configure IPv6 OSPF.

```

config router ospf6
  Description: Configure IPv6 OSPF.
  set abr-type [cisco|ibm|...]
  set auto-cost-ref-bandwidth {integer}
  set default-information-originate [enable|always|...]
  set log-neighbour-changes [enable|disable]
  set default-information-metric {integer}
  set default-information-metric-type [1|2]
  set default-information-route-map {string}
  set default-metric {integer}
  set router-id {ipv4-address-any}
  set spf-timers {user}
  set bfd [enable|disable]
config area
  Description: OSPF6 area configuration.
  edit <id>
    set default-cost {integer}
    set nssa-translator-role [candidate|never|...]
    set stub-type [no-summary|summary]
    set type [regular|nssa|...]
    set nssa-default-information-originate [enable|disable]
    set nssa-default-information-originate-metric {integer}
    set nssa-default-information-originate-metric-type [1|2]
    set nssa-redistribution [enable|disable]
    set authentication [none|ah|...]
    set key-rollover-interval {integer}
    set ipsec-auth-alg [md5|sha1|...]
    set ipsec-enc-alg [null|des|...]
    config ipsec-keys
      Description: IPsec authentication and encryption keys.
      edit <spi>
        set auth-key {password}
        set enc-key {password}
      next
    end
  end

```

```

config range
  Description: OSPF6 area range configuration.
  edit <id>
    set prefix6 {ipv6-network}
    set advertise [disable|enable]
  next
end
config virtual-link
  Description: OSPF6 virtual link configuration.
  edit <name>
    set dead-interval {integer}
    set hello-interval {integer}
    set retransmit-interval {integer}
    set transmit-delay {integer}
    set peer {ipv4-address-any}
    set authentication [none|ah|...]
    set key-rollover-interval {integer}
    set ipsec-auth-alg [md5|sha1|...]
    set ipsec-enc-alg [null|des|...]
    config ipsec-keys
      Description: IPsec authentication and encryption keys.
      edit <spi>
        set auth-key {password}
        set enc-key {password}
      next
    end
  next
end
next
end
config ospf6-interface
  Description: OSPF6 interface configuration.
  edit <name>
    set area-id {ipv4-address-any}
    set interface {string}
    set retransmit-interval {integer}
    set transmit-delay {integer}
    set cost {integer}
    set priority {integer}
    set dead-interval {integer}
    set hello-interval {integer}
    set status [disable|enable]
    set network-type [broadcast|point-to-point|...]
    set bfd [global|enable|...]
    set mtu {integer}
    set mtu-ignore [enable|disable]
    set authentication [none|ah|...]
    set key-rollover-interval {integer}
    set ipsec-auth-alg [md5|sha1|...]
    set ipsec-enc-alg [null|des|...]
    config ipsec-keys
      Description: IPsec authentication and encryption keys.
      edit <spi>
        set auth-key {password}
        set enc-key {password}
      next
    end
  end
end

```

```

config neighbor
  Description: OSPFv3 neighbors are used when OSPFv3 runs on non-broadcast media
  edit <ip6>
    set poll-interval {integer}
    set cost {integer}
    set priority {integer}
  next
end
next
end
config redistribute
  Description: Redistribute configuration.
  edit <name>
    set status [enable|disable]
    set metric {integer}
    set routemap {string}
    set metric-type [1|2]
  next
end
set passive-interface <name1>, <name2>, ...
config summary-address
  Description: IPv6 address summary configuration.
  edit <id>
    set prefix6 {ipv6-network}
    set advertise [disable|enable]
    set tag {integer}
  next
end
end
end

```

## config router ospf6

Parameter	Description	Type	Size	Default								
abr-type	Area border router type.	option	-	standard								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>cisco</i></td> <td>Cisco.</td> </tr> <tr> <td><i>ibm</i></td> <td>IBM.</td> </tr> <tr> <td><i>standard</i></td> <td>Standard.</td> </tr> </tbody> </table>	Option	Description	<i>cisco</i>	Cisco.	<i>ibm</i>	IBM.	<i>standard</i>	Standard.			
Option	Description											
<i>cisco</i>	Cisco.											
<i>ibm</i>	IBM.											
<i>standard</i>	Standard.											
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000								
default-information-originate	Enable/disable generation of default route.	option	-	disable								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>always</i></td> <td>Always advertise the default router.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>always</i>	Always advertise the default router.	<i>disable</i>	Disable setting.			
Option	Description											
<i>enable</i>	Enable setting.											
<i>always</i>	Always advertise the default router.											
<i>disable</i>	Disable setting.											
log-neighbour-changes	Enable logging of OSPFv3 neighbour's changes	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10								
default-information-metric-type	Default information metric type.	option	-	2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Type 1.</td> </tr> <tr> <td>2</td> <td>Type 2.</td> </tr> </tbody> </table>	Option	Description	1	Type 1.	2	Type 2.					
Option	Description											
1	Type 1.											
2	Type 2.											
default-information-route-map	Default information route map.	string	Maximum length: 35									
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10								
router-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0								
spf-timers	SPF calculation frequency.	user	Not Specified									

Parameter	Description	Type	Size	Default						
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Bidirectional Forwarding Detection (BFD).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Bidirectional Forwarding Detection (BFD).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).									
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							

## config area

Parameter	Description	Type	Size	Default								
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 16777215	10								
nssa-translator-role	NSSA translator role type.	option	-	candidate								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>candidate</i></td> <td>Candidate.</td> </tr> <tr> <td><i>never</i></td> <td>Never.</td> </tr> <tr> <td><i>always</i></td> <td>Always.</td> </tr> </tbody> </table>	Option	Description	<i>candidate</i>	Candidate.	<i>never</i>	Never.	<i>always</i>	Always.			
Option	Description											
<i>candidate</i>	Candidate.											
<i>never</i>	Never.											
<i>always</i>	Always.											
stub-type	Stub summary setting.	option	-	summary								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-summary</i></td> <td>No summary.</td> </tr> <tr> <td><i>summary</i></td> <td>Summary.</td> </tr> </tbody> </table>	Option	Description	<i>no-summary</i>	No summary.	<i>summary</i>	Summary.					
Option	Description											
<i>no-summary</i>	No summary.											
<i>summary</i>	Summary.											
type	Area type setting.	option	-	regular								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>Regular.</td> </tr> <tr> <td><i>nssa</i></td> <td>NSSA.</td> </tr> <tr> <td><i>stub</i></td> <td>Stub.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	Regular.	<i>nssa</i>	NSSA.	<i>stub</i>	Stub.			
Option	Description											
<i>regular</i>	Regular.											
<i>nssa</i>	NSSA.											
<i>stub</i>	Stub.											

Parameter	Description	Type	Size	Default								
nssa-default-information-originate	Enable/disable originate type 7 default into NSSA area.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable originate type 7 default into NSSA area.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable originate type 7 default into NSSA area.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable originate type 7 default into NSSA area.	<i>disable</i>	Disable originate type 7 default into NSSA area.					
Option	Description											
<i>enable</i>	Enable originate type 7 default into NSSA area.											
<i>disable</i>	Disable originate type 7 default into NSSA area.											
nssa-default-information-originate-metric	OSPFv3 default metric.	integer	Minimum value: 0 Maximum value: 16777214	10								
nssa-default-information-originate-metric-type	OSPFv3 metric type for default routes.	option	-	2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Type 1.</td> </tr> <tr> <td>2</td> <td>Type 2.</td> </tr> </tbody> </table>	Option	Description	1	Type 1.	2	Type 2.					
Option	Description											
1	Type 1.											
2	Type 2.											
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redistribute into NSSA area.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redistribute into NSSA area.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redistribute into NSSA area.	<i>disable</i>	Disable redistribute into NSSA area.					
Option	Description											
<i>enable</i>	Enable redistribute into NSSA area.											
<i>disable</i>	Disable redistribute into NSSA area.											
authentication	Authentication mode.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Disable authentication.</td> </tr> <tr> <td><i>ah</i></td> <td>Authentication Header.</td> </tr> <tr> <td><i>esp</i></td> <td>Encapsulating Security Payload.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Disable authentication.	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.			
Option	Description											
<i>none</i>	Disable authentication.											
<i>ah</i>	Authentication Header.											
<i>esp</i>	Encapsulating Security Payload.											
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300								

Parameter	Description	Type	Size	Default														
ipsec-auth-alg	Authentication algorithm.	option	-	md5														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> <tr> <td><i>sha1</i></td> <td>SHA1.</td> </tr> <tr> <td><i>sha256</i></td> <td>SHA256.</td> </tr> <tr> <td><i>sha384</i></td> <td>SHA384.</td> </tr> <tr> <td><i>sha512</i></td> <td>SHA512.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.					
Option	Description																	
<i>md5</i>	MD5.																	
<i>sha1</i>	SHA1.																	
<i>sha256</i>	SHA256.																	
<i>sha384</i>	SHA384.																	
<i>sha512</i>	SHA512.																	
ipsec-enc-alg	Encryption algorithm.	option	-	null														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null</i></td> <td>No encryption.</td> </tr> <tr> <td><i>des</i></td> <td>DES.</td> </tr> <tr> <td><i>3des</i></td> <td>3DES.</td> </tr> <tr> <td><i>aes128</i></td> <td>AES128.</td> </tr> <tr> <td><i>aes192</i></td> <td>AES192.</td> </tr> <tr> <td><i>aes256</i></td> <td>AES256.</td> </tr> </tbody> </table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.			
Option	Description																	
<i>null</i>	No encryption.																	
<i>des</i>	DES.																	
<i>3des</i>	3DES.																	
<i>aes128</i>	AES128.																	
<i>aes192</i>	AES192.																	
<i>aes256</i>	AES256.																	

### config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

### config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	



## config range

Parameter	Description	Type	Size	Default						
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0						
advertise	Enable/disable advertise status.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>disable</td></tr><tr><td><i>enable</i></td><td>enable</td></tr></tbody></table>	Option	Description	<i>disable</i>	disable	<i>enable</i>	enable			
Option	Description									
<i>disable</i>	disable									
<i>enable</i>	enable									

## config virtual-link

Parameter	Description	Type	Size	Default				
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40				
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10				
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5				
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1				
peer	A.B.C.D, peer router ID.	ipv4-address-any	Not Specified	0.0.0.0				
authentication	Authentication mode.	option	-	area				
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>Disable authentication.</td></tr></tbody></table>	Option	Description	<i>none</i>	Disable authentication.			
Option	Description							
<i>none</i>	Disable authentication.							

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ah</i></td> <td>Authentication Header.</td> </tr> <tr> <td><i>esp</i></td> <td>Encapsulating Security Payload.</td> </tr> <tr> <td><i>area</i></td> <td>Use the routing area's authentication configuration.</td> </tr> </tbody> </table>	Option	Description	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.	<i>area</i>	Use the routing area's authentication configuration.									
Option	Description																	
<i>ah</i>	Authentication Header.																	
<i>esp</i>	Encapsulating Security Payload.																	
<i>area</i>	Use the routing area's authentication configuration.																	
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300														
ipsec-auth-alg	Authentication algorithm.	option	-	md5														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> <tr> <td><i>sha1</i></td> <td>SHA1.</td> </tr> <tr> <td><i>sha256</i></td> <td>SHA256.</td> </tr> <tr> <td><i>sha384</i></td> <td>SHA384.</td> </tr> <tr> <td><i>sha512</i></td> <td>SHA512.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.					
Option	Description																	
<i>md5</i>	MD5.																	
<i>sha1</i>	SHA1.																	
<i>sha256</i>	SHA256.																	
<i>sha384</i>	SHA384.																	
<i>sha512</i>	SHA512.																	
ipsec-enc-alg	Encryption algorithm.	option	-	null														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null</i></td> <td>No encryption.</td> </tr> <tr> <td><i>des</i></td> <td>DES.</td> </tr> <tr> <td><i>3des</i></td> <td>3DES.</td> </tr> <tr> <td><i>aes128</i></td> <td>AES128.</td> </tr> <tr> <td><i>aes192</i></td> <td>AES192.</td> </tr> <tr> <td><i>aes256</i></td> <td>AES256.</td> </tr> </tbody> </table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.			
Option	Description																	
<i>null</i>	No encryption.																	
<i>des</i>	DES.																	
<i>3des</i>	3DES.																	
<i>aes128</i>	AES128.																	
<i>aes192</i>	AES192.																	
<i>aes256</i>	AES256.																	

### config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

## config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

## config ospf6-interface

Parameter	Description	Type	Size	Default
area-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0
interface	Configuration interface name.	string	Maximum length: 15	
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	priority	integer	Minimum value: 0 Maximum value: 255	1
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	0

Parameter	Description	Type	Size	Default												
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	0												
status	Enable/disable OSPF6 routing on this interface.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable OSPF6 routing.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable OSPF6 routing.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable OSPF6 routing.	<i>enable</i>	Enable OSPF6 routing.									
Option	Description															
<i>disable</i>	Disable OSPF6 routing.															
<i>enable</i>	Enable OSPF6 routing.															
network-type	Network type.	option	-	broadcast												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>broadcast</i></td> <td>broadcast</td> </tr> <tr> <td><i>point-to-point</i></td> <td>point-to-point</td> </tr> <tr> <td><i>non-broadcast</i></td> <td>non-broadcast</td> </tr> <tr> <td><i>point-to-multipoint</i></td> <td>point-to-multipoint</td> </tr> <tr> <td><i>point-to-multipoint-non-broadcast</i></td> <td>point-to-multipoint and non-broadcast.</td> </tr> </tbody> </table>	Option	Description	<i>broadcast</i>	broadcast	<i>point-to-point</i>	point-to-point	<i>non-broadcast</i>	non-broadcast	<i>point-to-multipoint</i>	point-to-multipoint	<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.			
Option	Description															
<i>broadcast</i>	broadcast															
<i>point-to-point</i>	point-to-point															
<i>non-broadcast</i>	non-broadcast															
<i>point-to-multipoint</i>	point-to-multipoint															
<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.															
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	global												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Use global configuration of Bidirectional Forwarding Detection (BFD).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Bidirectional Forwarding Detection (BFD) on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Bidirectional Forwarding Detection (BFD) on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.							
Option	Description															
<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).															
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.															
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.															
mtu	MTU for OSPFv3 packets.	integer	Minimum value: 576 Maximum value: 65535	0												
mtu-ignore	Enable/disable ignoring MTU field in DBD packets.	option	-	disable												

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Ignore MTU field in DBD packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not ignore MTU field in DBD packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Ignore MTU field in DBD packets.	<i>disable</i>	Do not ignore MTU field in DBD packets.											
Option	Description																	
<i>enable</i>	Ignore MTU field in DBD packets.																	
<i>disable</i>	Do not ignore MTU field in DBD packets.																	
authentication	Authentication mode.	option	-	area														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Disable authentication.</td> </tr> <tr> <td><i>ah</i></td> <td>Authentication Header.</td> </tr> <tr> <td><i>esp</i></td> <td>Encapsulating Security Payload.</td> </tr> <tr> <td><i>area</i></td> <td>Use the routing area's authentication configuration.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Disable authentication.	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.	<i>area</i>	Use the routing area's authentication configuration.							
Option	Description																	
<i>none</i>	Disable authentication.																	
<i>ah</i>	Authentication Header.																	
<i>esp</i>	Encapsulating Security Payload.																	
<i>area</i>	Use the routing area's authentication configuration.																	
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300														
ipsec-auth-alg	Authentication algorithm.	option	-	md5														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> <tr> <td><i>sha1</i></td> <td>SHA1.</td> </tr> <tr> <td><i>sha256</i></td> <td>SHA256.</td> </tr> <tr> <td><i>sha384</i></td> <td>SHA384.</td> </tr> <tr> <td><i>sha512</i></td> <td>SHA512.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.					
Option	Description																	
<i>md5</i>	MD5.																	
<i>sha1</i>	SHA1.																	
<i>sha256</i>	SHA256.																	
<i>sha384</i>	SHA384.																	
<i>sha512</i>	SHA512.																	
ipsec-enc-alg	Encryption algorithm.	option	-	null														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null</i></td> <td>No encryption.</td> </tr> <tr> <td><i>des</i></td> <td>DES.</td> </tr> <tr> <td><i>3des</i></td> <td>3DES.</td> </tr> <tr> <td><i>aes128</i></td> <td>AES128.</td> </tr> <tr> <td><i>aes192</i></td> <td>AES192.</td> </tr> <tr> <td><i>aes256</i></td> <td>AES256.</td> </tr> </tbody> </table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.			
Option	Description																	
<i>null</i>	No encryption.																	
<i>des</i>	DES.																	
<i>3des</i>	3DES.																	
<i>aes128</i>	AES128.																	
<i>aes192</i>	AES192.																	
<i>aes256</i>	AES256.																	

### config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

### config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

### config neighbor

Parameter	Description	Type	Size	Default
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	priority	integer	Minimum value: 0 Maximum value: 255	1

### config redistribute

Parameter	Description	Type	Size	Default						
status	status	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0						
routemap	Route map name.	string	Maximum length: 35							
metric-type	Metric type.	option	-	2						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Type 1.</td> </tr> <tr> <td>2</td> <td>Type 2.</td> </tr> </tbody> </table>	Option	Description	1	Type 1.	2	Type 2.			
Option	Description									
1	Type 1.									
2	Type 2.									

### config summary-address

Parameter	Description	Type	Size	Default						
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0						
advertise	Enable/disable advertise status.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>disable</td> </tr> <tr> <td><i>enable</i></td> <td>enable</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	disable	<i>enable</i>	enable			
Option	Description									
<i>disable</i>	disable									
<i>enable</i>	enable									
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0						

### config router bgp

Configure BGP.

```

config router bgp
  Description: Configure BGP.
  set as {integer}
  set router-id {ipv4-address-any}
  set keepalive-timer {integer}
  set holdtime-timer {integer}
  set always-compare-med [enable|disable]
  set bestpath-as-path-ignore [enable|disable]
  set bestpath-cmp-confed-aspath [enable|disable]
  set bestpath-cmp-routerid [enable|disable]

```

```

set bestpath-med-confed [enable|disable]
set bestpath-med-missing-as-worst [enable|disable]
set client-to-client-reflection [enable|disable]
set dampening [enable|disable]
set deterministic-med [enable|disable]
set ebgp-multipath [enable|disable]
set ibgp-multipath [enable|disable]
set enforce-first-as [enable|disable]
set fast-external-failover [enable|disable]
set log-neighbour-changes [enable|disable]
set network-import-check [enable|disable]
set ignore-optional-capability [enable|disable]
set additional-path [enable|disable]
set additional-path6 [enable|disable]
set multipath-recursive-distance [enable|disable]
set cluster-id {ipv4-address-any}
set confederation-identifier {integer}
set confederation-peers <peer1>, <peer2>, ...
set dampening-route-map {string}
set dampening-reachability-half-life {integer}
set dampening-reuse {integer}
set dampening-suppress {integer}
set dampening-max-suppress-time {integer}
set dampening-unreachability-half-life {integer}
set default-local-preference {integer}
set scan-time {integer}
set distance-external {integer}
set distance-internal {integer}
set distance-local {integer}
set synchronization [enable|disable]
set graceful-restart [enable|disable]
set graceful-restart-time {integer}
set graceful-stalepath-time {integer}
set graceful-update-delay {integer}
set graceful-end-on-timer [enable|disable]
set additional-path-select {integer}
set additional-path-select6 {integer}
config aggregate-address
    Description: BGP aggregate address table.
    edit <id>
        set prefix {ipv4-classnet-any}
        set as-set [enable|disable]
        set summary-only [enable|disable]
    next
end
config aggregate-address6
    Description: BGP IPv6 aggregate address table.
    edit <id>
        set prefix6 {ipv6-prefix}
        set as-set [enable|disable]
        set summary-only [enable|disable]
    next
end
config neighbor
    Description: BGP neighbor table.
    edit <ip>
        set advertisement-interval {integer}

```



---

```
set allowas-in-enable [enable|disable]
set allowas-in-enable6 [enable|disable]
set allowas-in {integer}
set allowas-in6 {integer}
set attribute-unchanged {option1}, {option2}, ...
set attribute-unchanged6 {option1}, {option2}, ...
set activate [enable|disable]
set activate6 [enable|disable]
set bfd [enable|disable]
set capability-dynamic [enable|disable]
set capability-orf [none|receive|...]
set capability-orf6 [none|receive|...]
set capability-graceful-restart [enable|disable]
set capability-graceful-restart6 [enable|disable]
set capability-route-refresh [enable|disable]
set capability-default-originate [enable|disable]
set capability-default-originate6 [enable|disable]
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set link-down-failover [enable|disable]
set stale-route [enable|disable]
set next-hop-self [enable|disable]
set next-hop-self6 [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set remove-private-as [enable|disable]
set remove-private-as6 [enable|disable]
set route-reflector-client [enable|disable]
set route-reflector-client6 [enable|disable]
set route-server-client [enable|disable]
set route-server-client6 [enable|disable]
set shutdown [enable|disable]
set soft-reconfiguration [enable|disable]
set soft-reconfiguration6 [enable|disable]
set as-override [enable|disable]
set as-override6 [enable|disable]
set strict-capability-match [enable|disable]
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set interface {string}
set maximum-prefix {integer}
set maximum-prefix6 {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-warning-only [enable|disable]
```

```

set maximum-prefix-warning-only6 [enable|disable]
set prefix-list-in {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out6 {string}
set remote-as {integer}
set local-as {integer}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in6 {string}
set route-map-out {string}
set route-map-out-preferable {string}
set route-map-out6 {string}
set route-map-out6-preferable {string}
set send-community [standard|extended|...]
set send-community6 [standard|extended|...]
set keep-alive-timer {integer}
set holdtime-timer {integer}
set connect-timer {integer}
set unsuppress-map {string}
set unsuppress-map6 {string}
set update-source {string}
set weight {integer}
set restart-time {integer}
set additional-path [send|receive|...]
set additional-path6 [send|receive|...]
set adv-additional-path {integer}
set adv-additional-path6 {integer}
set password {password}
config conditional-advertise
    Description: Conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap {string}
        set condition-type [exist|non-exist]
    next
end
next
end
config neighbor-group
    Description: BGP neighbor group table.
    edit <name>
        set advertisement-interval {integer}
        set allowas-in-enable [enable|disable]
        set allowas-in-enable6 [enable|disable]
        set allowas-in {integer}
        set allowas-in6 {integer}
        set attribute-unchanged {option1}, {option2}, ...
        set attribute-unchanged6 {option1}, {option2}, ...
        set activate [enable|disable]
        set activate6 [enable|disable]
        set bfd [enable|disable]
        set capability-dynamic [enable|disable]
        set capability-orf [none|receive|...]
        set capability-orf6 [none|receive|...]
        set capability-graceful-restart [enable|disable]

```

---

```
set capability-graceful-restart6 [enable|disable]
set capability-route-refresh [enable|disable]
set capability-default-originate [enable|disable]
set capability-default-originate6 [enable|disable]
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set link-down-failover [enable|disable]
set stale-route [enable|disable]
set next-hop-self [enable|disable]
set next-hop-self6 [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set remove-private-as [enable|disable]
set remove-private-as6 [enable|disable]
set route-reflector-client [enable|disable]
set route-reflector-client6 [enable|disable]
set route-server-client [enable|disable]
set route-server-client6 [enable|disable]
set shutdown [enable|disable]
set soft-reconfiguration [enable|disable]
set soft-reconfiguration6 [enable|disable]
set as-override [enable|disable]
set as-override6 [enable|disable]
set strict-capability-match [enable|disable]
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set interface {string}
set maximum-prefix {integer}
set maximum-prefix6 {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set prefix-list-in {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out6 {string}
set remote-as {integer}
set local-as {integer}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in6 {string}
set route-map-out {string}
```

```

    set route-map-out-preferable {string}
    set route-map-out6 {string}
    set route-map-out6-preferable {string}
    set send-community [standard|extended|...]
    set send-community6 [standard|extended|...]
    set keep-alive-timer {integer}
    set holdtime-timer {integer}
    set connect-timer {integer}
    set unsuppress-map {string}
    set unsuppress-map6 {string}
    set update-source {string}
    set weight {integer}
    set restart-time {integer}
    set additional-path [send|receive|...]
    set additional-path6 [send|receive|...]
    set adv-additional-path {integer}
    set adv-additional-path6 {integer}
  next
end
config neighbor-range
  Description: BGP neighbor range table.
  edit <id>
    set prefix {ipv4-classnet}
    set max-neighbor-num {integer}
    set neighbor-group {string}
  next
end
config neighbor-range6
  Description: BGP IPv6 neighbor range table.
  edit <id>
    set prefix6 {ipv6-network}
    set max-neighbor-num {integer}
    set neighbor-group {string}
  next
end
config network
  Description: BGP network table.
  edit <id>
    set prefix {ipv4-classnet}
    set backdoor [enable|disable]
    set route-map {string}
  next
end
config network6
  Description: BGP IPv6 network table.
  edit <id>
    set prefix6 {ipv6-network}
    set backdoor [enable|disable]
    set route-map {string}
  next
end
config redistribute
  Description: BGP IPv4 redistribute table.
  edit <name>
    set status [enable|disable]
    set route-map {string}
  next

```

```

end
config redistribute6
  Description: BGP IPv6 redistribute table.
  edit <name>
    set status [enable|disable]
    set route-map {string}
  next
end
config admin-distance
  Description: Administrative distance modifications.
  edit <id>
    set neighbour-prefix {ipv4-classnet}
    set route-list {string}
    set distance {integer}
  next
end
config vrf-leak
  Description: BGP VRF leaking table.
  edit <vrf>
    config target
      Description: Target VRF table.
      edit <vrf>
        set route-map {string}
        set interface {string}
      next
    end
  next
end
end
end

```

## config router bgp

Parameter	Description	Type	Size	Default
as	Router AS number, valid from 1 to 4294967295, 0 to disable BGP.	integer	Minimum value: 0 Maximum value: 4294967295	0
router-id	Router ID.	ipv4-address-any	Not Specified	
keepalive-timer	Frequency to send keep alive requests.	integer	Minimum value: 0 Maximum value: 65535	60
holdtime-timer	Number of seconds to mark peer as dead.	integer	Minimum value: 3 Maximum value: 65535	180

Parameter	Description	Type	Size	Default
always-compare-med	Enable/disable always compare MED.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-as-path-ignore	Enable/disable ignore AS path.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-cmp-confed-asp-path	Enable/disable compare federation AS path length.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-cmp-routerid	Enable/disable compare router ID for identical EBGp paths.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-med-confed	Enable/disable compare MED among confederation paths.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-med-missing-as-worst	Enable/disable treat missing MED as least preferred.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
client-to-client-reflection	Enable/disable client-to-client route reflection.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dampening	Enable/disable route-flap dampening.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
deterministic-med	Enable/disable enforce deterministic comparison of MED.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ebgp-multipath	Enable/disable EBGp multi-path.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ibgp-multipath	Enable/disable IBGP multi-path.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
enforce-first-as	Enable/disable enforce first AS for EBGp routes.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
fast-external-failover	Enable/disable reset peer BGP session if link goes down.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
log-neighbour-changes	Enable logging of BGP neighbour's changes	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
network-import-check	Enable/disable ensure BGP network route exists in IGP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ignore-optional-capability	Don't send unknown optional capability notification message	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path	Enable/disable selection of BGP IPv4 additional paths.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path6	Enable/disable selection of BGP IPv6 additional paths.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									



Parameter	Description	Type	Size	Default
multipath-recursive-distance	Enable/disable use of recursive distance to select multipath.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
cluster-id	Route reflector cluster ID.	ipv4-address-any	Not Specified	0.0.0.0
confederation-identifier	Confederation identifier.	integer	Minimum value: 1 Maximum value: 4294967295	0
confederation-peers <peer>	Confederation peers. Peer ID.	string	Maximum length: 79	
dampening-route-map	Criteria for dampening.	string	Maximum length: 35	
dampening-reachability-half-life	Reachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45	15
dampening-reuse	Threshold to reuse routes.	integer	Minimum value: 1 Maximum value: 20000	750
dampening-suppress	Threshold to suppress routes.	integer	Minimum value: 1 Maximum value: 20000	2000
dampening-max-suppress-time	Maximum minutes a route can be suppressed.	integer	Minimum value: 1 Maximum value: 255	60
dampening-unreachability-half-life	Unreachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45	15

Parameter	Description	Type	Size	Default						
default-local-preference	Default local preference.	integer	Minimum value: 0 Maximum value: 4294967295	100						
scan-time	Background scanner interval (sec), 0 to disable it.	integer	Minimum value: 5 Maximum value: 60	60						
distance-external	Distance for routes external to the AS.	integer	Minimum value: 1 Maximum value: 255	20						
distance-internal	Distance for routes internal to the AS.	integer	Minimum value: 1 Maximum value: 255	200						
distance-local	Distance for routes local to the AS.	integer	Minimum value: 1 Maximum value: 255	200						
synchronization	Enable/disable only advertise routes from iBGP if routes present in an IGP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
graceful-restart	Enable/disable BGP graceful restart capabilities.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
graceful-restart-time	Time needed for neighbors to restart (sec).	integer	Minimum value: 1 Maximum value: 3600	120						

Parameter	Description	Type	Size	Default						
graceful-stalepath-time	Time to hold stale paths of restarting neighbor (sec).	integer	Minimum value: 1 Maximum value: 3600	360						
graceful-update-delay	Route advertisement/selection delay after restart (sec).	integer	Minimum value: 1 Maximum value: 3600	120						
graceful-end-on-timer	Enable/disable to exit graceful restart on timer only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path-select	Number of additional paths to be selected for each IPv4 NLRI.	integer	Minimum value: 2 Maximum value: 255	2						
additional-path-select6	Number of additional paths to be selected for each IPv6 NLRI.	integer	Minimum value: 2 Maximum value: 255	2						

### config aggregate-address

Parameter	Description	Type	Size	Default						
prefix	Aggregate prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0						
as-set	Enable/disable generate AS set path information.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

## config aggregate-address6

Parameter	Description	Type	Size	Default
prefix6	Aggregate IPv6 prefix.	ipv6-prefix	Not Specified	::/0
as-set	Enable/disable generate AS set path information.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config neighbor

Parameter	Description	Type	Size	Default
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 1 Maximum value: 600	30
allows-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
allows-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
allows-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0

Parameter	Description	Type	Size	Default								
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0								
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>as-path</i></td> <td>AS path.</td> </tr> <tr> <td><i>med</i></td> <td>MED.</td> </tr> <tr> <td><i>next-hop</i></td> <td>Next hop.</td> </tr> </tbody> </table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>as-path</i></td> <td>AS path.</td> </tr> <tr> <td><i>med</i></td> <td>MED.</td> </tr> <tr> <td><i>next-hop</i></td> <td>Next hop.</td> </tr> </tbody> </table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
bfd	Enable/disable BFD for this neighbor.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default										
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>receive</i></td> <td>Receive ORF lists.</td> </tr> <tr> <td><i>send</i></td> <td>Send ORF list.</td> </tr> <tr> <td><i>both</i></td> <td>Send and receive ORF lists.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>receive</i></td> <td>Receive ORF lists.</td> </tr> <tr> <td><i>send</i></td> <td>Send ORF list.</td> </tr> <tr> <td><i>both</i></td> <td>Send and receive ORF lists.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
link-down-failover	Enable/disable failover upon link down.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
stale-route	Enable/disable stale route after neighbor down.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
override-capability	Enable/disable override result of capability negotiation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									



Parameter	Description	Type	Size	Default						
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
shutdown	Enable/disable shutdown this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
strict-capability-match	Enable/disable strict capability matching.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35							
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35							
description	Description.	string	Maximum length: 63							
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35							
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35							
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255						
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35							
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35							
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35							
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35							
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default						
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0						
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0						
maximum-prefix-threshold	Maximum IPv4 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35							
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35							
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35							
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295	0						
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0						
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0						
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35							
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35							
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35							
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35							
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35							
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default										
send-community	IPv4 Send community attribute to neighbor.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standard</i></td> <td>Standard.</td> </tr> <tr> <td><i>extended</i></td> <td>Extended.</td> </tr> <tr> <td><i>both</i></td> <td>Both.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable</td> </tr> </tbody> </table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
Option	Description													
<i>standard</i>	Standard.													
<i>extended</i>	Extended.													
<i>both</i>	Both.													
<i>disable</i>	Disable													
send-community6	IPv6 Send community attribute to neighbor.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standard</i></td> <td>Standard.</td> </tr> <tr> <td><i>extended</i></td> <td>Extended.</td> </tr> <tr> <td><i>both</i></td> <td>Both.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable</td> </tr> </tbody> </table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
Option	Description													
<i>standard</i>	Standard.													
<i>extended</i>	Extended.													
<i>both</i>	Both.													
<i>disable</i>	Disable													
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295										
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295										
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535	4294967295										
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15											
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295										

Parameter	Description	Type	Size	Default										
restart-time	Graceful restart delay time .	integer	Minimum value: 0 Maximum value: 3600	0										
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>send</i></td> <td>Enable sending additional paths.</td> </tr> <tr> <td><i>receive</i></td> <td>Enable receiving additional paths.</td> </tr> <tr> <td><i>both</i></td> <td>Enable sending and receiving additional paths.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable additional paths.</td> </tr> </tbody> </table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
Option	Description													
<i>send</i>	Enable sending additional paths.													
<i>receive</i>	Enable receiving additional paths.													
<i>both</i>	Enable sending and receiving additional paths.													
<i>disable</i>	Disable additional paths.													
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>send</i></td> <td>Enable sending additional paths.</td> </tr> <tr> <td><i>receive</i></td> <td>Enable receiving additional paths.</td> </tr> <tr> <td><i>both</i></td> <td>Enable sending and receiving additional paths.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable additional paths.</td> </tr> </tbody> </table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
Option	Description													
<i>send</i>	Enable sending additional paths.													
<i>receive</i>	Enable receiving additional paths.													
<i>both</i>	Enable sending and receiving additional paths.													
<i>disable</i>	Disable additional paths.													
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										
password	Password used in MD5 authentication.	password	Not Specified											

### config conditional-advertise

Parameter	Description	Type	Size	Default
condition-routemap	Name of condition route map.	string	Maximum length: 35	
condition-type	Type of condition.	option	-	exist

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exist</i></td> <td>True if condition route map is matched.</td> </tr> <tr> <td><i>non-exist</i></td> <td>True if condition route map is not matched.</td> </tr> </tbody> </table>	Option	Description	<i>exist</i>	True if condition route map is matched.	<i>non-exist</i>	True if condition route map is not matched.			
Option	Description									
<i>exist</i>	True if condition route map is matched.									
<i>non-exist</i>	True if condition route map is not matched.									

## config neighbor-group

Parameter	Description	Type	Size	Default						
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 1 Maximum value: 600	30						
allows-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allows-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allows-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0						
allows-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0						
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>as-path</i></td> <td>AS path.</td> </tr> <tr> <td><i>med</i></td> <td>MED.</td> </tr> </tbody> </table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.			
Option	Description									
<i>as-path</i>	AS path.									
<i>med</i>	MED.									



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>next-hop</i></td> <td>Next hop.</td> </tr> </tbody> </table>	Option	Description	<i>next-hop</i>	Next hop.							
Option	Description											
<i>next-hop</i>	Next hop.											
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>as-path</i></td> <td>AS path.</td> </tr> <tr> <td><i>med</i></td> <td>MED.</td> </tr> <tr> <td><i>next-hop</i></td> <td>Next hop.</td> </tr> </tbody> </table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
bfd	Enable/disable BFD for this neighbor.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none								

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>receive</i></td> <td>Receive ORF lists.</td> </tr> <tr> <td><i>send</i></td> <td>Send ORF list.</td> </tr> <tr> <td><i>both</i></td> <td>Send and receive ORF lists.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>receive</i></td> <td>Receive ORF lists.</td> </tr> <tr> <td><i>send</i></td> <td>Send ORF list.</td> </tr> <tr> <td><i>both</i></td> <td>Send and receive ORF lists.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
link-down-failover	Enable/disable failover upon link down.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
stale-route	Enable/disable stale route after neighbor down.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
override-capability	Enable/disable override result of capability negotiation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
shutdown	Enable/disable shutdown this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
strict-capability-match	Enable/disable strict capability matching.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35	
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35	
description	Description.	string	Maximum length: 63	
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35	
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35	
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35	
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35	
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35	
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35	
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35	
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35	
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15	
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
maximum-prefix-threshold	Maximum IPv4 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35							
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35							
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35							
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35							
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295	0						
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0						



Parameter	Description	Type	Size	Default										
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0										
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35											
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35											
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35											
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35											
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35											
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35											
send-community	IPv4 Send community attribute to neighbor.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standard</i></td> <td>Standard.</td> </tr> <tr> <td><i>extended</i></td> <td>Extended.</td> </tr> <tr> <td><i>both</i></td> <td>Both.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable</td> </tr> </tbody> </table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
Option	Description													
<i>standard</i>	Standard.													
<i>extended</i>	Extended.													
<i>both</i>	Both.													
<i>disable</i>	Disable													
send-community6	IPv6 Send community attribute to neighbor.	option	-	both										

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standard</i></td> <td>Standard.</td> </tr> <tr> <td><i>extended</i></td> <td>Extended.</td> </tr> <tr> <td><i>both</i></td> <td>Both.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable</td> </tr> </tbody> </table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
Option	Description													
<i>standard</i>	Standard.													
<i>extended</i>	Extended.													
<i>both</i>	Both.													
<i>disable</i>	Disable													
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295										
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295										
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535	4294967295										
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15											
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295										
restart-time	Graceful restart delay time .	integer	Minimum value: 0 Maximum value: 3600	0										
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>send</i></td> <td>Enable sending additional paths.</td> </tr> <tr> <td><i>receive</i></td> <td>Enable receiving additional paths.</td> </tr> </tbody> </table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.							
Option	Description													
<i>send</i>	Enable sending additional paths.													
<i>receive</i>	Enable receiving additional paths.													

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>both</i></td> <td>Enable sending and receiving additional paths.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable additional paths.</td> </tr> </tbody> </table>	Option	Description	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.							
Option	Description													
<i>both</i>	Enable sending and receiving additional paths.													
<i>disable</i>	Disable additional paths.													
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>send</i></td> <td>Enable sending additional paths.</td> </tr> <tr> <td><i>receive</i></td> <td>Enable receiving additional paths.</td> </tr> <tr> <td><i>both</i></td> <td>Enable sending and receiving additional paths.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable additional paths.</td> </tr> </tbody> </table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
Option	Description													
<i>send</i>	Enable sending additional paths.													
<i>receive</i>	Enable receiving additional paths.													
<i>both</i>	Enable sending and receiving additional paths.													
<i>disable</i>	Disable additional paths.													
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										

### config neighbor-range

Parameter	Description	Type	Size	Default
prefix	Neighbor range prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	

### config neighbor-range6

Parameter	Description	Type	Size	Default
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	

### config network

Parameter	Description	Type	Size	Default						
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
backdoor	Enable/disable route as backdoor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-map	Route map to modify generated route.	string	Maximum length: 35							

### config network6

Parameter	Description	Type	Size	Default						
prefix6	Network IPv6 prefix.	ipv6-network	Not Specified	::/0						
backdoor	Enable/disable route as backdoor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-map	Route map to modify generated route.	string	Maximum length: 35							

### config redistribute

Parameter	Description	Type	Size	Default
status	Status	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-map	Route map name.	string	Maximum length: 35							

### config redistribute6

Parameter	Description	Type	Size	Default						
status	Status	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-map	Route map name.	string	Maximum length: 35							

### config admin-distance

Parameter	Description	Type	Size	Default
neighbour-prefix	Neighbor address prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
route-list	Access list of routes to apply new distance to.	string	Maximum length: 35	
distance	Administrative distance to apply .	integer	Minimum value: 1 Maximum value: 255	0

### config target

Parameter	Description	Type	Size	Default
route-map	Route map of VRF leaking.	string	Maximum length: 35	
interface	Interface which is used to leak routes to target VRF.	string	Maximum length: 15	

---

## config router isis

### Configure IS-IS.

```
config router isis
  Description: Configure IS-IS.
  set is-type [level-1-2|level-1|...]
  set adv-passive-only [enable|disable]
  set adv-passive-only6 [enable|disable]
  set auth-mode-l1 [password|md5]
  set auth-mode-l2 [password|md5]
  set auth-password-l1 {password}
  set auth-password-l2 {password}
  set auth-keychain-l1 {string}
  set auth-keychain-l2 {string}
  set auth-sendonly-l1 [enable|disable]
  set auth-sendonly-l2 [enable|disable]
  set ignore-lsp-errors [enable|disable]
  set lsp-gen-interval-l1 {integer}
  set lsp-gen-interval-l2 {integer}
  set lsp-refresh-interval {integer}
  set max-lsp-lifetime {integer}
  set spf-interval-exp-l1 {user}
  set spf-interval-exp-l2 {user}
  set dynamic-hostname [enable|disable]
  set adjacency-check [enable|disable]
  set adjacency-check6 [enable|disable]
  set overload-bit [enable|disable]
  set overload-bit-suppress {option1}, {option2}, ...
  set overload-bit-on-startup {integer}
  set default-originate [enable|disable]
  set default-originate6 [enable|disable]
  set metric-style [narrow|wide|...]
  set redistribute-l1 [enable|disable]
  set redistribute-l1-list {string}
  set redistribute-l2 [enable|disable]
  set redistribute-l2-list {string}
  set redistribute6-l1 [enable|disable]
  set redistribute6-l1-list {string}
  set redistribute6-l2 [enable|disable]
  set redistribute6-l2-list {string}
config isis-net
  Description: IS-IS net configuration.
  edit <id>
    set net {user}
  next
end
config isis-interface
  Description: IS-IS interface configuration.
  edit <name>
    set status [enable|disable]
    set status6 [enable|disable]
    set network-type [broadcast|point-to-point|...]
    set circuit-type [level-1-2|level-1|...]
    set csnp-interval-l1 {integer}
    set csnp-interval-l2 {integer}
    set hello-interval-l1 {integer}
```

```

    set hello-interval-12 {integer}
    set hello-multiplier-11 {integer}
    set hello-multiplier-12 {integer}
    set hello-padding [enable|disable]
    set lsp-interval {integer}
    set lsp-retransmit-interval {integer}
    set metric-11 {integer}
    set metric-12 {integer}
    set wide-metric-11 {integer}
    set wide-metric-12 {integer}
    set auth-password-11 {password}
    set auth-password-12 {password}
    set auth-keychain-11 {string}
    set auth-keychain-12 {string}
    set auth-send-only-11 [enable|disable]
    set auth-send-only-12 [enable|disable]
    set auth-mode-11 [md5|password]
    set auth-mode-12 [md5|password]
    set priority-11 {integer}
    set priority-12 {integer}
    set mesh-group [enable|disable]
    set mesh-group-id {integer}
  next
end
config summary-address
  Description: IS-IS summary addresses.
  edit <id>
    set prefix {ipv4-classnet-any}
    set level [level-1-2|level-1|...]
  next
end
config summary-address6
  Description: IS-IS IPv6 summary address.
  edit <id>
    set prefix6 {ipv6-prefix}
    set level [level-1-2|level-1|...]
  next
end
config redistribute
  Description: IS-IS redistribute protocols.
  edit <protocol>
    set status [enable|disable]
    set metric {integer}
    set metric-type [external|internal]
    set level [level-1-2|level-1|...]
    set routemap {string}
  next
end
config redistribute6
  Description: IS-IS IPv6 redistribution for routing protocols.
  edit <protocol>
    set status [enable|disable]
    set metric {integer}
    set metric-type [external|internal]
    set level [level-1-2|level-1|...]
    set routemap {string}
  next

```

```

end
end

```

## config router isis

Parameter	Description	Type	Size	Default								
is-type	IS type.	option	-	level-1-2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>level-1-2</i></td> <td>Level 1 and 2.</td> </tr> <tr> <td><i>level-1</i></td> <td>Level 1 only.</td> </tr> <tr> <td><i>level-2-only</i></td> <td>Level 2 only.</td> </tr> </tbody> </table>	Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1 only.	<i>level-2-only</i>	Level 2 only.			
Option	Description											
<i>level-1-2</i>	Level 1 and 2.											
<i>level-1</i>	Level 1 only.											
<i>level-2-only</i>	Level 2 only.											
adv-passive-only	Enable/disable IS-IS advertisement of passive interfaces only.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Advertise passive interfaces only.</td> </tr> <tr> <td><i>disable</i></td> <td>Advertise all IS-IS enabled interfaces.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Advertise passive interfaces only.	<i>disable</i>	Advertise all IS-IS enabled interfaces.					
Option	Description											
<i>enable</i>	Advertise passive interfaces only.											
<i>disable</i>	Advertise all IS-IS enabled interfaces.											
adv-passive-only6	Enable/disable IPv6 IS-IS advertisement of passive interfaces only.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Advertise passive interfaces only.</td> </tr> <tr> <td><i>disable</i></td> <td>Advertise all IS-IS enabled interfaces.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Advertise passive interfaces only.	<i>disable</i>	Advertise all IS-IS enabled interfaces.					
Option	Description											
<i>enable</i>	Advertise passive interfaces only.											
<i>disable</i>	Advertise all IS-IS enabled interfaces.											
auth-mode-l1	Level 1 authentication mode.	option	-	password								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>password</i></td> <td>Password.</td> </tr> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> </tbody> </table>	Option	Description	<i>password</i>	Password.	<i>md5</i>	MD5.					
Option	Description											
<i>password</i>	Password.											
<i>md5</i>	MD5.											
auth-mode-l2	Level 2 authentication mode.	option	-	password								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>password</i></td> <td>Password.</td> </tr> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> </tbody> </table>	Option	Description	<i>password</i>	Password.	<i>md5</i>	MD5.					
Option	Description											
<i>password</i>	Password.											
<i>md5</i>	MD5.											
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified									



Parameter	Description	Type	Size	Default
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified	
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	
auth-sendonly-l1	Enable/disable level 1 authentication send-only.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable level 1 authentication send-only.		
	<i>disable</i>	Disable level 1 authentication send-only.		
auth-sendonly-l2	Enable/disable level 2 authentication send-only.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable level 2 authentication send-only.		
	<i>disable</i>	Disable level 2 authentication send-only.		
ignore-lsp-errors	Enable/disable ignoring of LSP errors with bad checksums.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ignoring of LSP errors with bad checksums.		
	<i>disable</i>	Disable ignoring of LSP errors with bad checksums.		
lsp-gen-interval-l1	Minimum interval for level 1 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30
lsp-gen-interval-l2	Minimum interval for level 2 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30
lsp-refresh-interval	LSP refresh time in seconds.	integer	Minimum value: 1 Maximum value: 65535	900

Parameter	Description	Type	Size	Default						
max-lsp-lifetime	Maximum LSP lifetime in seconds.	integer	Minimum value: 350 Maximum value: 65535	1200						
spf-interval-exp-l1	Level 1 SPF calculation delay.	user	Not Specified							
spf-interval-exp-l2	Level 2 SPF calculation delay.	user	Not Specified							
dynamic-hostname	Enable/disable dynamic hostname.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dynamic hostname.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dynamic hostname.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dynamic hostname.	<i>disable</i>	Disable dynamic hostname.			
Option	Description									
<i>enable</i>	Enable dynamic hostname.									
<i>disable</i>	Disable dynamic hostname.									
adjacency-check	Enable/disable adjacency check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adjacency check.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adjacency check.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adjacency check.	<i>disable</i>	Disable adjacency check.			
Option	Description									
<i>enable</i>	Enable adjacency check.									
<i>disable</i>	Disable adjacency check.									
adjacency-check6	Enable/disable IPv6 adjacency check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPv6 adjacency check.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPv6 adjacency check.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPv6 adjacency check.	<i>disable</i>	Disable IPv6 adjacency check.			
Option	Description									
<i>enable</i>	Enable IPv6 adjacency check.									
<i>disable</i>	Disable IPv6 adjacency check.									
overload-bit	Enable/disable signal other routers not to use us in SPF.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable overload bit.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable overload bit.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable overload bit.	<i>disable</i>	Disable overload bit.			
Option	Description									
<i>enable</i>	Enable overload bit.									
<i>disable</i>	Disable overload bit.									
overload-bit-suppress	Suppress overload-bit for the specific prefixes.	option	-							

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>external</i></td> <td>External.</td> </tr> <tr> <td><i>interlevel</i></td> <td>Inter-level.</td> </tr> </tbody> </table>	Option	Description	<i>external</i>	External.	<i>interlevel</i>	Inter-level.																	
Option	Description																							
<i>external</i>	External.																							
<i>interlevel</i>	Inter-level.																							
overload-bit-on-startup	Overload-bit only temporarily after reboot.	integer	Minimum value: 5 Maximum value: 86400	0																				
default-originate	Enable/disable distribution of default route information.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable distribution of default route information.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable distribution of default route information.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable distribution of default route information.	<i>disable</i>	Disable distribution of default route information.																	
Option	Description																							
<i>enable</i>	Enable distribution of default route information.																							
<i>disable</i>	Disable distribution of default route information.																							
default-originate6	Enable/disable distribution of default IPv6 route information.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable distribution of default IPv6 route information.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable distribution of default IPv6 route information.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable distribution of default IPv6 route information.	<i>disable</i>	Disable distribution of default IPv6 route information.																	
Option	Description																							
<i>enable</i>	Enable distribution of default IPv6 route information.																							
<i>disable</i>	Disable distribution of default IPv6 route information.																							
metric-style	Use old-style (ISO 10589) or new-style packet formats	option	-	narrow																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>narrow</i></td> <td>Use old style of TLVs with narrow metric.</td> </tr> <tr> <td><i>wide</i></td> <td>Use new style of TLVs to carry wider metric.</td> </tr> <tr> <td><i>transition</i></td> <td>Send and accept both styles of TLVs during transition.</td> </tr> <tr> <td><i>narrow-transition</i></td> <td>Narrow and accept both styles of TLVs during transition.</td> </tr> <tr> <td><i>narrow-transition-l1</i></td> <td>Narrow-transition level-1 only.</td> </tr> <tr> <td><i>narrow-transition-l2</i></td> <td>Narrow-transition level-2 only.</td> </tr> <tr> <td><i>wide-l1</i></td> <td>Wide level-1 only.</td> </tr> <tr> <td><i>wide-l2</i></td> <td>Wide level-2 only.</td> </tr> <tr> <td><i>wide-transition</i></td> <td>Wide and accept both styles of TLVs during transition.</td> </tr> </tbody> </table>	Option	Description	<i>narrow</i>	Use old style of TLVs with narrow metric.	<i>wide</i>	Use new style of TLVs to carry wider metric.	<i>transition</i>	Send and accept both styles of TLVs during transition.	<i>narrow-transition</i>	Narrow and accept both styles of TLVs during transition.	<i>narrow-transition-l1</i>	Narrow-transition level-1 only.	<i>narrow-transition-l2</i>	Narrow-transition level-2 only.	<i>wide-l1</i>	Wide level-1 only.	<i>wide-l2</i>	Wide level-2 only.	<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.			
Option	Description																							
<i>narrow</i>	Use old style of TLVs with narrow metric.																							
<i>wide</i>	Use new style of TLVs to carry wider metric.																							
<i>transition</i>	Send and accept both styles of TLVs during transition.																							
<i>narrow-transition</i>	Narrow and accept both styles of TLVs during transition.																							
<i>narrow-transition-l1</i>	Narrow-transition level-1 only.																							
<i>narrow-transition-l2</i>	Narrow-transition level-2 only.																							
<i>wide-l1</i>	Wide level-1 only.																							
<i>wide-l2</i>	Wide level-2 only.																							
<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.																							

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wide-transition-I1</i></td> <td>Wide-transition level-1 only.</td> </tr> <tr> <td><i>wide-transition-I2</i></td> <td>Wide-transition level-2 only.</td> </tr> <tr> <td><i>transition-I1</i></td> <td>Transition level-1 only.</td> </tr> <tr> <td><i>transition-I2</i></td> <td>Transition level-2 only.</td> </tr> </tbody> </table>	Option	Description	<i>wide-transition-I1</i>	Wide-transition level-1 only.	<i>wide-transition-I2</i>	Wide-transition level-2 only.	<i>transition-I1</i>	Transition level-1 only.	<i>transition-I2</i>	Transition level-2 only.			
Option	Description													
<i>wide-transition-I1</i>	Wide-transition level-1 only.													
<i>wide-transition-I2</i>	Wide-transition level-2 only.													
<i>transition-I1</i>	Transition level-1 only.													
<i>transition-I2</i>	Transition level-2 only.													
redistribute-I1	Enable/disable redistribution of level 1 routes into level 2.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redistribution of level 1 routes into level 2.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redistribution of level 1 routes into level 2.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redistribution of level 1 routes into level 2.	<i>disable</i>	Disable redistribution of level 1 routes into level 2.							
Option	Description													
<i>enable</i>	Enable redistribution of level 1 routes into level 2.													
<i>disable</i>	Disable redistribution of level 1 routes into level 2.													
redistribute-I1-list	Access-list for route redistribution from I1 to I2.	string	Maximum length: 35											
redistribute-I2	Enable/disable redistribution of level 2 routes into level 1.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redistribution of level 2 routes into level 1.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redistribution of level 2 routes into level 1.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redistribution of level 2 routes into level 1.	<i>disable</i>	Disable redistribution of level 2 routes into level 1.							
Option	Description													
<i>enable</i>	Enable redistribution of level 2 routes into level 1.													
<i>disable</i>	Disable redistribution of level 2 routes into level 1.													
redistribute-I2-list	Access-list for route redistribution from I2 to I1.	string	Maximum length: 35											
redistribute6-I1	Enable/disable redistribution of level 1 IPv6 routes into level 2.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redistribution of level 1 IPv6 routes into level 2.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redistribution of level 1 IPv6 routes into level 2.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redistribution of level 1 IPv6 routes into level 2.	<i>disable</i>	Disable redistribution of level 1 IPv6 routes into level 2.							
Option	Description													
<i>enable</i>	Enable redistribution of level 1 IPv6 routes into level 2.													
<i>disable</i>	Disable redistribution of level 1 IPv6 routes into level 2.													
redistribute6-I1-list	Access-list for IPv6 route redistribution from I1 to I2.	string	Maximum length: 35											
redistribute6-I2	Enable/disable redistribution of level 2 IPv6 routes into level 1.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redistribution of level 2 IPv6 routes into level 1.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redistribution of level 2 IPv6 routes into level 1.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redistribution of level 2 IPv6 routes into level 1.	<i>disable</i>	Disable redistribution of level 2 IPv6 routes into level 1.							
Option	Description													
<i>enable</i>	Enable redistribution of level 2 IPv6 routes into level 1.													
<i>disable</i>	Disable redistribution of level 2 IPv6 routes into level 1.													

Parameter	Description	Type	Size	Default
redistribute6-l2-list	Access-list for IPv6 route redistribution from I2 to I1.	string	Maximum length: 35	

### config isis-net

Parameter	Description	Type	Size	Default
net	IS-IS net xx.xxxx. ... .xxxx.xx.	user	Not Specified	

### config isis-interface

Parameter	Description	Type	Size	Default								
status	Enable/disable interface for IS-IS.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable interface for IS-IS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable interface for IS-IS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable interface for IS-IS.	<i>disable</i>	Disable interface for IS-IS.					
Option	Description											
<i>enable</i>	Enable interface for IS-IS.											
<i>disable</i>	Disable interface for IS-IS.											
status6	Enable/disable IPv6 interface for IS-IS.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPv6 interface for IS-IS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPv6 interface for IS-IS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPv6 interface for IS-IS.	<i>disable</i>	Disable IPv6 interface for IS-IS.					
Option	Description											
<i>enable</i>	Enable IPv6 interface for IS-IS.											
<i>disable</i>	Disable IPv6 interface for IS-IS.											
network-type	IS-IS interface's network type	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>broadcast</i></td> <td>Broadcast.</td> </tr> <tr> <td><i>point-to-point</i></td> <td>Point-to-point.</td> </tr> <tr> <td><i>loopback</i></td> <td>Loopback.</td> </tr> </tbody> </table>	Option	Description	<i>broadcast</i>	Broadcast.	<i>point-to-point</i>	Point-to-point.	<i>loopback</i>	Loopback.			
Option	Description											
<i>broadcast</i>	Broadcast.											
<i>point-to-point</i>	Point-to-point.											
<i>loopback</i>	Loopback.											
circuit-type	IS-IS interface's circuit type	option	-	level-1-2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>level-1-2</i></td> <td>Level 1 and 2.</td> </tr> <tr> <td><i>level-1</i></td> <td>Level 1.</td> </tr> <tr> <td><i>level-2</i></td> <td>Level 2.</td> </tr> </tbody> </table>	Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1.	<i>level-2</i>	Level 2.			
Option	Description											
<i>level-1-2</i>	Level 1 and 2.											
<i>level-1</i>	Level 1.											
<i>level-2</i>	Level 2.											

Parameter	Description	Type	Size	Default						
csnp-interval-l1	Level 1 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535	10						
csnp-interval-l2	Level 2 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535	10						
hello-interval-l1	Level 1 hello interval.	integer	Minimum value: 0 Maximum value: 65535	10						
hello-interval-l2	Level 2 hello interval.	integer	Minimum value: 0 Maximum value: 65535	10						
hello-multiplier-l1	Level 1 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100	3						
hello-multiplier-l2	Level 2 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100	3						
hello-padding	Enable/disable padding to IS-IS hello packets.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable padding to IS-IS hello packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable padding to IS-IS hello packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable padding to IS-IS hello packets.	<i>disable</i>	Disable padding to IS-IS hello packets.			
Option	Description									
<i>enable</i>	Enable padding to IS-IS hello packets.									
<i>disable</i>	Disable padding to IS-IS hello packets.									
lsp-interval	LSP transmission interval (milliseconds).	integer	Minimum value: 1 Maximum value: 4294967295	33						
lsp-retransmit-interval	LSP retransmission interval (sec).	integer	Minimum value: 1 Maximum value: 65535	5						

Parameter	Description	Type	Size	Default
metric-l1	Level 1 metric for interface.	integer	Minimum value: 1 Maximum value: 63	10
metric-l2	Level 2 metric for interface.	integer	Minimum value: 1 Maximum value: 63	10
wide-metric-l1	Level 1 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10
wide-metric-l2	Level 2 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified	
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified	
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	
auth-send-only-l1	Enable/disable authentication send-only for level 1 PDUs.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable authentication send-only for level 1 PDUs.		
	<i>disable</i>	Disable authentication send-only for level 1 PDUs.		
auth-send-only-l2	Enable/disable authentication send-only for level 2 PDUs.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable authentication send-only for level 2 PDUs.		
	<i>disable</i>	Disable authentication send-only for level 2 PDUs.		

Parameter	Description	Type	Size	Default						
auth-mode-l1	Level 1 authentication mode.	option	-	password						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> <tr> <td><i>password</i></td> <td>Password.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	MD5.	<i>password</i>	Password.			
Option	Description									
<i>md5</i>	MD5.									
<i>password</i>	Password.									
auth-mode-l2	Level 2 authentication mode.	option	-	password						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>MD5.</td> </tr> <tr> <td><i>password</i></td> <td>Password.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	MD5.	<i>password</i>	Password.			
Option	Description									
<i>md5</i>	MD5.									
<i>password</i>	Password.									
priority-l1	Level 1 priority.	integer	Minimum value: 0 Maximum value: 127	64						
priority-l2	Level 2 priority.	integer	Minimum value: 0 Maximum value: 127	64						
mesh-group	Enable/disable IS-IS mesh group.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IS-IS mesh group.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IS-IS mesh group.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IS-IS mesh group.	<i>disable</i>	Disable IS-IS mesh group.			
Option	Description									
<i>enable</i>	Enable IS-IS mesh group.									
<i>disable</i>	Disable IS-IS mesh group.									
mesh-group-id	Mesh group ID <0-4294967295>, 0: mesh-group blocked.	integer	Minimum value: 0 Maximum value: 4294967295	0						

### config summary-address

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
level	Level.	option	-	level-2



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		

### config summary-address6

Parameter	Description	Type	Size	Default
prefix6	IPv6 prefix.	ipv6-prefix	Not Specified	::/0
level	Level.	option	-	level-2
	<b>Option</b>	<b>Description</b>		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		

### config redistribute

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable.		
	<i>disable</i>	Disable.		
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0
metric-type	Metric type.	option	-	internal
	<b>Option</b>	<b>Description</b>		
	<i>external</i>	External.		
	<i>internal</i>	Internal.		
level	Level.	option	-	level-2

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>level-1-2</i></td> <td>Level 1 and 2.</td> </tr> <tr> <td><i>level-1</i></td> <td>Level 1.</td> </tr> <tr> <td><i>level-2</i></td> <td>Level 2.</td> </tr> </tbody> </table>	Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1.	<i>level-2</i>	Level 2.			
Option	Description											
<i>level-1-2</i>	Level 1 and 2.											
<i>level-1</i>	Level 1.											
<i>level-2</i>	Level 2.											
routemap	Route map name.	string	Maximum length: 35									

### config redistribute6

Parameter	Description	Type	Size	Default								
status	Enable/disable redistribution.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redistribution.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redistribution.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redistribution.	<i>disable</i>	Disable redistribution.					
Option	Description											
<i>enable</i>	Enable redistribution.											
<i>disable</i>	Disable redistribution.											
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0								
metric-type	Metric type.	option	-	internal								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>external</i></td> <td>External metric type.</td> </tr> <tr> <td><i>internal</i></td> <td>Internal metric type.</td> </tr> </tbody> </table>	Option	Description	<i>external</i>	External metric type.	<i>internal</i>	Internal metric type.					
Option	Description											
<i>external</i>	External metric type.											
<i>internal</i>	Internal metric type.											
level	Level.	option	-	level-2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>level-1-2</i></td> <td>Level 1 and 2.</td> </tr> <tr> <td><i>level-1</i></td> <td>Level 1.</td> </tr> <tr> <td><i>level-2</i></td> <td>Level 2.</td> </tr> </tbody> </table>	Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1.	<i>level-2</i>	Level 2.			
Option	Description											
<i>level-1-2</i>	Level 1 and 2.											
<i>level-1</i>	Level 1.											
<i>level-2</i>	Level 2.											
routemap	Route map name.	string	Maximum length: 35									

### config router multicast-flow

Configure multicast-flow.

```

config router multicast-flow
  Description: Configure multicast-flow.
  edit <name>
    set comments {string}
    config flows
      Description: Multicast-flow entries.
      edit <id>
        set group-addr {ipv4-address-any}
        set source-addr {ipv4-address-any}
      next
    end
  next
end

```

## config router multicast-flow

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

## config flows

Parameter	Description	Type	Size	Default
group-addr	Multicast group IP address.	ipv4-address-any	Not Specified	0.0.0.0
source-addr	Multicast source IP address.	ipv4-address-any	Not Specified	0.0.0.0

## config router multicast

Configure router multicast.

```

config router multicast
  Description: Configure router multicast.
  set route-threshold {integer}
  set route-limit {integer}
  set multicast-routing [enable|disable]
  config pim-sm-global
    Description: PIM sparse-mode global settings.
    set message-interval {integer}
    set join-prune-holdtime {integer}
    set accept-register-list {string}
    set accept-source-list {string}
    set bsr-candidate [enable|disable]
    set bsr-interface {string}
    set bsr-priority {integer}
    set bsr-hash {integer}
    set bsr-allow-quick-refresh [enable|disable]
  end
end

```

```

set cisco-register-checksum [enable|disable]
set cisco-register-checksum-group {string}
set cisco-crp-prefix [enable|disable]
set cisco-ignore-rp-set-priority [enable|disable]
set register-rp-reachability [enable|disable]
set register-source [disable|interface|...]
set register-source-interface {string}
set register-source-ip {ipv4-address}
set register-suppression {integer}
set null-register-retries {integer}
set rp-register-keepalive {integer}
set spt-threshold [enable|disable]
set spt-threshold-group {string}
set ssm [enable|disable]
set ssm-range {string}
set register-rate-limit {integer}
config rp-address
    Description: Statically configure RP addresses.
    edit <id>
        set ip-address {ipv4-address}
        set group {string}
    next
end
end
config interface
    Description: PIM interfaces.
    edit <name>
        set ttl-threshold {integer}
        set pim-mode [sparse-mode|dense-mode]
        set passive [enable|disable]
        set bfd [enable|disable]
        set neighbour-filter {string}
        set hello-interval {integer}
        set hello-holdtime {integer}
        set cisco-exclude-genid [enable|disable]
        set dr-priority {integer}
        set propagation-delay {integer}
        set state-refresh-interval {integer}
        set rp-candidate [enable|disable]
        set rp-candidate-group {string}
        set rp-candidate-priority {integer}
        set rp-candidate-interval {integer}
        set multicast-flow {string}
        set static-group {string}
        set rpf-nbr-fail-back [enable|disable]
        set rpf-nbr-fail-back-filter {string}
        config join-group
            Description: Join multicast groups.
            edit <address>
                next
            end
        config igmp
            Description: IGMP configuration options.
            set access-group {string}
            set version [3|2|...]
            set immediate-leave-group {string}
            set last-member-query-interval {integer}

```

```

        set last-member-query-count {integer}
        set query-max-response-time {integer}
        set query-interval {integer}
        set query-timeout {integer}
        set router-alert-check [enable|disable]
    end
  next
end
end

```

## config router multicast

Parameter	Description	Type	Size	Default						
route-threshold	Generate warnings when the number of multicast routes exceeds this number, must not be greater than route-limit.	integer	Minimum value: 1 Maximum value: 2147483647							
route-limit	Maximum number of multicast routes.	integer	Minimum value: 1 Maximum value: 2147483647	2147483647						
multicast-routing	Enable/disable IP multicast routing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IP multicast routing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IP multicast routing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IP multicast routing.	<i>disable</i>	Disable IP multicast routing.			
Option	Description									
<i>enable</i>	Enable IP multicast routing.									
<i>disable</i>	Disable IP multicast routing.									

## config pim-sm-global

Parameter	Description	Type	Size	Default
message-interval	Period of time between sending periodic PIM join/prune messages in seconds .	integer	Minimum value: 1 Maximum value: 65535	60
join-prune-holdtime	Join/prune holdtime .	integer	Minimum value: 1 Maximum value: 65535	210

Parameter	Description	Type	Size	Default						
accept-register-list	Sources allowed to register packets with this Rendezvous Point (RP).	string	Maximum length: 35							
accept-source-list	Sources allowed to send multicast traffic.	string	Maximum length: 35							
bsr-candidate	Enable/disable allowing this router to become a bootstrap router (BSR).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow this router to function as a BSR.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow this router to function as a BSR.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Allow this router to function as a BSR.	<i>disable</i>	Do not allow this router to function as a BSR.		
Option	Description									
<i>enable</i>	Allow this router to function as a BSR.									
<i>disable</i>	Do not allow this router to function as a BSR.									
bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15							
bsr-priority	BSR priority .	integer	Minimum value: 0 Maximum value: 255	0						
bsr-hash	BSR hash length .	integer	Minimum value: 0 Maximum value: 32	10						
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow quick refresh packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow quick refresh packets.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Allow quick refresh packets.	<i>disable</i>	Do not allow quick refresh packets.		
Option	Description									
<i>enable</i>	Allow quick refresh packets.									
<i>disable</i>	Do not allow quick refresh packets.									
cisco-register-checksum	Checksum entire register packet(for old Cisco IOS compatibility).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>register checksum entire packet.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not register checksum entire packet.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	register checksum entire packet.	<i>disable</i>	Do not register checksum entire packet.		
Option	Description									
<i>enable</i>	register checksum entire packet.									
<i>disable</i>	Do not register checksum entire packet.									
cisco-register-checksum-group	Cisco register checksum only these groups.	string	Maximum length: 35							
cisco-crp-prefix	Enable/disable making candidate RP compatible with old Cisco IOS.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Do not allow sending group prefix of zero.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow sending group prefix of zero.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Do not allow sending group prefix of zero.	<i>disable</i>	Allow sending group prefix of zero.					
Option	Description											
<i>enable</i>	Do not allow sending group prefix of zero.											
<i>disable</i>	Allow sending group prefix of zero.											
cisco-ignore-rp-set-priority	Use only hash for RP selection (compatibility with old Cisco IOS).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Ignore RP-SET priority value.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not ignore RP-SET priority value.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Ignore RP-SET priority value.	<i>disable</i>	Do not ignore RP-SET priority value.					
Option	Description											
<i>enable</i>	Ignore RP-SET priority value.											
<i>disable</i>	Do not ignore RP-SET priority value.											
register-rp-reachability	Enable/disable check RP is reachable before registering packets.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Check target RP is unicast reachable before registering.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not check RP unicast reachability.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Check target RP is unicast reachable before registering.	<i>disable</i>	Do not check RP unicast reachability.					
Option	Description											
<i>enable</i>	Check target RP is unicast reachable before registering.											
<i>disable</i>	Do not check RP unicast reachability.											
register-source	Override source address in register packets.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Use source address of RPF interface.</td> </tr> <tr> <td><i>interface</i></td> <td>Use primary IP of an interface.</td> </tr> <tr> <td><i>ip-address</i></td> <td>Use a local IP address.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Use source address of RPF interface.	<i>interface</i>	Use primary IP of an interface.	<i>ip-address</i>	Use a local IP address.			
Option	Description											
<i>disable</i>	Use source address of RPF interface.											
<i>interface</i>	Use primary IP of an interface.											
<i>ip-address</i>	Use a local IP address.											
register-source-interface	Override with primary interface address.	string	Maximum length: 15									
register-source-ip	Override with local IP address.	ipv4-address	Not Specified	0.0.0.0								
register-supression	Period of time to honor register-stop message .	integer	Minimum value: 1 Maximum value: 65535	60								
null-register-retries	Maximum retries of null register .	integer	Minimum value: 1 Maximum value: 20	1								

Parameter	Description	Type	Size	Default						
rp-register-keepalive	Timeout for RP receiving data on .	integer	Minimum value: 1 Maximum value: 65535	185						
spt-threshold	Enable/disable switching to source specific trees.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Switch to Source tree when available.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not switch to Source tree when available.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Switch to Source tree when available.	<i>disable</i>	Do not switch to Source tree when available.			
Option	Description									
<i>enable</i>	Switch to Source tree when available.									
<i>disable</i>	Do not switch to Source tree when available.									
spt-threshold-group	Groups allowed to switch to source tree.	string	Maximum length: 35							
ssm	Enable/disable source specific multicast.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow source specific multicast.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow source specific multicast.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow source specific multicast.	<i>disable</i>	Do not allow source specific multicast.			
Option	Description									
<i>enable</i>	Allow source specific multicast.									
<i>disable</i>	Do not allow source specific multicast.									
ssm-range	Groups allowed to source specific multicast.	string	Maximum length: 35							
register-rate-limit	Limit of packets/sec per source registered through this RP .	integer	Minimum value: 0 Maximum value: 65535	0						

### config rp-address

Parameter	Description	Type	Size	Default
ip-address	RP router address.	ipv4-address	Not Specified	0.0.0.0
group	Groups to use this RP.	string	Maximum length: 35	



## config interface

Parameter	Description	Type	Size	Default						
ttl-threshold	Minimum TTL of multicast packets that will be forwarded .	integer	Minimum value: 1 Maximum value: 255	1						
pim-mode	PIM operation mode.	option	-	sparse-mode						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sparse-mode</i></td> <td>sparse-mode</td> </tr> <tr> <td><i>dense-mode</i></td> <td>dense-mode</td> </tr> </tbody> </table>	Option	Description	<i>sparse-mode</i>	sparse-mode	<i>dense-mode</i>	dense-mode			
Option	Description									
<i>sparse-mode</i>	sparse-mode									
<i>dense-mode</i>	dense-mode									
passive	Enable/disable listening to IGMP but not participating in PIM.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Listen only.</td> </tr> <tr> <td><i>disable</i></td> <td>Participate in PIM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Listen only.	<i>disable</i>	Participate in PIM.			
Option	Description									
<i>enable</i>	Listen only.									
<i>disable</i>	Participate in PIM.									
bfd	Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).									
neighbour-filter	Routers acknowledged as neighbor routers.	string	Maximum length: 35							
hello-interval	Interval between sending PIM hello messages .	integer	Minimum value: 1 Maximum value: 65535	30						
hello-holdtime	Time before old neighbor information expires .	integer	Minimum value: 1 Maximum value: 65535							
cisco-exclude-genid	Exclude GenID from hello packets (compatibility with old Cisco IOS).	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Do not send GenID.</td> </tr> <tr> <td><i>disable</i></td> <td>Send GenID according to standard.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Do not send GenID.	<i>disable</i>	Send GenID according to standard.			
Option	Description									
<i>enable</i>	Do not send GenID.									
<i>disable</i>	Send GenID according to standard.									
dr-priority	DR election priority.	integer	Minimum value: 1 Maximum value: 4294967295	1						
propagation-delay	Delay flooding packets on this interface .	integer	Minimum value: 100 Maximum value: 5000	500						
state-refresh-interval	Interval between sending state-refresh packets .	integer	Minimum value: 1 Maximum value: 100	60						
rp-candidate	Enable/disable compete to become RP in elections.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Compete for RP elections.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not compete for RP elections.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Compete for RP elections.	<i>disable</i>	Do not compete for RP elections.			
Option	Description									
<i>enable</i>	Compete for RP elections.									
<i>disable</i>	Do not compete for RP elections.									
rp-candidate-group	Multicast groups managed by this RP.	string	Maximum length: 35							
rp-candidate-priority	Router's priority as RP.	integer	Minimum value: 0 Maximum value: 255	192						
rp-candidate-interval	RP candidate advertisement interval .	integer	Minimum value: 1 Maximum value: 16383	60						
multicast-flow	Acceptable source for multicast group.	string	Maximum length: 35							
static-group	Statically set multicast groups to forward out.	string	Maximum length: 35							
rpf-nbr-fail-back	Enable/disable fail back for RPF neighbor query.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable fail back for RPF neighbor query.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable fail back for RPF neighbor query.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable fail back for RPF neighbor query.	<i>disable</i>	Disable fail back for RPF neighbor query.			
Option	Description									
<i>enable</i>	Enable fail back for RPF neighbor query.									
<i>disable</i>	Disable fail back for RPF neighbor query.									
rpf-nbr-fail-back-filter	Filter for fail back RPF neighbors.	string	Maximum length: 35							

### config igmp

Parameter	Description	Type	Size	Default								
access-group	Groups IGMP hosts are allowed to join.	string	Maximum length: 35									
version	Maximum version of IGMP to support.	option	-	3								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Version 3 and lower.</td> </tr> <tr> <td>2</td> <td>Version 2 and lower.</td> </tr> <tr> <td>1</td> <td>Version 1.</td> </tr> </tbody> </table>	Option	Description	3	Version 3 and lower.	2	Version 2 and lower.	1	Version 1.			
Option	Description											
3	Version 3 and lower.											
2	Version 2 and lower.											
1	Version 1.											
immediate-leave-group	Groups to drop membership for immediately after receiving IGMPv2 leave.	string	Maximum length: 35									
last-member-query-interval	Timeout between IGMPv2 leave and removing group .	integer	Minimum value: 1 Maximum value: 65535	1000								
last-member-query-count	Number of group specific queries before removing group .	integer	Minimum value: 2 Maximum value: 7	2								
query-max-response-time	Maximum time to wait for a IGMP query response .	integer	Minimum value: 1 Maximum value: 25	10								
query-interval	Interval between queries to IGMP hosts .	integer	Minimum value: 1 Maximum value: 65535	125								

Parameter	Description	Type	Size	Default
query-timeout	Timeout between queries before becoming querier for network .	integer	Minimum value: 60 Maximum value: 900	255
router-alert-check	Enable/disable require IGMP packets contain router alert option.	option	-	disable

Option	Description
<i>enable</i>	Require Router Alert option in IGMP packets.
<i>disable</i>	don't require Router Alert option in IGMP packets

## config router multicast6

Configure IPv6 multicast.

```

config router multicast6
  Description: Configure IPv6 multicast.
  set multicast-routing [enable|disable]
  set multicast-pmtu [enable|disable]
  config interface
    Description: Protocol Independent Multicast (PIM) interfaces.
    edit <name>
      set hello-interval {integer}
      set hello-holdtime {integer}
    next
  end
  config pim-sm-global
    Description: PIM sparse-mode global settings.
    set register-rate-limit {integer}
    config rp-address
      Description: Statically configured RP addresses.
      edit <id>
        set ip6-address {ipv6-address}
      next
    end
  end
end
end

```

## config router multicast6

Parameter	Description	Type	Size	Default
multicast-routing	Enable/disable IPv6 multicast routing.	option	-	disable

Option	Description
<i>enable</i>	Enable IPv6 multicast routing.

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IPv6 multicast routing.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IPv6 multicast routing.					
Option	Description									
<i>disable</i>	Disable IPv6 multicast routing.									
multicast-pmtu	Enable/disable PMTU for IPv6 multicast.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PMTU for IPv6 multicast.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PMTU for IPv6 multicast.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PMTU for IPv6 multicast.	<i>disable</i>	Disable PMTU for IPv6 multicast.			
Option	Description									
<i>enable</i>	Enable PMTU for IPv6 multicast.									
<i>disable</i>	Disable PMTU for IPv6 multicast.									

### config interface

Parameter	Description	Type	Size	Default
hello-interval	Interval between sending PIM hello messages ..	integer	Minimum value: 1 Maximum value: 65535	30
hello-holdtime	Time before old neighbour information expires .	integer	Minimum value: 1 Maximum value: 65535	

### config pim-sm-global

Parameter	Description	Type	Size	Default
register-rate-limit	Limit of packets/sec per source registered through this RP (0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535	0

### config rp-address

Parameter	Description	Type	Size	Default
ip6-address	RP router IPv6 address.	ipv6-address	Not Specified	::

### config router info

Show routing information.

---

```
config router info
  Description: Show routing information.
end
```

## config router info6

Show IPv6 routing information.

```
config router info6
  Description: Show IPv6 routing information.
end
```

## config router auth-path

Configure authentication based routing.

```
config router auth-path
  Description: Configure authentication based routing.
  edit <name>
    set device {string}
    set gateway {ipv4-address}
  next
end
```

## config router auth-path

Parameter	Description	Type	Size	Default
device	Outgoing interface.	string	Maximum length: 35	
gateway	Gateway IP address.	ipv4-address	Not Specified	0.0.0.0

## config router setting

Configure router settings.

```
config router setting
  Description: Configure router settings.
  set show-filter {string}
  set hostname {string}
end
```

## config router setting

Parameter	Description	Type	Size	Default
show-filter	Prefix-list as filter for showing routes.	string	Maximum length: 35	
hostname	Hostname for this virtual domain router.	string	Maximum length: 14	

## config router bfd

Configure BFD.

```
config router bfd
  Description: Configure BFD.
  config neighbor
    Description: neighbor
    edit <ip>
      set interface {string}
    next
  end
end
```

### config neighbor

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	

## config router bfd6

Configure IPv6 BFD.

```
config router bfd6
  Description: Configure IPv6 BFD.
  config neighbor
    Description: Configure neighbor of IPv6 BFD.
    edit <ip6-address>
      set interface {string}
    next
  end
end
```

### config neighbor

Parameter	Description	Type	Size	Default
interface	Interface to the BFD neighbor.	string	Maximum length: 15	

## ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 664](#)

### config ssh-filter profile

SSH filter profile.

```
config ssh-filter profile
  Description: SSH filter profile.
  edit <name>
    set block {option1}, {option2}, ...
    set log {option1}, {option2}, ...
    set default-command-log [enable|disable]
  config shell-commands
    Description: SSH command filter.
    edit <id>
      set type [simple|regex]
      set pattern {string}
      set action [block|allow]
      set log [enable|disable]
      set alert [enable|disable]
      set severity [low|medium|...]
    next
  end
next
end
```

### config ssh-filter profile

Parameter	Description	Type	Size	Default														
block	SSH blocking options.	option	-															
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>x11</i></td><td>X server forwarding.</td></tr><tr><td><i>shell</i></td><td>SSH shell.</td></tr><tr><td><i>exec</i></td><td>SSH execution.</td></tr><tr><td><i>port-forward</i></td><td>Port forwarding.</td></tr><tr><td><i>tun-forward</i></td><td>Tunnel forwarding.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr></tbody></table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.			
Option	Description																	
<i>x11</i>	X server forwarding.																	
<i>shell</i>	SSH shell.																	
<i>exec</i>	SSH execution.																	
<i>port-forward</i>	Port forwarding.																	
<i>tun-forward</i>	Tunnel forwarding.																	
<i>sftp</i>	SFTP.																	



Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>scp</i></td> <td>SCP.</td> </tr> <tr> <td><i>unknown</i></td> <td>Unknown channel.</td> </tr> </tbody> </table>	Option	Description	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.															
Option	Description																					
<i>scp</i>	SCP.																					
<i>unknown</i>	Unknown channel.																					
log	SSH logging options.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>x11</i></td> <td>X server forwarding.</td> </tr> <tr> <td><i>shell</i></td> <td>SSH shell.</td> </tr> <tr> <td><i>exec</i></td> <td>SSH execution.</td> </tr> <tr> <td><i>port-forward</i></td> <td>Port forwarding.</td> </tr> <tr> <td><i>tun-forward</i></td> <td>Tunnel forwarding.</td> </tr> <tr> <td><i>sftp</i></td> <td>SFTP.</td> </tr> <tr> <td><i>scp</i></td> <td>SCP.</td> </tr> <tr> <td><i>unknown</i></td> <td>Unknown channel.</td> </tr> </tbody> </table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.			
Option	Description																					
<i>x11</i>	X server forwarding.																					
<i>shell</i>	SSH shell.																					
<i>exec</i>	SSH execution.																					
<i>port-forward</i>	Port forwarding.																					
<i>tun-forward</i>	Tunnel forwarding.																					
<i>sftp</i>	SFTP.																					
<i>scp</i>	SCP.																					
<i>unknown</i>	Unknown channel.																					
default-command-log	Enable/disable logging unmatched shell commands.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable log unmatched shell commands.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable log unmatched shell commands.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable log unmatched shell commands.	<i>disable</i>	Disable log unmatched shell commands.															
Option	Description																					
<i>enable</i>	Enable log unmatched shell commands.																					
<i>disable</i>	Disable log unmatched shell commands.																					

### config shell-commands

Parameter	Description	Type	Size	Default						
type	Matching type.	option	-	simple						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>simple</i></td> <td>Match single command.</td> </tr> <tr> <td><i>regex</i></td> <td>Match command line using regular expression.</td> </tr> </tbody> </table>	Option	Description	<i>simple</i>	Match single command.	<i>regex</i>	Match command line using regular expression.			
Option	Description									
<i>simple</i>	Match single command.									
<i>regex</i>	Match command line using regular expression.									
pattern	SSH shell command pattern.	string	Maximum length: 128							
action	Action to take for SSH shell command matches.	option	-	block						

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block the SSH shell command.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow the SSH shell command.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block the SSH shell command.	<i>allow</i>	Allow the SSH shell command.							
Option	Description													
<i>block</i>	Block the SSH shell command.													
<i>allow</i>	Allow the SSH shell command.													
log	Enable/disable logging.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.							
Option	Description													
<i>enable</i>	Enable logging.													
<i>disable</i>	Disable logging.													
alert	Enable/disable alert.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable alert.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable alert.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable alert.	<i>disable</i>	Disable alert.							
Option	Description													
<i>enable</i>	Enable alert.													
<i>disable</i>	Disable alert.													
severity	Log severity.	option	-	medium										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Severity low.</td> </tr> <tr> <td><i>medium</i></td> <td>Severity medium.</td> </tr> <tr> <td><i>high</i></td> <td>Severity high.</td> </tr> <tr> <td><i>critical</i></td> <td>Severity critical.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Severity low.	<i>medium</i>	Severity medium.	<i>high</i>	Severity high.	<i>critical</i>	Severity critical.			
Option	Description													
<i>low</i>	Severity low.													
<i>medium</i>	Severity medium.													
<i>high</i>	Severity high.													
<i>critical</i>	Severity critical.													

## switch-controller

This section includes syntax for the following commands:

- [config switch-controller storm-control-policy](#) on page 692
- [config switch-controller qos qos-policy](#) on page 691
- [config switch-controller vlan-policy](#) on page 752
- [config switch-controller flow-tracking](#) on page 741
- [config switch-controller snmp-community](#) on page 745
- [config switch-controller lldp-settings](#) on page 679
- [config switch-controller nac-device](#) on page 755
- [config switch-controller initial-config vlans](#) on page 697
- [config switch-controller managed-switch](#) on page 700
- [config switch-controller ptp policy](#) on page 699
- [config switch-controller sflow](#) on page 739
- [config switch-controller system](#) on page 736
- [config switch-controller nac-settings](#) on page 669
- [config switch-controller network-monitor-settings](#) on page 740
- [config switch-controller auto-config default](#) on page 694
- [config switch-controller security-policy 802-1X](#) on page 671
- [config switch-controller virtual-port-pool](#) on page 698
- [config switch-controller location](#) on page 675
- [config switch-controller mac-policy](#) on page 754
- [config switch-controller switch-log](#) on page 738
- [config switch-controller qos dot1p-map](#) on page 684
- [config switch-controller qos ip-dscp-map](#) on page 687
- [config switch-controller switch-interface-tag](#) on page 670
- [config switch-controller stp-settings](#) on page 731
- [config switch-controller global](#) on page 733
- [config switch-controller traffic-sniffer](#) on page 749
- [config switch-controller auto-config custom](#) on page 695
- [config switch-controller ptp settings](#) on page 699
- [config switch-controller security-policy local-access](#) on page 674
- [config switch-controller initial-config template](#) on page 695
- [config switch-controller switch-group](#) on page 731
- [config switch-controller lldp-profile](#) on page 680
- [config switch-controller port-policy](#) on page 753
- [config switch-controller snmp-trap-threshold](#) on page 744
- [config switch-controller qos queue-policy](#) on page 689
- [config switch-controller snmp-user](#) on page 747
- [config switch-controller custom-command](#) on page 698
- [config switch-controller 802-1X-settings](#) on page 671
- [config switch-controller igmp-snooping](#) on page 739

- [config switch-controller stp-instance](#) on page 732
- [config switch-controller traffic-policy](#) on page 668
- [config switch-controller remote-log](#) on page 750
- [config switch-controller switch-profile](#) on page 697
- [config switch-controller storm-control](#) on page 733
- [config switch-controller quarantine](#) on page 740
- [config switch-controller auto-config policy](#) on page 693
- [config switch-controller snmp-sysinfo](#) on page 743

## config switch-controller traffic-policy

Configure FortiSwitch traffic policy.

```
config switch-controller traffic-policy
  Description: Configure FortiSwitch traffic policy.
  edit <name>
    set description {string}
    set policer-status [enable|disable]
    set guaranteed-bandwidth {integer}
    set guaranteed-burst {integer}
    set maximum-burst {integer}
    set type [ingress|egress]
    set cos-queue {integer}
  next
end
```

## config switch-controller traffic-policy

Parameter	Description	Type	Size	Default						
description	Description of the traffic policy.	string	Maximum length: 63							
policer-status	Enable/disable policer config on the traffic policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable policer config on the traffic policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable policer config on the traffic policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable policer config on the traffic policy.	<i>disable</i>	Disable policer config on the traffic policy.			
Option	Description									
<i>enable</i>	Enable policer config on the traffic policy.									
<i>disable</i>	Disable policer config on the traffic policy.									
guaranteed-bandwidth	Guaranteed bandwidth in kbps (max value = 524287000).	integer	Minimum value: 0 Maximum value: 524287000	10000						

Parameter	Description	Type	Size	Default						
guaranteed-burst	Guaranteed burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	45000						
maximum-burst	Maximum burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	67500						
type	Configure type of policy(ingress/egress).	option	-	ingress						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ingress</i></td> <td>Ingress policy.</td> </tr> <tr> <td><i>egress</i></td> <td>Egress policy.</td> </tr> </tbody> </table>	Option	Description	<i>ingress</i>	Ingress policy.	<i>egress</i>	Egress policy.			
Option	Description									
<i>ingress</i>	Ingress policy.									
<i>egress</i>	Egress policy.									
cos-queue	COS queue, or unset to disable.	integer	Minimum value: 0 Maximum value: 7							

## config switch-controller nac-settings

Configure integrated NAC settings for FortiSwitch.

```

config switch-controller nac-settings
  Description: Configure integrated NAC settings for FortiSwitch.
  edit <name>
    set mode [local|global]
    set inactive-timer {integer}
    set onboarding-vlan {string}
    set auto-auth [disable|enable]
    set bounce-nac-port [disable|enable]
    set link-down-flush [disable|enable]
  next
end

```

## config switch-controller nac-settings

Parameter	Description	Type	Size	Default
mode	Set NAC mode to be used on the FortiSwitch ports.	option	-	local

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>local</i></td> <td>Local mode in which managed FortiSwitch port local settings is used.</td> </tr> <tr> <td><i>global</i></td> <td>Global mode which enables NAC on all the managed FortiSwitch ports.</td> </tr> </tbody> </table>	Option	Description	<i>local</i>	Local mode in which managed FortiSwitch port local settings is used.	<i>global</i>	Global mode which enables NAC on all the managed FortiSwitch ports.			
Option	Description									
<i>local</i>	Local mode in which managed FortiSwitch port local settings is used.									
<i>global</i>	Global mode which enables NAC on all the managed FortiSwitch ports.									
inactive-timer	Time interval(minutes, 0 = no expiry) to be included in the inactive NAC devices expiry calculation (mac age-out + inactive-time + periodic scan interval).	integer	Minimum value: 0 Maximum value: 1440	15						
onboarding-vlan	Default NAC Onboarding VLAN when NAC devices are discovered.	string	Maximum length: 15							
auto-auth	Enable/disable NAC device auto authorization when discovered and nac-policy matched.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable NAC device auto authorization.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable NAC device auto authorization.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable NAC device auto authorization.	<i>enable</i>	Enable NAC device auto authorization.			
Option	Description									
<i>disable</i>	Disable NAC device auto authorization.									
<i>enable</i>	Enable NAC device auto authorization.									
bounce-nac-port	Enable/disable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured on the port. Helps to re-initiate the DHCP process for a device.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.			
Option	Description									
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.									
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.									
link-down-flush	Clear NAC devices on switch ports on link down event.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable clearing NAC devices on a switch port when link down event happens.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable clearing NAC devices on a switch port when link down event happens.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable clearing NAC devices on a switch port when link down event happens.	<i>enable</i>	Enable clearing NAC devices on a switch port when link down event happens.			
Option	Description									
<i>disable</i>	Disable clearing NAC devices on a switch port when link down event happens.									
<i>enable</i>	Enable clearing NAC devices on a switch port when link down event happens.									

## config switch-controller switch-interface-tag

Configure switch object tags.

```
config switch-controller switch-interface-tag
  Description: Configure switch object tags.
  edit <name>
```

```
next
end
```

## config switch-controller 802-1X-settings

Configure global 802.1X settings.

```
config switch-controller 802-1X-settings
  Description: Configure global 802.1X settings.
  set link-down-auth [set-unauth|no-action]
  set reauth-period {integer}
  set max-reauth-attempt {integer}
  set tx-period {integer}
end
```

## config switch-controller 802-1X-settings

Parameter	Description	Type	Size	Default						
link-down-auth	Interface-reauthentication state to set if a link is down.	option	-	set-unauth						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>set-unauth</i></td><td>Interface set to unauth when down. Reauthentication is needed.</td></tr><tr><td><i>no-action</i></td><td>Interface reauthentication is not needed.</td></tr></tbody></table>	Option	Description	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.	<i>no-action</i>	Interface reauthentication is not needed.			
Option	Description									
<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.									
<i>no-action</i>	Interface reauthentication is not needed.									
reauth-period	Period of time to allow for reauthentication .	integer	Minimum value: 0 Maximum value: 1440	60						
max-reauth-attempt	Maximum number of authentication attempts .	integer	Minimum value: 0 Maximum value: 15	3						
tx-period	802.1X Tx period .	integer	Minimum value: 4 Maximum value: 60	30						

## config switch-controller security-policy 802-1X

Configure 802.1x MAC Authentication Bypass (MAB) policies.

```
config switch-controller security-policy 802-1X
  Description: Configure 802.1x MAC Authentication Bypass (MAB) policies.
  edit <name>
    set security-mode [802.1X|802.1X-mac-based]
    set user-group <name1>, <name2>, ...
```

```

set mac-auth-bypass [disable|enable]
set open-auth [disable|enable]
set eap-passthru [disable|enable]
set eap-auto-untagged-vlans [disable|enable]
set guest-vlan [disable|enable]
set guest-vlan-id {string}
set guest-auth-delay {integer}
set auth-fail-vlan [disable|enable]
set auth-fail-vlan-id {string}
set framevid-apply [disable|enable]
set radius-timeout-overwrite [disable|enable]
set policy-type {option}
set authserver-timeout-period {integer}
set authserver-timeout-vlan [disable|enable]
set authserver-timeout-vlanid {string}
next
end

```

## config switch-controller security-policy 802-1X

Parameter	Description	Type	Size	Default						
security-mode	Port or MAC based 802.1X security mode.	option	-	802.1X						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.1X</i></td> <td>802.1X port based authentication.</td> </tr> <tr> <td><i>802.1X-mac-based</i></td> <td>802.1X MAC based authentication.</td> </tr> </tbody> </table>	Option	Description	<i>802.1X</i>	802.1X port based authentication.	<i>802.1X-mac-based</i>	802.1X MAC based authentication.			
Option	Description									
<i>802.1X</i>	802.1X port based authentication.									
<i>802.1X-mac-based</i>	802.1X MAC based authentication.									
user-group <name>	Name of user-group to assign to this MAC Authentication Bypass (MAB) policy. Group name.	string	Maximum length: 79							
mac-auth-bypass	Enable/disable MAB for this policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable MAB.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable MAB.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable MAB.	<i>enable</i>	Enable MAB.			
Option	Description									
<i>disable</i>	Disable MAB.									
<i>enable</i>	Enable MAB.									
open-auth	Enable/disable open authentication for this policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable open authentication.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable open authentication.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable open authentication.	<i>enable</i>	Enable open authentication.			
Option	Description									
<i>disable</i>	Disable open authentication.									
<i>enable</i>	Enable open authentication.									



Parameter	Description	Type	Size	Default						
eap-passthru	Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for more flexible authentication.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable EAP pass-through mode on this interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable EAP pass-through mode on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable EAP pass-through mode on this interface.	<i>enable</i>	Enable EAP pass-through mode on this interface.			
Option	Description									
<i>disable</i>	Disable EAP pass-through mode on this interface.									
<i>enable</i>	Enable EAP pass-through mode on this interface.									
eap-auto-untagged-vlans	Enable/disable automatic inclusion of untagged VLANs.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable automatic inclusion of untagged VLANs.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable automatic inclusion of untagged VLANs.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable automatic inclusion of untagged VLANs.	<i>enable</i>	Enable automatic inclusion of untagged VLANs.			
Option	Description									
<i>disable</i>	Disable automatic inclusion of untagged VLANs.									
<i>enable</i>	Enable automatic inclusion of untagged VLANs.									
guest-vlan	Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable guest VLAN on this interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable guest VLAN on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable guest VLAN on this interface.	<i>enable</i>	Enable guest VLAN on this interface.			
Option	Description									
<i>disable</i>	Disable guest VLAN on this interface.									
<i>enable</i>	Enable guest VLAN on this interface.									
guest-vlan-id	Guest VLAN name.	string	Maximum length: 15							
guest-auth-delay	Guest authentication delay .	integer	Minimum value: 1 Maximum value: 900	30						
auth-fail-vlan	Enable to allow limited access to clients that cannot authenticate.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable authentication fail VLAN on this interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable authentication fail VLAN on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable authentication fail VLAN on this interface.	<i>enable</i>	Enable authentication fail VLAN on this interface.			
Option	Description									
<i>disable</i>	Disable authentication fail VLAN on this interface.									
<i>enable</i>	Enable authentication fail VLAN on this interface.									
auth-fail-vlan-id	VLAN ID on which authentication failed.	string	Maximum length: 15							
framevid-apply	Enable/disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.			
Option	Description									
<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.									
<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.									
radius-timeout-overwrite	Enable to override the global RADIUS session timeout.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Override the global RADIUS session timeout.</td> </tr> <tr> <td><i>enable</i></td> <td>Use the global RADIUS session timeout.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Override the global RADIUS session timeout.	<i>enable</i>	Use the global RADIUS session timeout.			
Option	Description									
<i>disable</i>	Override the global RADIUS session timeout.									
<i>enable</i>	Use the global RADIUS session timeout.									
policy-type	Policy type.	option	-	802.1X						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.1X</i></td> <td>802.1X security policy.</td> </tr> </tbody> </table>	Option	Description	<i>802.1X</i>	802.1X security policy.					
Option	Description									
<i>802.1X</i>	802.1X security policy.									
authserver-timeout-period	Authentication server timeout period .	integer	Minimum value: 3 Maximum value: 15	3						
authserver-timeout-vlan	Enable/disable the authentication server timeout VLAN to allow limited access when RADIUS is unavailable.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable authentication server timeout VLAN on this interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable authentication server timeout VLAN on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable authentication server timeout VLAN on this interface.	<i>enable</i>	Enable authentication server timeout VLAN on this interface.			
Option	Description									
<i>disable</i>	Disable authentication server timeout VLAN on this interface.									
<i>enable</i>	Enable authentication server timeout VLAN on this interface.									
authserver-timeout-vlanid	Authentication server timeout VLAN name.	string	Maximum length: 15							

## config switch-controller security-policy local-access

Configure allowaccess list for mgmt and internal interfaces on managed FortiSwitch.

```

config switch-controller security-policy local-access
  Description: Configure allowaccess list for mgmt and internal interfaces on managed
  FortiSwitch.
  edit <name>
    set mgmt-allowaccess {option1}, {option2}, ...
    set internal-allowaccess {option1}, {option2}, ...
  next
end

```

## config switch-controller security-policy local-access

Parameter	Description	Type	Size	Default																
mgmt-allowaccess	Allowed access on the switch management interface.	option	-	https ping ssh																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>radius-acct</i></td> <td>RADIUS accounting access.</td> </tr> </tbody> </table>	Option	Description	<i>https</i>	HTTPS access.	<i>ping</i>	PING access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>radius-acct</i>	RADIUS accounting access.			
Option	Description																			
<i>https</i>	HTTPS access.																			
<i>ping</i>	PING access.																			
<i>ssh</i>	SSH access.																			
<i>snmp</i>	SNMP access.																			
<i>http</i>	HTTP access.																			
<i>telnet</i>	TELNET access.																			
<i>radius-acct</i>	RADIUS accounting access.																			
internal-allowaccess	Allowed access on the switch internal interface.	option	-	https ping ssh																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>radius-acct</i></td> <td>RADIUS accounting access.</td> </tr> </tbody> </table>	Option	Description	<i>https</i>	HTTPS access.	<i>ping</i>	PING access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>radius-acct</i>	RADIUS accounting access.			
Option	Description																			
<i>https</i>	HTTPS access.																			
<i>ping</i>	PING access.																			
<i>ssh</i>	SSH access.																			
<i>snmp</i>	SNMP access.																			
<i>http</i>	HTTP access.																			
<i>telnet</i>	TELNET access.																			
<i>radius-acct</i>	RADIUS accounting access.																			

## config switch-controller location

Configure FortiSwitch location services.

```

config switch-controller location
  Description: Configure FortiSwitch location services.
  edit <name>
    config address-civic
      Description: Configure location civic address.
      set additional {string}
      set additional-code {string}
      set block {string}
      set branch-road {string}
      set building {string}
      set city {string}
    
```

```

set city-division {string}
set country {string}
set country-subdivision {string}
set county {string}
set direction {string}
set floor {string}
set landmark {string}
set language {string}
set name {string}
set number {string}
set number-suffix {string}
set place-type {string}
set post-office-box {string}
set postal-community {string}
set primary-road {string}
set road-section {string}
set room {string}
set script {string}
set seat {string}
set street {string}
set street-name-post-mod {string}
set street-name-pre-mod {string}
set street-suffix {string}
set sub-branch-road {string}
set trailing-str-suffix {string}
set unit {string}
set zip {string}
set parent-key {string}
end
config coordinates
  Description: Configure location GPS coordinates.
  set altitude {string}
  set altitude-unit [m|f]
  set datum [WGS84|NAD83|...]
  set latitude {string}
  set longitude {string}
  set parent-key {string}
end
config elin-number
  Description: Configure location ELIN number.
  set elin-num {string}
  set parent-key {string}
end
next
end

```

### config address-civic

Parameter	Description	Type	Size	Default
additional	Location additional details.	string	Maximum length: 47	
additional-code	Location additional code details.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
block	Location block details.	string	Maximum length: 47	
branch-road	Location branch road details.	string	Maximum length: 47	
building	Location building details.	string	Maximum length: 47	
city	Location city details.	string	Maximum length: 47	
city-division	Location city division details.	string	Maximum length: 47	
country	The two-letter ISO 3166 country code in capital ASCII letters eg. US, CA, DK, DE.	string	Maximum length: 47	
country-subdivision	National subdivisions (state, canton, region, province, or prefecture).	string	Maximum length: 47	
county	County, parish, gun (JP), or district (IN).	string	Maximum length: 47	
direction	Leading street direction.	string	Maximum length: 47	
floor	Floor.	string	Maximum length: 47	
landmark	Landmark or vanity address.	string	Maximum length: 47	
language	Language.	string	Maximum length: 47	
name	Name (residence and office occupant).	string	Maximum length: 47	
number	House number.	string	Maximum length: 47	
number-suffix	House number suffix.	string	Maximum length: 47	
place-type	Placetype.	string	Maximum length: 47	
post-office-box	Post office box (P.O. box).	string	Maximum length: 47	
postal-community	Postal community name.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
primary-road	Primary road name.	string	Maximum length: 47	
road-section	Road section.	string	Maximum length: 47	
room	Room number.	string	Maximum length: 47	
script	Script used to present the address information.	string	Maximum length: 47	
seat	Seat number.	string	Maximum length: 47	
street	Street.	string	Maximum length: 47	
street-name-post-mod	Street name post modifier.	string	Maximum length: 47	
street-name-pre-mod	Street name pre modifier.	string	Maximum length: 47	
street-suffix	Street suffix.	string	Maximum length: 47	
sub-branch-road	Sub branch road name.	string	Maximum length: 47	
trailing-str-suffix	Trailing street suffix.	string	Maximum length: 47	
unit	Unit (apartment, suite).	string	Maximum length: 47	
zip	Postal/zip code.	string	Maximum length: 47	
parent-key	Parent key name.	string	Maximum length: 63	

### config coordinates

Parameter	Description	Type	Size	Default
altitude	+/- Floating point no. eg. 117.47.	string	Maximum length: 15	
altitude-unit	m ( meters), f ( floors).	option	-	m
	<b>Option</b>	<b>Description</b>		
	<i>m</i>	set altitude unit meters		

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>f</i></td> <td>set altitude unit floors</td> </tr> </tbody> </table>	Option	Description	<i>f</i>	set altitude unit floors							
Option	Description											
<i>f</i>	set altitude unit floors											
datum	WGS84, NAD83, NAD83/MLLW.	option	-	WGS84								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>WGS84</i></td> <td>set coordinates datum WGS84</td> </tr> <tr> <td><i>NAD83</i></td> <td>set coordinates datum NAD83</td> </tr> <tr> <td><i>NAD83/MLLW</i></td> <td>set coordinates datum NAD83/MLLW</td> </tr> </tbody> </table>	Option	Description	<i>WGS84</i>	set coordinates datum WGS84	<i>NAD83</i>	set coordinates datum NAD83	<i>NAD83/MLLW</i>	set coordinates datum NAD83/MLLW			
Option	Description											
<i>WGS84</i>	set coordinates datum WGS84											
<i>NAD83</i>	set coordinates datum NAD83											
<i>NAD83/MLLW</i>	set coordinates datum NAD83/MLLW											
latitude	Floating point start with ( +/- ) or end with ( N or S ) eg. +/-16.67 or 16.67N.	string	Maximum length: 15									
longitude	Floating point start with ( +/- ) or end with ( E or W ) eg. +/-26.789 or 26.789E.	string	Maximum length: 15									
parent-key	Parent key name.	string	Maximum length: 63									

### config elin-number

Parameter	Description	Type	Size	Default
elin-num	Configure ELIN callback number.	string	Maximum length: 31	
parent-key	Parent key name.	string	Maximum length: 63	

### config switch-controller lldp-settings

Configure FortiSwitch LLDP settings.

```

config switch-controller lldp-settings
  Description: Configure FortiSwitch LLDP settings.
  set tx-hold {integer}
  set tx-interval {integer}
  set fast-start-interval {integer}
  set management-interface [internal|mgmt]
  set device-detection [disable|enable]
end

```

## config switch-controller lldp-settings

Parameter	Description	Type	Size	Default						
tx-hold	Number of tx-intervals before local LLDP data expires . Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 1 Maximum value: 16	4						
tx-interval	Frequency of LLDP PDU transmission from FortiSwitch . Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 5 Maximum value: 4095	30						
fast-start-interval	Frequency of LLDP PDU transmission from FortiSwitch for the first 4 packets when the link is up .	integer	Minimum value: 0 Maximum value: 255	2						
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	option	-	internal						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>internal</i></td> <td>Use internal interface.</td> </tr> <tr> <td><i>mgmt</i></td> <td>Use management interface.</td> </tr> </tbody> </table>	Option	Description	<i>internal</i>	Use internal interface.	<i>mgmt</i>	Use management interface.			
Option	Description									
<i>internal</i>	Use internal interface.									
<i>mgmt</i>	Use management interface.									
device-detection	Enable/disable dynamic detection of LLDP neighbor devices for VLAN assignment.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dynamic detection of LLDP neighbor devices.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dynamic detection of LLDP neighbor devices.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dynamic detection of LLDP neighbor devices.	<i>enable</i>	Enable dynamic detection of LLDP neighbor devices.			
Option	Description									
<i>disable</i>	Disable dynamic detection of LLDP neighbor devices.									
<i>enable</i>	Enable dynamic detection of LLDP neighbor devices.									

## config switch-controller lldp-profile

Configure FortiSwitch LLDP profiles.

```
config switch-controller lldp-profile
  Description: Configure FortiSwitch LLDP profiles.
  edit <name>
    set med-tlvs {option1}, {option2}, ...
    set 802 1-tlvs {option1}, {option2}, ...
    set 802 3-tlvs {option1}, {option2}, ...
    set auto-isl [disable|enable]
    set auto-isl-hello-timer {integer}
    set auto-isl-receive-timeout {integer}
    set auto-isl-port-group {integer}
    set auto-mclag-icl [disable|enable]
  config med-network-policy
```



```

Description: Configuration method to edit Media Endpoint Discovery (MED) network
policy type-length-value (TLV) categories.
edit <name>
  set status [disable|enable]
  set vlan-intf {string}
  set assign-vlan [disable|enable]
  set priority {integer}
  set dscp {integer}
next
end
config med-location-service
Description: Configuration method to edit Media Endpoint Discovery (MED) location
service type-length-value (TLV) categories.
edit <name>
  set status [disable|enable]
  set sys-location-id {string}
next
end
config custom-tlvs
Description: Configuration method to edit custom TLV entries.
edit <name>
  set oui {user}
  set subtype {integer}
  set information-string {user}
next
end
next
end

```

## config switch-controller lldp-profile

Parameter	Description	Type	Size	Default										
med-tlvs	Transmitted LLDP-MED TLVs (type-length-value descriptions).	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>inventory-management</i></td> <td>Inventory management TLVs.</td> </tr> <tr> <td><i>network-policy</i></td> <td>Network policy TLVs.</td> </tr> <tr> <td><i>power-management</i></td> <td>Power management TLVs.</td> </tr> <tr> <td><i>location-identification</i></td> <td>Location identification TLVs.</td> </tr> </tbody> </table>	Option	Description	<i>inventory-management</i>	Inventory management TLVs.	<i>network-policy</i>	Network policy TLVs.	<i>power-management</i>	Power management TLVs.	<i>location-identification</i>	Location identification TLVs.			
Option	Description													
<i>inventory-management</i>	Inventory management TLVs.													
<i>network-policy</i>	Network policy TLVs.													
<i>power-management</i>	Power management TLVs.													
<i>location-identification</i>	Location identification TLVs.													
802 1-tlvs	Transmitted IEEE 802.1 TLVs.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>port-vlan-id</i></td> <td>Port native VLAN TLV.</td> </tr> </tbody> </table>	Option	Description	<i>port-vlan-id</i>	Port native VLAN TLV.									
Option	Description													
<i>port-vlan-id</i>	Port native VLAN TLV.													

Parameter	Description	Type	Size	Default						
802 3-tlvs	Transmitted IEEE 802.3 TLVs.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>max-frame-size</i></td> <td>Maximum frame size TLV.</td> </tr> <tr> <td><i>power-negotiation</i></td> <td>PoE+ classification TLV.</td> </tr> </tbody> </table>	Option	Description	<i>max-frame-size</i>	Maximum frame size TLV.	<i>power-negotiation</i>	PoE+ classification TLV.			
Option	Description									
<i>max-frame-size</i>	Maximum frame size TLV.									
<i>power-negotiation</i>	PoE+ classification TLV.									
auto-isl	Enable/disable auto inter-switch LAG.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable automatic MCLAG inter chassis link.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable automatic MCLAG inter chassis link.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable automatic MCLAG inter chassis link.	<i>enable</i>	Enable automatic MCLAG inter chassis link.			
Option	Description									
<i>disable</i>	Disable automatic MCLAG inter chassis link.									
<i>enable</i>	Enable automatic MCLAG inter chassis link.									
auto-isl-hello-timer	Auto inter-switch LAG hello timer duration .	integer	Minimum value: 1 Maximum value: 30	3						
auto-isl-receive-timeout	Auto inter-switch LAG timeout if no response is received .	integer	Minimum value: 0 Maximum value: 90	60						
auto-isl-port-group	Auto inter-switch LAG port group ID .	integer	Minimum value: 0 Maximum value: 9	0						
auto-mclag-icl	Enable/disable MCLAG inter chassis link.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable auto inter-switch-LAG.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable auto inter-switch-LAG.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable auto inter-switch-LAG.	<i>enable</i>	Enable auto inter-switch-LAG.			
Option	Description									
<i>disable</i>	Disable auto inter-switch-LAG.									
<i>enable</i>	Enable auto inter-switch-LAG.									

### config med-network-policy

Parameter	Description	Type	Size	Default						
status	Enable or disable this TLV.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not transmit this network policy TLV.</td> </tr> <tr> <td><i>enable</i></td> <td>Transmit this TLV if a VLAN has been added to the port.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not transmit this network policy TLV.	<i>enable</i>	Transmit this TLV if a VLAN has been added to the port.			
Option	Description									
<i>disable</i>	Do not transmit this network policy TLV.									
<i>enable</i>	Transmit this TLV if a VLAN has been added to the port.									

Parameter	Description	Type	Size	Default						
vlan-intf	VLAN interface to advertise; if configured on port.	string	Maximum length: 15							
assign-vlan	Enable/disable VLAN assignment when this profile is applied on managed FortiSwitch port.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable VLAN assignment when this profile is applied on port.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable VLAN assignment when this profile is applied on port.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable VLAN assignment when this profile is applied on port.	<i>enable</i>	Enable VLAN assignment when this profile is applied on port.			
Option	Description									
<i>disable</i>	Disable VLAN assignment when this profile is applied on port.									
<i>enable</i>	Enable VLAN assignment when this profile is applied on port.									
priority	Advertised Layer 2 priority .	integer	Minimum value: 0 Maximum value: 7	0						
dscp	Advertised Differentiated Services Code Point (DSCP) value, a packet header value indicating the level of service requested for traffic, such as high priority or best effort delivery.	integer	Minimum value: 0 Maximum value: 63	0						

### config med-location-service

Parameter	Description	Type	Size	Default						
status	Enable or disable this TLV.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not transmit this location service TLV.</td> </tr> <tr> <td><i>enable</i></td> <td>Transmit this location service TLV.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not transmit this location service TLV.	<i>enable</i>	Transmit this location service TLV.			
Option	Description									
<i>disable</i>	Do not transmit this location service TLV.									
<i>enable</i>	Transmit this location service TLV.									
sys-location-id	Location service ID.	string	Maximum length: 63							

### config custom-tlvs

Parameter	Description	Type	Size	Default
oui	Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.	user	Not Specified	000000
subtype	Organizationally defined subtype .	integer	Minimum value: 0 Maximum value: 255	0
information-string	Organizationally defined information string .	user	Not Specified	

## config switch-controller qos dot1p-map

Configure FortiSwitch QoS 802.1p.

```
config switch-controller qos dot1p-map
  Description: Configure FortiSwitch QoS 802.1p.
  edit <name>
    set description {string}
    set egress-pri-tagging [disable|enable]
    set priority-0 [queue-0|queue-1|...]
    set priority-1 [queue-0|queue-1|...]
    set priority-2 [queue-0|queue-1|...]
    set priority-3 [queue-0|queue-1|...]
    set priority-4 [queue-0|queue-1|...]
    set priority-5 [queue-0|queue-1|...]
    set priority-6 [queue-0|queue-1|...]
    set priority-7 [queue-0|queue-1|...]
  next
end
```

## config switch-controller qos dot1p-map

Parameter	Description	Type	Size	Default																		
description	Description of the 802.1p name.	string	Maximum length: 63																			
egress-pri-tagging	Enable/disable egress priority-tag frame.	option	-	disable																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable egress priority tagging.</td></tr><tr><td><i>enable</i></td><td>Enable egress priority tagging.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable egress priority tagging.	<i>enable</i>	Enable egress priority tagging.															
Option	Description																					
<i>disable</i>	Disable egress priority tagging.																					
<i>enable</i>	Enable egress priority tagging.																					
priority-0	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>queue-0</i></td><td>COS queue 0 (lowest priority).</td></tr><tr><td><i>queue-1</i></td><td>COS queue 1.</td></tr><tr><td><i>queue-2</i></td><td>COS queue 2.</td></tr><tr><td><i>queue-3</i></td><td>COS queue 3.</td></tr><tr><td><i>queue-4</i></td><td>COS queue 4.</td></tr><tr><td><i>queue-5</i></td><td>COS queue 5.</td></tr><tr><td><i>queue-6</i></td><td>COS queue 6.</td></tr><tr><td><i>queue-7</i></td><td>COS queue 7 (highest priority).</td></tr></tbody></table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).			
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					

Parameter	Description	Type	Size	Default																		
priority-1	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).			
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-2	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).			
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-3	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.					
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-7</i>	COS queue 7 (highest priority).																	
Option	Description																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-4	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).			
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-5	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).			
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-6	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.											
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).											
Option	Description																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-7	COS queue mapped to dot1p priority number.	option	-	queue-0																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>queue-0</i></td> <td>COS queue 0 (lowest priority).</td> </tr> <tr> <td><i>queue-1</i></td> <td>COS queue 1.</td> </tr> <tr> <td><i>queue-2</i></td> <td>COS queue 2.</td> </tr> <tr> <td><i>queue-3</i></td> <td>COS queue 3.</td> </tr> <tr> <td><i>queue-4</i></td> <td>COS queue 4.</td> </tr> <tr> <td><i>queue-5</i></td> <td>COS queue 5.</td> </tr> <tr> <td><i>queue-6</i></td> <td>COS queue 6.</td> </tr> <tr> <td><i>queue-7</i></td> <td>COS queue 7 (highest priority).</td> </tr> </tbody> </table>	Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).			
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					

## config switch-controller qos ip-dscp-map

Configure FortiSwitch QoS IP precedence/DSCP.

```

config switch-controller qos ip-dscp-map
  Description: Configure FortiSwitch QoS IP precedence/DSCP.
  edit <name>
    set description {string}
    config map
      Description: Maps between IP-DSCP value to COS queue.
      edit <name>
        set cos-queue {integer}
        set diffserv {option1}, {option2}, ...
        set ip-precedence {option1}, {option2}, ...
        set value {user}
      next
    end
  next
end

```

## config switch-controller qos ip-dscp-map

Parameter	Description	Type	Size	Default
description	Description of the ip-dscp map name.	string	Maximum length: 63	

## config map

Parameter	Description	Type	Size	Default
cos-queue	COS queue number.	integer	Minimum value: 0 Maximum value: 7	0
diffserv	Differentiated service.	option	-	

Option	Description
CS0	DSCP CS0.
CS1	DSCP CS1.
AF11	DSCP AF11.
AF12	DSCP AF12.
AF13	DSCP AF13.
CS2	DSCP CS2.
AF21	DSCP AF21.
AF22	DSCP AF22.
AF23	DSCP AF23.
CS3	DSCP CS3.
AF31	DSCP AF31.
AF32	DSCP AF32.
AF33	DSCP AF33.
CS4	DSCP CS4.
AF41	DSCP AF41.
AF42	DSCP AF42.
AF43	DSCP AF43.
CS5	DSCP CS5.
EF	DSCP EF.



Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CS6</td> <td>DSCP CS6.</td> </tr> <tr> <td>CS7</td> <td>DSCP CS7.</td> </tr> </tbody> </table>	Option	Description	CS6	DSCP CS6.	CS7	DSCP CS7.															
Option	Description																					
CS6	DSCP CS6.																					
CS7	DSCP CS7.																					
ip-precedence	IP Precedence.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>network-control</i></td> <td>Network control.</td> </tr> <tr> <td><i>internetwork-control</i></td> <td>Internetwork control.</td> </tr> <tr> <td><i>critic-ecp</i></td> <td>Critic ECP.</td> </tr> <tr> <td><i>flashoverride</i></td> <td>Flash override.</td> </tr> <tr> <td><i>flash</i></td> <td>Flash.</td> </tr> <tr> <td><i>immediate</i></td> <td>Immediate.</td> </tr> <tr> <td><i>priority</i></td> <td>Priority.</td> </tr> <tr> <td><i>routine</i></td> <td>Routine.</td> </tr> </tbody> </table>	Option	Description	<i>network-control</i>	Network control.	<i>internetwork-control</i>	Internetwork control.	<i>critic-ecp</i>	Critic ECP.	<i>flashoverride</i>	Flash override.	<i>flash</i>	Flash.	<i>immediate</i>	Immediate.	<i>priority</i>	Priority.	<i>routine</i>	Routine.			
Option	Description																					
<i>network-control</i>	Network control.																					
<i>internetwork-control</i>	Internetwork control.																					
<i>critic-ecp</i>	Critic ECP.																					
<i>flashoverride</i>	Flash override.																					
<i>flash</i>	Flash.																					
<i>immediate</i>	Immediate.																					
<i>priority</i>	Priority.																					
<i>routine</i>	Routine.																					
value	Raw values of DSCP .	user	Not Specified																			

## config switch-controller qos queue-policy

Configure FortiSwitch QoS egress queue policy.

```

config switch-controller qos queue-policy
  Description: Configure FortiSwitch QoS egress queue policy.
  edit <name>
    set schedule [strict|round-robin|...]
    set rate-by [kbps|percent]
    config cos-queue
      Description: COS queue configuration.
      edit <name>
        set description {string}
        set min-rate {integer}
        set max-rate {integer}
        set min-rate-percent {integer}
        set max-rate-percent {integer}
        set drop-policy [taildrop|weighted-random-early-detection]
        set ecn [disable|enable]
        set weight {integer}
      next
    end
  next
end

```

## config switch-controller qos queue-policy

Parameter	Description	Type	Size	Default								
schedule	COS queue scheduling.	option	-	round-robin								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>strict</i></td> <td>Strict scheduling (queue7: highest priority, queue0: lowest priority).</td> </tr> <tr> <td><i>round-robin</i></td> <td>Round robin scheduling.</td> </tr> <tr> <td><i>weighted</i></td> <td>Weighted round robin scheduling.</td> </tr> </tbody> </table>	Option	Description	<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).	<i>round-robin</i>	Round robin scheduling.	<i>weighted</i>	Weighted round robin scheduling.			
Option	Description											
<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).											
<i>round-robin</i>	Round robin scheduling.											
<i>weighted</i>	Weighted round robin scheduling.											
rate-by	COS queue rate by kbps or percent.	option	-	kbps								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kbps</i></td> <td>Rate by kbps.</td> </tr> <tr> <td><i>percent</i></td> <td>Rate by percent.</td> </tr> </tbody> </table>	Option	Description	<i>kbps</i>	Rate by kbps.	<i>percent</i>	Rate by percent.					
Option	Description											
<i>kbps</i>	Rate by kbps.											
<i>percent</i>	Rate by percent.											

## config cos-queue

Parameter	Description	Type	Size	Default
description	Description of the COS queue.	string	Maximum length: 63	
min-rate	Minimum rate .	integer	Minimum value: 0 Maximum value: 4294967295	0
max-rate	Maximum rate .	integer	Minimum value: 0 Maximum value: 4294967295	0
min-rate-percent	Minimum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-rate-percent	Maximum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
drop-policy	COS queue drop policy.	option	-	taildrop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>taildrop</i></td> <td>Taildrop policy.</td> </tr> <tr> <td><i>weighted-random-early-detection</i></td> <td>Weighted random early detection drop policy.</td> </tr> </tbody> </table>	Option	Description	<i>taildrop</i>	Taildrop policy.	<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.			
Option	Description									
<i>taildrop</i>	Taildrop policy.									
<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.									
ecn	Enable/disable ECN packet marking to drop eligible packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable ECN packet marking to drop eligible packets.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable ECN packet marking to drop eligible packets.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable ECN packet marking to drop eligible packets.	<i>enable</i>	Enable ECN packet marking to drop eligible packets.			
Option	Description									
<i>disable</i>	Disable ECN packet marking to drop eligible packets.									
<i>enable</i>	Enable ECN packet marking to drop eligible packets.									
weight	Weight of weighted round robin scheduling.	integer	Minimum value: 0 Maximum value: 4294967295	1						

## config switch-controller qos qos-policy

Configure FortiSwitch QoS policy.

```
config switch-controller qos qos-policy
  Description: Configure FortiSwitch QoS policy.
  edit <name>
    set default-cos {integer}
    set trust-dot1p-map {string}
    set trust-ip-dscp-map {string}
    set queue-policy {string}
  next
end
```

## config switch-controller qos qos-policy

Parameter	Description	Type	Size	Default
default-cos	Default cos queue for untagged packets.	integer	Minimum value: 0 Maximum value: 7	0

Parameter	Description	Type	Size	Default
trust-dot1p-map	QoS trust 802.1p map.	string	Maximum length: 63	
trust-ip-dscp-map	QoS trust ip dscp map.	string	Maximum length: 63	
queue-policy	QoS egress queue policy.	string	Maximum length: 63	default

## config switch-controller storm-control-policy

Configure FortiSwitch storm control policy to be applied on managed-switch ports.

```
config switch-controller storm-control-policy
  Description: Configure FortiSwitch storm control policy to be applied on managed-switch ports.
  edit <name>
    set description {string}
    set storm-control-mode [global|override|...]
    set rate {integer}
    set unknown-unicast [enable|disable]
    set unknown-multicast [enable|disable]
    set broadcast [enable|disable]
  next
end
```

## config switch-controller storm-control-policy

Parameter	Description	Type	Size	Default								
description	Description of the storm control policy.	string	Maximum length: 63									
storm-control-mode	Set Storm control mode.	option	-	global								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Apply Global or switch level storm control configuration.</td> </tr> <tr> <td><i>override</i></td> <td>Override global and switch level storm control to use port level configuration.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disable storm control on the port entirely overriding global and switch level storm control.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Apply Global or switch level storm control configuration.	<i>override</i>	Override global and switch level storm control to use port level configuration.	<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.			
Option	Description											
<i>global</i>	Apply Global or switch level storm control configuration.											
<i>override</i>	Override global and switch level storm control to use port level configuration.											
<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.											
rate	Threshold rate in packets per second at which storm traffic is controlled in override mode .	integer	Minimum value: 0 Maximum value: 10000000	500								

Parameter	Description	Type	Size	Default						
unknown-unicast	Enable/disable storm control to drop/allow unknown unicast traffic in override mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable storm control for unknown unicast traffic to allow all packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.			
Option	Description									
<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.									
<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.									
unknown-multicast	Enable/disable storm control to drop/allow unknown multicast traffic in override mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable storm control for unknown multicast traffic to allow all packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.			
Option	Description									
<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.									
<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.									
broadcast	Enable/disable storm control to drop/allow broadcast traffic in override mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable storm control for broadcast traffic to allow all packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.			
Option	Description									
<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.									
<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.									

## config switch-controller auto-config policy

Policy definitions which can define the behavior on auto configured interfaces.

```

config switch-controller auto-config policy
  Description: Policy definitions which can define the behavior on auto configured
              interfaces.
  edit <name>
    set qos-policy {string}
    set storm-control-policy {string}
    set poe-status [enable|disable]
    set igmp-flood-report [enable|disable]
    set igmp-flood-traffic [enable|disable]
  next
end

```

## config switch-controller auto-config policy

Parameter	Description	Type	Size	Default						
qos-policy	Auto-Config QoS policy.	string	Maximum length: 63	default						
storm-control-policy	Auto-Config storm control policy.	string	Maximum length: 63	auto-config						
poE-status	Enable/disable PoE status.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable PoE status.</td></tr><tr><td><i>disable</i></td><td>Disable PoE status.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.			
Option	Description									
<i>enable</i>	Enable PoE status.									
<i>disable</i>	Disable PoE status.									
igmp-flood-report	Enable/disable IGMP flood report.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable IGMP flood report.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP flood report.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable IGMP flood report.	<i>disable</i>	Disable IGMP flood report.			
Option	Description									
<i>enable</i>	Enable IGMP flood report.									
<i>disable</i>	Disable IGMP flood report.									
igmp-flood-traffic	Enable/disable IGMP flood traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable IGMP flood traffic.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP flood traffic.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable IGMP flood traffic.	<i>disable</i>	Disable IGMP flood traffic.			
Option	Description									
<i>enable</i>	Enable IGMP flood traffic.									
<i>disable</i>	Disable IGMP flood traffic.									

## config switch-controller auto-config default

Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.

```
config switch-controller auto-config default
  Description: Policies which are applied automatically to all ISL/ICL/FortiLink
  interfaces.
  set fgt-policy {string}
  set isl-policy {string}
  set icl-policy {string}
end
```

## config switch-controller auto-config default

Parameter	Description	Type	Size	Default
fgt-policy	Default FortiLink auto-config policy.	string	Maximum length: 63	default
isl-policy	Default ISL auto-config policy.	string	Maximum length: 63	default
icl-policy	Default ICL auto-config policy.	string	Maximum length: 63	default-icl

## config switch-controller auto-config custom

Policies which can override the 'default' for specific ISL/ICL/FortiLink interface.

```
config switch-controller auto-config custom
  Description: Policies which can override the 'default' for specific ISL/ICL/FortiLink
  interface.
  edit <name>
    config switch-binding
      Description: Switch binding list.
      edit <switch-id>
        set policy {string}
      next
    end
  next
end
```

## config switch-binding

Parameter	Description	Type	Size	Default
policy	Custom auto-config policy.	string	Maximum length: 63	default

## config switch-controller initial-config template

Configure template for auto-generated VLANs.

```
config switch-controller initial-config template
  Description: Configure template for auto-generated VLANs.
  edit <name>
    set vlanid {integer}
    set ip {ipv4-classnet-host}
    set allowaccess {option1}, {option2}, ...
    set auto-ip [enable|disable]
    set dhcp-server [enable|disable]
  next
end
```

## config switch-controller initial-config template

Parameter	Description	Type	Size	Default																								
vlanid	Unique VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0																								
ip	Interface IPv4 address and subnet mask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																								
allowaccess	Permitted types of management access to this interface.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>fgfm</i></td> <td>FortiManager access.</td> </tr> <tr> <td><i>radius-acct</i></td> <td>RADIUS accounting access.</td> </tr> <tr> <td><i>probe-response</i></td> <td>Probe access.</td> </tr> <tr> <td><i>fabric</i></td> <td>Security Fabric access.</td> </tr> <tr> <td><i>ftm</i></td> <td>FTM access.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.			
Option	Description																											
<i>ping</i>	PING access.																											
<i>https</i>	HTTPS access.																											
<i>ssh</i>	SSH access.																											
<i>snmp</i>	SNMP access.																											
<i>http</i>	HTTP access.																											
<i>telnet</i>	TELNET access.																											
<i>fgfm</i>	FortiManager access.																											
<i>radius-acct</i>	RADIUS accounting access.																											
<i>probe-response</i>	Probe access.																											
<i>fabric</i>	Security Fabric access.																											
<i>ftm</i>	FTM access.																											
auto-ip	Automatically allocate interface address and subnet block.	option	-	enable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auto-ip status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable auto-ip status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auto-ip status.	<i>disable</i>	Disable auto-ip status.																					
Option	Description																											
<i>enable</i>	Enable auto-ip status.																											
<i>disable</i>	Disable auto-ip status.																											
dhcp-server	Enable/disable a DHCP server on this interface.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCP server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCP server.	<i>disable</i>	Disable DHCP server.																					
Option	Description																											
<i>enable</i>	Enable DHCP server.																											
<i>disable</i>	Disable DHCP server.																											



---

## config switch-controller initial-config vlans

Configure initial template for auto-generated VLAN interfaces.

```
config switch-controller initial-config vlans
  Description: Configure initial template for auto-generated VLAN interfaces.
  set default-vlan {string}
  set quarantine {string}
  set rspan {string}
  set voice {string}
  set video {string}
  set nac {string}
end
```

## config switch-controller initial-config vlans

Parameter	Description	Type	Size	Default
default-vlan	Default VLAN (native) assigned to all switch ports upon discovery.	string	Maximum length: 63	default
quarantine	VLAN for quarantined traffic.	string	Maximum length: 63	quarantine
rspan	VLAN for RSPAN/ERSPAN mirrored traffic.	string	Maximum length: 63	rspan
voice	VLAN dedicated for voice devices.	string	Maximum length: 63	voice
video	VLAN dedicated for video devices.	string	Maximum length: 63	video
nac	VLAN for NAC onboarding devices.	string	Maximum length: 63	onboarding

## config switch-controller switch-profile

Configure FortiSwitch switch profile.

```
config switch-controller switch-profile
  Description: Configure FortiSwitch switch profile.
  edit <name>
    set login-passwd-override [enable|disable]
    set login-passwd {password}
  next
end
```

## config switch-controller switch-profile

Parameter	Description	Type	Size	Default						
login-passwd-override	Enable/disable overriding the admin administrator password for a managed FortiSwitch with the FortiGate admin administrator account password.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Override a managed FortiSwitch's admin administrator password.</td></tr><tr><td><i>disable</i></td><td>Use the managed FortiSwitch admin administrator account password.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Override a managed FortiSwitch's admin administrator password.	<i>disable</i>	Use the managed FortiSwitch admin administrator account password.			
Option	Description									
<i>enable</i>	Override a managed FortiSwitch's admin administrator password.									
<i>disable</i>	Use the managed FortiSwitch admin administrator account password.									
login-passwd	Login password of managed FortiSwitch.	password	Not Specified							

## config switch-controller custom-command

Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices.

```
config switch-controller custom-command
  Description: Configure the FortiGate switch controller to send custom commands to managed
  FortiSwitch devices.
  edit <command-name>
    set description {string}
    set command {var-string}
  next
end
```

## config switch-controller custom-command

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 35	
command	String of commands to send to FortiSwitch devices (For example (%0a = return key): config switch trunk %0a edit myTrunk %0a set members port1 port2 %0a end %0a).	var-string	Maximum length: 4095	

## config switch-controller virtual-port-pool

Configure virtual pool.

```
config switch-controller virtual-port-pool
  Description: Configure virtual pool.
  edit <name>
    set description {string}
  next
```

end

## config switch-controller virtual-port-pool

Parameter	Description	Type	Size	Default
description	Virtual switch pool description.	string	Maximum length: 63	

## config switch-controller ptp settings

Global PTP settings.

```
config switch-controller ptp settings
  Description: Global PTP settings.
  set mode [disable|transparent-e2e|...]
end
```

## config switch-controller ptp settings

Parameter	Description	Type	Size	Default								
mode	Enable/disable PTP mode.	option	-	disable								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable PTP function. Packets are forwarded with no action.</td></tr><tr><td><i>transparent-e2e</i></td><td>Enable end-to-end transparent clock.</td></tr><tr><td><i>transparent-p2p</i></td><td>Enable peer-to-peer transparent clock.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable PTP function. Packets are forwarded with no action.	<i>transparent-e2e</i>	Enable end-to-end transparent clock.	<i>transparent-p2p</i>	Enable peer-to-peer transparent clock.			
Option	Description											
<i>disable</i>	Disable PTP function. Packets are forwarded with no action.											
<i>transparent-e2e</i>	Enable end-to-end transparent clock.											
<i>transparent-p2p</i>	Enable peer-to-peer transparent clock.											

## config switch-controller ptp policy

PTP policy configuration.

```
config switch-controller ptp policy
  Description: PTP policy configuration.
  edit <name>
    set status [disable|enable]
  next
end
```

## config switch-controller ptp policy

Parameter	Description	Type	Size	Default
status	Enable/disable PTP policy.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable PTP policy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable PTP policy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable PTP policy.	<i>enable</i>	Enable PTP policy.			
Option	Description									
<i>disable</i>	Disable PTP policy.									
<i>enable</i>	Enable PTP policy.									

## config switch-controller managed-switch

Configure FortiSwitch devices that are managed by this FortiGate.

```

config switch-controller managed-switch
  Description: Configure FortiSwitch devices that are managed by this FortiGate.
  edit <switch-id>
    set name {string}
    set description {string}
    set switch-profile {string}
    set access-profile {string}
    set fsw-wan1-peer {string}
    set fsw-wan1-admin [discovered|disable|...]
    set poe-pre-standard-detection [enable|disable]
    set poe-detection-type {integer}
    set directly-connected {integer}
    set version {integer}
    set max-allowed-trunk-members {integer}
    set pre-provisioned {integer}
    set l3-discovered {integer}
    set tdr-supported {string}
    set dynamic-capability {user}
    set switch-device-tag {string}
    set switch-dhcp_opt43_key {string}
    set mclag-igmp-snooping-aware [enable|disable]
    set dynamically-discovered {integer}
    set type [virtual|physical]
    set owner-vdom {string}
    set flow-identity {user}
    set staged-image-version {string}
    set delayed-restart-trigger {integer}
  config ports
    Description: Managed-switch port list.
    edit <port-name>
      set port-owner {string}
      set switch-id {string}
      set speed [10half|10full|...]
      set status [up|down]
      set poe-status [enable|disable]
      set ip-source-guard [disable|enable]
      set ptp-policy {string}
      set aggregator-mode [bandwidth|count]
      set rpvst-port [disabled|enabled]
      set poe-pre-standard-detection [enable|disable]
      set port-number {integer}
      set port-prefix-type {integer}
      set fortilink-port {integer}
  
```

```

set poe-capable {integer}
set stacking-port {integer}
set p2p-port {integer}
set mclag-icl-port {integer}
set fiber-port {integer}
set media-type {string}
set flags {integer}
set isl-local-trunk-name {string}
set isl-peer-port-name {string}
set isl-peer-device-name {string}
set fgt-peer-port-name {string}
set fgt-peer-device-name {string}
set vlan {string}
set allowed-vlans-all [enable|disable]
set allowed-vlans <vlan-name1>, <vlan-name2>, ...
set untagged-vlans <vlan-name1>, <vlan-name2>, ...
set type [physical|trunk]
set access-mode [normal|nac]
set dhcp-snooping [untrusted|trusted]
set dhcp-snoop-option82-trust [enable|disable]
set arp-inspection-trust [untrusted|trusted]
set igmps-flood-reports [enable|disable]
set igmps-flood-traffic [enable|disable]
set stp-state [enabled|disabled]
set stp-root-guard [enabled|disabled]
set stp-bpdu-guard [enabled|disabled]
set stp-bpdu-guard-timeout {integer}
set edge-port [enable|disable]
set discard-mode [none|all-untagged|...]
set packet-sampler [enabled|disabled]
set packet-sample-rate {integer}
set sflow-counter-interval {integer}
set sample-direction [tx|rx|...]
set flow-control [disable|tx|...]
set pause-meter {integer}
set pause-meter-resume [75%|50%|...]
set loop-guard [enabled|disabled]
set loop-guard-timeout {integer}
set qos-policy {string}
set storm-control-policy {string}
set port-security-policy {string}
set export-to-pool {string}
set export-tags <tag-name1>, <tag-name2>, ...
set learning-limit {integer}
set sticky-mac [enable|disable]
set lldp-status [disable|rx-only|...]
set lldp-profile {string}
set export-to {string}
set mac-addr {mac-address}
set port-selection-criteria [src-mac|dst-mac|...]
set description {string}
set lacp-speed [slow|fast]
set mode [static|lacp-passive|...]
set bundle [enable|disable]
set member-withdrawal-behavior [forward|block]
set mclag [enable|disable]
set min-bundle {integer}

```

```

        set max-bundle {integer}
        set members <member-name1>, <member-name2>, ...
    next
end
config ip-source-guard
    Description: IP source guard.
    edit <port>
        set description {string}
        config binding-entry
            Description: IP and MAC address configuration.
            edit <entry-name>
                set ip {ipv4-address-any}
                set mac {mac-address}
            next
        end
    next
end
config stp-settings
    Description: Configuration method to edit Spanning Tree Protocol (STP) settings used
        to prevent bridge loops.
    set local-override [enable|disable]
    set name {string}
    set revision {integer}
    set hello-time {integer}
    set forward-time {integer}
    set max-age {integer}
    set max-hops {integer}
    set pending-timer {integer}
end
config stp-instance
    Description: Configuration method to edit Spanning Tree Protocol (STP) instances.
    edit <id>
        set priority [0|4096|...]
    next
end
set override-snmp-sysinfo [disable|enable]
config snmp-sysinfo
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
        system info.
    set status [disable|enable]
    set engine-id {string}
    set description {string}
    set contact-info {string}
    set location {string}
end
set override-snmp-trap-threshold [enable|disable]
config snmp-trap-threshold
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
        trap threshold values.
    set trap-high-cpu-threshold {integer}
    set trap-low-memory-threshold {integer}
    set trap-log-full-threshold {integer}
end
set override-snmp-community [enable|disable]
config snmp-community
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
        communities.
    edit <id>

```

```

set name {string}
set status [disable|enable]
config hosts
    Description: Configure IPv4 SNMP managers (hosts).
    edit <id>
        set ip {user}
    next
end
set query-v1-status [disable|enable]
set query-v1-port {integer}
set query-v2c-status [disable|enable]
set query-v2c-port {integer}
set trap-v1-status [disable|enable]
set trap-v1-lport {integer}
set trap-v1-rport {integer}
set trap-v2c-status [disable|enable]
set trap-v2c-lport {integer}
set trap-v2c-rport {integer}
set events {option1}, {option2}, ...
next
end
set override-snmp-user [enable|disable]
config snmp-user
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
    users.
    edit <name>
        set queries [disable|enable]
        set query-port {integer}
        set security-level [no-auth-no-priv|auth-no-priv|...]
        set auth-proto [md5|sha]
        set auth-pwd {password}
        set priv-proto [aes|des]
        set priv-pwd {password}
    next
end
set qos-drop-policy [taildrop|random-early-detection]
set qos-red-probability {integer}
config switch-log
    Description: Configuration method to edit FortiSwitch logging settings (logs are
    transferred to and inserted into the FortiGate event log).
    set local-override [enable|disable]
    set status [enable|disable]
    set severity [emergency|alert|...]
end
config remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
    edit <name>
        set status [enable|disable]
        set server {string}
        set port {integer}
        set severity [emergency|alert|...]
        set csv [enable|disable]
        set facility [kernel|user|...]
    next
end
config storm-control

```

```

Description: Configuration method to edit FortiSwitch storm control for measuring
            traffic activity using data rates to prevent traffic disruption.
set local-override [enable|disable]
set rate {integer}
set unknown-unicast [enable|disable]
set unknown-multicast [enable|disable]
set broadcast [enable|disable]
end
config mirror
Description: Configuration method to edit FortiSwitch packet mirror.
edit <name>
    set status [active|inactive]
    set switching-packet [enable|disable]
    set dst {string}
    set src-ingress <name1>, <name2>, ...
    set src-egress <name1>, <name2>, ...
next
end
config static-mac
Description: Configuration method to edit FortiSwitch Static and Sticky MAC.
edit <id>
    set type [static|sticky]
    set vlan {string}
    set mac {mac-address}
    set interface {string}
    set description {string}
next
end
config custom-command
Description: Configuration method to edit FortiSwitch commands to be pushed to this
            FortiSwitch device upon rebooting the FortiGate switch controller or the
            FortiSwitch.
edit <command-entry>
    set command-name {string}
next
end
config igmp-snooping
Description: Configure FortiSwitch IGMP snooping global settings.
set local-override [enable|disable]
set aging-time {integer}
set flood-unknown-multicast [enable|disable]
end
config 802-1X-settings
Description: Configuration method to edit FortiSwitch 802.1X global settings.
set local-override [enable|disable]
set link-down-auth [set-unauth|no-action]
set reauth-period {integer}
set max-reauth-attempt {integer}
set tx-period {integer}
end
next
end

```



## config switch-controller managed-switch

Parameter	Description	Type	Size	Default								
name	Managed-switch name.	string	Maximum length: 35									
description	Description.	string	Maximum length: 63									
switch-profile	FortiSwitch profile.	string	Maximum length: 35	default								
access-profile	FortiSwitch access profile.	string	Maximum length: 31	default								
fsw-wan1-peer	Fortiswitch WAN1 peer port.	string	Maximum length: 35									
fsw-wan1-admin	FortiSwitch WAN1 admin status; enable to authorize the FortiSwitch as a managed switch.	option	-	discovered								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discovered</i></td> <td>Link waiting to be authorized.</td> </tr> <tr> <td><i>disable</i></td> <td>Link unauthorized.</td> </tr> <tr> <td><i>enable</i></td> <td>Link authorized.</td> </tr> </tbody> </table>		Option	Description	<i>discovered</i>	Link waiting to be authorized.	<i>disable</i>	Link unauthorized.	<i>enable</i>	Link authorized.		
Option	Description											
<i>discovered</i>	Link waiting to be authorized.											
<i>disable</i>	Link unauthorized.											
<i>enable</i>	Link authorized.											
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PoE pre-standard detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PoE pre-standard detection.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable PoE pre-standard detection.	<i>disable</i>	Disable PoE pre-standard detection.				
Option	Description											
<i>enable</i>	Enable PoE pre-standard detection.											
<i>disable</i>	Disable PoE pre-standard detection.											
poe-detection-type	PoE detection type for FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0								
directly-connected	Directly connected FortiSwitch.	integer	Minimum value: 0 Maximum value: 1	0								

Parameter	Description	Type	Size	Default						
version	FortiSwitch version.	integer	Minimum value: 0 Maximum value: 255	0						
max-allowed-trunk-members	FortiSwitch maximum allowed trunk members.	integer	Minimum value: 0 Maximum value: 255	0						
pre-provisioned	Pre-provisioned managed switch.	integer	Minimum value: 0 Maximum value: 255	0						
l3-discovered	Layer 3 management discovered.	integer	Minimum value: 0 Maximum value: 1	0						
tdr-supported	TDR supported.	string	Maximum length: 31							
dynamic-capability	List of features this FortiSwitch supports (not configurable) that is sent to the FortiGate device for subsequent configuration initiated by the FortiGate device.	user	Not Specified	0x00000000000000000000000000000000						
switch-device-tag	User definable label/tag.	string	Maximum length: 32							
switch-dhcp_opt43_key	DHCP option43 key.	string	Maximum length: 63							
mclag-igmp-snooping-aware	Enable/disable MCLAG IGMP-snooping awareness.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MCLAG IGMP-snooping awareness.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MCLAG IGMP-snooping awareness.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable MCLAG IGMP-snooping awareness.	<i>disable</i>	Disable MCLAG IGMP-snooping awareness.		
Option	Description									
<i>enable</i>	Enable MCLAG IGMP-snooping awareness.									
<i>disable</i>	Disable MCLAG IGMP-snooping awareness.									
dynamically-discovered	Dynamically discovered FortiSwitch.	integer	Minimum value: 0 Maximum value: 1	0						

Parameter	Description	Type	Size	Default
type	Indication of switch type, physical or virtual.	option	-	physical
	<b>Option</b>	<b>Description</b>		
	<i>virtual</i>	Switch is of type virtual.		
	<i>physical</i>	Switch is of type physical.		
owner-vdom	VDOM which owner of port belongs to.	string	Maximum length: 31	
flow-identity	Flow-tracking netflow ipfix switch identity in hex format.	user	Not Specified	00000000
staged-image-version	Staged image version for FortiSwitch.	string	Maximum length: 127	
delayed-restart-trigger	Delayed restart triggered for this FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0
override-snmp-sysinfo	Enable/disable overriding the global SNMP system information.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Use the global SNMP system information.		
	<i>enable</i>	Override the global SNMP system information.		
override-snmp-trap-threshold	Enable/disable overriding the global SNMP trap threshold values.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override the global SNMP trap threshold values.		
	<i>disable</i>	Use the global SNMP trap threshold values.		
override-snmp-community	Enable/disable overriding the global SNMP communities.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the global SNMP communities.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the global SNMP communities.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the global SNMP communities.	<i>disable</i>	Use the global SNMP communities.			
Option	Description									
<i>enable</i>	Override the global SNMP communities.									
<i>disable</i>	Use the global SNMP communities.									
override-snmp-user	Enable/disable overriding the global SNMP users.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the global SNMPv3 users.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the global SNMPv3 users.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the global SNMPv3 users.	<i>disable</i>	Use the global SNMPv3 users.			
Option	Description									
<i>enable</i>	Override the global SNMPv3 users.									
<i>disable</i>	Use the global SNMPv3 users.									
qos-drop-policy	Set QoS drop-policy.	option	-	taildrop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>taildrop</i></td> <td>Taildrop policy.</td> </tr> <tr> <td><i>random-early-detection</i></td> <td>Random early detection drop policy.</td> </tr> </tbody> </table>	Option	Description	<i>taildrop</i>	Taildrop policy.	<i>random-early-detection</i>	Random early detection drop policy.			
Option	Description									
<i>taildrop</i>	Taildrop policy.									
<i>random-early-detection</i>	Random early detection drop policy.									
qos-red-probability	Set QoS RED/WRED drop probability.	integer	Minimum value: 0 Maximum value: 100	12						

## config ports

Parameter	Description	Type	Size	Default								
port-owner	Switch port name.	string	Maximum length: 15									
switch-id	Switch id.	string	Maximum length: 16									
speed	Switch port speed; default and available settings depend on hardware.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>10half</i></td> <td>10M half-duplex.</td> </tr> <tr> <td><i>10full</i></td> <td>10M full-duplex.</td> </tr> <tr> <td><i>100half</i></td> <td>100M half-duplex.</td> </tr> </tbody> </table>	Option	Description	<i>10half</i>	10M half-duplex.	<i>10full</i>	10M full-duplex.	<i>100half</i>	100M half-duplex.			
Option	Description											
<i>10half</i>	10M half-duplex.											
<i>10full</i>	10M full-duplex.											
<i>100half</i>	100M half-duplex.											

Parameter	Description	Type	Size	Default																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>100full</i></td> <td>100M full-duplex.</td> </tr> <tr> <td><i>1000auto</i></td> <td>Auto-negotiation (1G full-duplex only).</td> </tr> <tr> <td><i>1000fiber</i></td> <td>1G full-duplex (fiber SFPs only)</td> </tr> <tr> <td><i>1000full</i></td> <td>1G full-duplex</td> </tr> <tr> <td><i>10000</i></td> <td>10G full-duplex</td> </tr> <tr> <td><i>40000</i></td> <td>40G full-duplex</td> </tr> <tr> <td><i>auto</i></td> <td>Auto-negotiation.</td> </tr> <tr> <td><i>auto-module</i></td> <td>Auto Module.</td> </tr> <tr> <td><i>100FX-half</i></td> <td>100Mbps half-duplex. 100Base-FX.</td> </tr> <tr> <td><i>100FX-full</i></td> <td>100Mbps full-duplex. 100Base-FX.</td> </tr> <tr> <td><i>100000full</i></td> <td>100Gbps full-duplex.</td> </tr> <tr> <td><i>2500auto</i></td> <td>Auto-Negotiation (2.5Gbps Only).</td> </tr> <tr> <td><i>25000full</i></td> <td>25Gbps full-duplex.</td> </tr> <tr> <td><i>50000full</i></td> <td>50Gbps full-duplex.</td> </tr> <tr> <td><i>10000cr</i></td> <td>10Gbps copper interface.</td> </tr> <tr> <td><i>10000sr</i></td> <td>10Gbps SFI interface.</td> </tr> <tr> <td><i>100000sr4</i></td> <td>100Gbps SFI interface.</td> </tr> <tr> <td><i>100000cr4</i></td> <td>100Gbps copper interface.</td> </tr> <tr> <td><i>25000cr4</i></td> <td>25Gbps copper interface.</td> </tr> <tr> <td><i>25000sr4</i></td> <td>25Gbps SFI interface.</td> </tr> <tr> <td><i>5000full</i></td> <td>5Gbps full-duplex.</td> </tr> </tbody> </table>	Option	Description	<i>100full</i>	100M full-duplex.	<i>1000auto</i>	Auto-negotiation (1G full-duplex only).	<i>1000fiber</i>	1G full-duplex (fiber SFPs only)	<i>1000full</i>	1G full-duplex	<i>10000</i>	10G full-duplex	<i>40000</i>	40G full-duplex	<i>auto</i>	Auto-negotiation.	<i>auto-module</i>	Auto Module.	<i>100FX-half</i>	100Mbps half-duplex. 100Base-FX.	<i>100FX-full</i>	100Mbps full-duplex. 100Base-FX.	<i>100000full</i>	100Gbps full-duplex.	<i>2500auto</i>	Auto-Negotiation (2.5Gbps Only).	<i>25000full</i>	25Gbps full-duplex.	<i>50000full</i>	50Gbps full-duplex.	<i>10000cr</i>	10Gbps copper interface.	<i>10000sr</i>	10Gbps SFI interface.	<i>100000sr4</i>	100Gbps SFI interface.	<i>100000cr4</i>	100Gbps copper interface.	<i>25000cr4</i>	25Gbps copper interface.	<i>25000sr4</i>	25Gbps SFI interface.	<i>5000full</i>	5Gbps full-duplex.			
Option	Description																																															
<i>100full</i>	100M full-duplex.																																															
<i>1000auto</i>	Auto-negotiation (1G full-duplex only).																																															
<i>1000fiber</i>	1G full-duplex (fiber SFPs only)																																															
<i>1000full</i>	1G full-duplex																																															
<i>10000</i>	10G full-duplex																																															
<i>40000</i>	40G full-duplex																																															
<i>auto</i>	Auto-negotiation.																																															
<i>auto-module</i>	Auto Module.																																															
<i>100FX-half</i>	100Mbps half-duplex. 100Base-FX.																																															
<i>100FX-full</i>	100Mbps full-duplex. 100Base-FX.																																															
<i>100000full</i>	100Gbps full-duplex.																																															
<i>2500auto</i>	Auto-Negotiation (2.5Gbps Only).																																															
<i>25000full</i>	25Gbps full-duplex.																																															
<i>50000full</i>	50Gbps full-duplex.																																															
<i>10000cr</i>	10Gbps copper interface.																																															
<i>10000sr</i>	10Gbps SFI interface.																																															
<i>100000sr4</i>	100Gbps SFI interface.																																															
<i>100000cr4</i>	100Gbps copper interface.																																															
<i>25000cr4</i>	25Gbps copper interface.																																															
<i>25000sr4</i>	25Gbps SFI interface.																																															
<i>5000full</i>	5Gbps full-duplex.																																															
status	Switch port admin status: up or down.	option	-	up																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>up</i></td> <td>Set admin status up.</td> </tr> <tr> <td><i>down</i></td> <td>Set admin status down.</td> </tr> </tbody> </table>	Option	Description	<i>up</i>	Set admin status up.	<i>down</i>	Set admin status down.																																									
Option	Description																																															
<i>up</i>	Set admin status up.																																															
<i>down</i>	Set admin status down.																																															
poe-status	Enable/disable PoE status.	option	-	enable																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PoE status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PoE status.																																											
Option	Description																																															
<i>enable</i>	Enable PoE status.																																															

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable PoE status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable PoE status.					
Option	Description									
<i>disable</i>	Disable PoE status.									
ip-source-guard	Enable/disable IP source guard.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IP source guard.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable IP source guard.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IP source guard.	<i>enable</i>	Enable IP source guard.			
Option	Description									
<i>disable</i>	Disable IP source guard.									
<i>enable</i>	Enable IP source guard.									
ptp-policy	PTP policy configuration.	string	Maximum length: 63	default						
aggregator-mode	LACP member select mode.	option	-	bandwidth						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bandwidth</i></td> <td>Member selection based on largest total bandwidth of links of similar speed.</td> </tr> <tr> <td><i>count</i></td> <td>Member selection based on largest count of similar link speed.</td> </tr> </tbody> </table>	Option	Description	<i>bandwidth</i>	Member selection based on largest total bandwidth of links of similar speed.	<i>count</i>	Member selection based on largest count of similar link speed.			
Option	Description									
<i>bandwidth</i>	Member selection based on largest total bandwidth of links of similar speed.									
<i>count</i>	Member selection based on largest count of similar link speed.									
rpvst-port	Enable/disable inter-operability with rapid PVST on this interface.	option	-	disabled						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disable inter-operability with rapid PVST on this interface.</td> </tr> <tr> <td><i>enabled</i></td> <td>Enable inter-operability with rapid PVST on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disable inter-operability with rapid PVST on this interface.	<i>enabled</i>	Enable inter-operability with rapid PVST on this interface.			
Option	Description									
<i>disabled</i>	Disable inter-operability with rapid PVST on this interface.									
<i>enabled</i>	Enable inter-operability with rapid PVST on this interface.									
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PoE pre-standard detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PoE pre-standard detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PoE pre-standard detection.	<i>disable</i>	Disable PoE pre-standard detection.			
Option	Description									
<i>enable</i>	Enable PoE pre-standard detection.									
<i>disable</i>	Disable PoE pre-standard detection.									
port-number	Port number.	integer	Minimum value: 1 Maximum value: 64	0						

Parameter	Description	Type	Size	Default
port-prefix-type	Port prefix type.	integer	Minimum value: 0 Maximum value: 1	0
fortilink-port	FortiLink uplink port.	integer	Minimum value: 0 Maximum value: 1	0
poe-capable	PoE capable.	integer	Minimum value: 0 Maximum value: 1	0
stacking-port	Stacking port.	integer	Minimum value: 0 Maximum value: 1	0
p2p-port	General peer to peer tunnel port.	integer	Minimum value: 0 Maximum value: 1	0
mclag-icl-port	MCLAG-ICL port.	integer	Minimum value: 0 Maximum value: 1	0
fiber-port	Fiber-port.	integer	Minimum value: 0 Maximum value: 1	0
media-type	Media type.	string	Maximum length: 31	
flags	Port properties flags.	integer	Minimum value: 0 Maximum value: 4294967295	0
isl-local-trunk-name	ISL local trunk name.	string	Maximum length: 15	
isl-peer-port-name	ISL peer port name.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default						
isl-peer-device-name	ISL peer device name.	string	Maximum length: 16							
fgt-peer-port-name	FGT peer port name.	string	Maximum length: 15							
fgt-peer-device-name	FGT peer device name.	string	Maximum length: 16							
vlan	Assign switch ports to a VLAN.	string	Maximum length: 15							
allowed-vlans-all	Enable/disable all defined vlans on this port.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable all defined VLANs on this port.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all defined VLANs on this port.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable all defined VLANs on this port.	<i>disable</i>	Disable all defined VLANs on this port.			
Option	Description									
<i>enable</i>	Enable all defined VLANs on this port.									
<i>disable</i>	Disable all defined VLANs on this port.									
allowed-vlans <vlan-name>	Configure switch port tagged vlans VLAN name.	string	Maximum length: 79							
untagged-vlans <vlan-name>	Configure switch port untagged vlans VLAN name.	string	Maximum length: 79							
type	Interface type: physical or trunk port.	option	-	physical						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>physical</i></td> <td>Physical port.</td> </tr> <tr> <td><i>trunk</i></td> <td>Trunk port.</td> </tr> </tbody> </table>	Option	Description	<i>physical</i>	Physical port.	<i>trunk</i>	Trunk port.			
Option	Description									
<i>physical</i>	Physical port.									
<i>trunk</i>	Trunk port.									
access-mode	Access mode of the port.	option	-	normal						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>normal</i></td> <td>Normal mode.</td> </tr> <tr> <td><i>nac</i></td> <td>NAC mode.</td> </tr> </tbody> </table>	Option	Description	<i>normal</i>	Normal mode.	<i>nac</i>	NAC mode.			
Option	Description									
<i>normal</i>	Normal mode.									
<i>nac</i>	NAC mode.									
dhcp-snooping	Trusted or untrusted DHCP-snooping interface.	option	-	untrusted						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>untrusted</i></td> <td>Untrusted DHCP snooping interface.</td> </tr> <tr> <td><i>trusted</i></td> <td>Trusted DHCP snooping interface.</td> </tr> </tbody> </table>	Option	Description	<i>untrusted</i>	Untrusted DHCP snooping interface.	<i>trusted</i>	Trusted DHCP snooping interface.			
Option	Description									
<i>untrusted</i>	Untrusted DHCP snooping interface.									
<i>trusted</i>	Trusted DHCP snooping interface.									



Parameter	Description	Type	Size	Default						
dhcp-snoop-option82-trust	Enable/disable allowance of DHCP with option-82 on untrusted interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable allowance of DHCP with option-82 on untrusted interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable allowance of DHCP with option-82 on untrusted interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.	<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.			
Option	Description									
<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.									
<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.									
arp-inspection-trust	Trusted or untrusted dynamic ARP inspection.	option	-	untrusted						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>untrusted</i></td> <td>Untrusted dynamic ARP inspection.</td> </tr> <tr> <td><i>trusted</i></td> <td>Trusted dynamic ARP inspection.</td> </tr> </tbody> </table>	Option	Description	<i>untrusted</i>	Untrusted dynamic ARP inspection.	<i>trusted</i>	Trusted dynamic ARP inspection.			
Option	Description									
<i>untrusted</i>	Untrusted dynamic ARP inspection.									
<i>trusted</i>	Trusted dynamic ARP inspection.									
igmps-flood-reports	Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable flooding of IGMP snooping reports to this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable flooding of IGMP snooping reports to this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.	<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.			
Option	Description									
<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.									
<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.									
igmps-flood-traffic	Enable/disable flooding of IGMP snooping traffic to this interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable flooding of IGMP snooping traffic to this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable flooding of IGMP snooping traffic to this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.	<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.			
Option	Description									
<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.									
<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.									
stp-state	Enable/disable Spanning Tree Protocol (STP) on this interface.	option	-	enabled						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enabled</i></td> <td>Enable STP on this interface.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disable STP on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enabled</i>	Enable STP on this interface.	<i>disabled</i>	Disable STP on this interface.			
Option	Description									
<i>enabled</i>	Enable STP on this interface.									
<i>disabled</i>	Disable STP on this interface.									
stp-root-guard	Enable/disable STP root guard on this interface.	option	-	disabled						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enabled</i></td> <td>Enable STP root-guard on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enabled</i>	Enable STP root-guard on this interface.					
Option	Description									
<i>enabled</i>	Enable STP root-guard on this interface.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Disable STP root-guard on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Disable STP root-guard on this interface.							
Option	Description											
<i>disabled</i>	Disable STP root-guard on this interface.											
stp-bpdu-guard	Enable/disable STP BPDU guard on this interface.	option	-	disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enabled</i></td> <td>Enable STP BPDU guard on this interface.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disable STP BPDU guard on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enabled</i>	Enable STP BPDU guard on this interface.	<i>disabled</i>	Disable STP BPDU guard on this interface.					
Option	Description											
<i>enabled</i>	Enable STP BPDU guard on this interface.											
<i>disabled</i>	Disable STP BPDU guard on this interface.											
stp-bpdu-guard-timeout	BPDU Guard disabling protection .	integer	Minimum value: 0 Maximum value: 120	5								
edge-port	Enable/disable this interface as an edge port, bridging connections between workstations and/or computers.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this interface as an edge port.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this interface as an edge port.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this interface as an edge port.	<i>disable</i>	Disable this interface as an edge port.					
Option	Description											
<i>enable</i>	Enable this interface as an edge port.											
<i>disable</i>	Disable this interface as an edge port.											
discard-mode	Configure discard mode for port.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Discard disabled.</td> </tr> <tr> <td><i>all-untagged</i></td> <td>Discard all frames that are untagged.</td> </tr> <tr> <td><i>all-tagged</i></td> <td>Discard all frames that are tagged.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Discard disabled.	<i>all-untagged</i>	Discard all frames that are untagged.	<i>all-tagged</i>	Discard all frames that are tagged.			
Option	Description											
<i>none</i>	Discard disabled.											
<i>all-untagged</i>	Discard all frames that are untagged.											
<i>all-tagged</i>	Discard all frames that are tagged.											
packet-sampler	Enable/disable packet sampling on this interface.	option	-	disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enabled</i></td> <td>Enable packet sampling on this interface.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disable packet sampling on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enabled</i>	Enable packet sampling on this interface.	<i>disabled</i>	Disable packet sampling on this interface.					
Option	Description											
<i>enabled</i>	Enable packet sampling on this interface.											
<i>disabled</i>	Disable packet sampling on this interface.											
packet-sample-rate	Packet sampling rate .	integer	Minimum value: 0 Maximum value: 99999	512								

Parameter	Description	Type	Size	Default										
sflow-counter-interval	sFlow sampling counter polling interval .	integer	Minimum value: 0 Maximum value: 255	0										
sample-direction	Packet sampling direction.	option	-	both										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tx</i></td> <td>Monitor transmitted traffic.</td> </tr> <tr> <td><i>rx</i></td> <td>Monitor received traffic.</td> </tr> <tr> <td><i>both</i></td> <td>Monitor transmitted and received traffic.</td> </tr> </tbody> </table>	Option	Description	<i>tx</i>	Monitor transmitted traffic.	<i>rx</i>	Monitor received traffic.	<i>both</i>	Monitor transmitted and received traffic.					
Option	Description													
<i>tx</i>	Monitor transmitted traffic.													
<i>rx</i>	Monitor received traffic.													
<i>both</i>	Monitor transmitted and received traffic.													
flow-control	Flow control direction.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable flow control.</td> </tr> <tr> <td><i>tx</i></td> <td>Enable flow control for transmission pause control frames.</td> </tr> <tr> <td><i>rx</i></td> <td>Enable flow control for receive pause control frames.</td> </tr> <tr> <td><i>both</i></td> <td>Enable flow control for both transmission and receive pause control frames.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable flow control.	<i>tx</i>	Enable flow control for transmission pause control frames.	<i>rx</i>	Enable flow control for receive pause control frames.	<i>both</i>	Enable flow control for both transmission and receive pause control frames.			
Option	Description													
<i>disable</i>	Disable flow control.													
<i>tx</i>	Enable flow control for transmission pause control frames.													
<i>rx</i>	Enable flow control for receive pause control frames.													
<i>both</i>	Enable flow control for both transmission and receive pause control frames.													
pause-meter	Configure ingress pause metering rate, in kbps .	integer	Minimum value: 128 Maximum value: 2147483647	0										
pause-meter-resume	Resume threshold for resuming traffic on ingress port.	option	-	50%										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>75%</i></td> <td>Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.</td> </tr> <tr> <td><i>50%</i></td> <td>Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.</td> </tr> <tr> <td><i>25%</i></td> <td>Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.</td> </tr> </tbody> </table>	Option	Description	<i>75%</i>	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.	<i>50%</i>	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.	<i>25%</i>	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.					
Option	Description													
<i>75%</i>	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.													
<i>50%</i>	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.													
<i>25%</i>	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.													
loop-guard	Enable/disable loop-guard on this interface, an STP optimization used to prevent network loops.	option	-	disabled										

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enabled</i></td> <td>Enable loop-guard on this interface.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disable loop-guard on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enabled</i>	Enable loop-guard on this interface.	<i>disabled</i>	Disable loop-guard on this interface.							
Option	Description													
<i>enabled</i>	Enable loop-guard on this interface.													
<i>disabled</i>	Disable loop-guard on this interface.													
loop-guard-timeout	Loop-guard timeout .	integer	Minimum value: 0 Maximum value: 120	45										
qos-policy	Switch controller QoS policy from available options.	string	Maximum length: 63	default										
storm-control-policy	Switch controller storm control policy from available options.	string	Maximum length: 63	default										
port-security-policy	Switch controller authentication policy to apply to this managed switch from available options.	string	Maximum length: 31											
export-to-pool	Switch controller export port to pool-list.	string	Maximum length: 35											
export-tags <tag-name>	Configure export tag(s) for FortiSwitch port when exported to a virtual port pool. FortiSwitch port tag name when exported to a virtual port pool.	string	Maximum length: 63											
learning-limit	Limit the number of dynamic MAC addresses on this Port .	integer	Minimum value: 0 Maximum value: 128	0										
sticky-mac	Enable or disable sticky-mac on the interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sticky mac on the interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sticky mac on the interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sticky mac on the interface.	<i>disable</i>	Disable sticky mac on the interface.							
Option	Description													
<i>enable</i>	Enable sticky mac on the interface.													
<i>disable</i>	Disable sticky mac on the interface.													
lldp-status	LLDP transmit and receive status.	option	-	tx-rx										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable LLDP TX and RX.</td> </tr> <tr> <td><i>rx-only</i></td> <td>Enable LLDP as RX only.</td> </tr> <tr> <td><i>tx-only</i></td> <td>Enable LLDP as TX only.</td> </tr> <tr> <td><i>tx-rx</i></td> <td>Enable LLDP TX and RX.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable LLDP TX and RX.	<i>rx-only</i>	Enable LLDP as RX only.	<i>tx-only</i>	Enable LLDP as TX only.	<i>tx-rx</i>	Enable LLDP TX and RX.			
Option	Description													
<i>disable</i>	Disable LLDP TX and RX.													
<i>rx-only</i>	Enable LLDP as RX only.													
<i>tx-only</i>	Enable LLDP as TX only.													
<i>tx-rx</i>	Enable LLDP TX and RX.													

Parameter	Description	Type	Size	Default														
lldp-profile	LLDP port TLV profile.	string	Maximum length: 63	default-auto-isl														
export-to	Export managed-switch port to a tenant VDOM.	string	Maximum length: 31															
mac-addr	Port/Trunk MAC.	mac-address	Not Specified	00:00:00:00:00:00														
port-selection-criteria	Algorithm for aggregate port selection.	option	-	src-dst-ip														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>src-mac</i></td> <td>Source MAC address.</td> </tr> <tr> <td><i>dst-mac</i></td> <td>Destination MAC address.</td> </tr> <tr> <td><i>src-dst-mac</i></td> <td>Source and destination MAC address.</td> </tr> <tr> <td><i>src-ip</i></td> <td>Source IP address.</td> </tr> <tr> <td><i>dst-ip</i></td> <td>Destination IP address.</td> </tr> <tr> <td><i>src-dst-ip</i></td> <td>Source and destination IP address.</td> </tr> </tbody> </table>	Option	Description	<i>src-mac</i>	Source MAC address.	<i>dst-mac</i>	Destination MAC address.	<i>src-dst-mac</i>	Source and destination MAC address.	<i>src-ip</i>	Source IP address.	<i>dst-ip</i>	Destination IP address.	<i>src-dst-ip</i>	Source and destination IP address.			
Option	Description																	
<i>src-mac</i>	Source MAC address.																	
<i>dst-mac</i>	Destination MAC address.																	
<i>src-dst-mac</i>	Source and destination MAC address.																	
<i>src-ip</i>	Source IP address.																	
<i>dst-ip</i>	Destination IP address.																	
<i>src-dst-ip</i>	Source and destination IP address.																	
description	Description for port.	string	Maximum length: 63															
lacp-speed	end Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second (fast).	option	-	slow														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>slow</i></td> <td>Send LACP message every 30 seconds.</td> </tr> <tr> <td><i>fast</i></td> <td>Send LACP message every second.</td> </tr> </tbody> </table>	Option	Description	<i>slow</i>	Send LACP message every 30 seconds.	<i>fast</i>	Send LACP message every second.											
Option	Description																	
<i>slow</i>	Send LACP message every 30 seconds.																	
<i>fast</i>	Send LACP message every second.																	
mode	LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.	option	-	static														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Static aggregation, do not send and ignore any control messages.</td> </tr> <tr> <td><i>lacp-passive</i></td> <td>Passively use LACP to negotiate 802.3ad aggregation.</td> </tr> <tr> <td><i>lacp-active</i></td> <td>Actively use LACP to negotiate 802.3ad aggregation.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Static aggregation, do not send and ignore any control messages.	<i>lacp-passive</i>	Passively use LACP to negotiate 802.3ad aggregation.	<i>lacp-active</i>	Actively use LACP to negotiate 802.3ad aggregation.									
Option	Description																	
<i>static</i>	Static aggregation, do not send and ignore any control messages.																	
<i>lacp-passive</i>	Passively use LACP to negotiate 802.3ad aggregation.																	
<i>lacp-active</i>	Actively use LACP to negotiate 802.3ad aggregation.																	
bundle	Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.	option	-	disable														

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable bundling.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable bundling.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable bundling.	<i>disable</i>	Disable bundling.			
Option	Description									
<i>enable</i>	Enable bundling.									
<i>disable</i>	Disable bundling.									
member-withdrawal-behavior	Port behavior after it withdraws because of loss of control packets.	option	-	block						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>forward</i></td> <td>Forward traffic.</td> </tr> <tr> <td><i>block</i></td> <td>Block traffic.</td> </tr> </tbody> </table>	Option	Description	<i>forward</i>	Forward traffic.	<i>block</i>	Block traffic.			
Option	Description									
<i>forward</i>	Forward traffic.									
<i>block</i>	Block traffic.									
mclag	Enable/disable multi-chassis link aggregation (MCLAG).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MCLAG.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MCLAG.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MCLAG.	<i>disable</i>	Disable MCLAG.			
Option	Description									
<i>enable</i>	Enable MCLAG.									
<i>disable</i>	Disable MCLAG.									
min-bundle	Minimum size of LAG bundle	integer	Minimum value: 1 Maximum value: 24	1						
max-bundle	Maximum size of LAG bundle	integer	Minimum value: 1 Maximum value: 24	24						
members <member-name>	Aggregated LAG bundle interfaces. Interface name from available options.	string	Maximum length: 79							

### config ip-source-guard

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	

## config binding-entry

Parameter	Description	Type	Size	Default
ip	Source IP for this rule.	ipv4-address-any	Not Specified	0.0.0.0
mac	MAC address for this rule.	mac-address	Not Specified	00:00:00:00:00:00

## config stp-settings

Parameter	Description	Type	Size	Default						
local-override	Enable to configure local STP settings that override global STP settings.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Override global STP settings.</td></tr><tr><td><i>disable</i></td><td>Use global STP settings.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Override global STP settings.	<i>disable</i>	Use global STP settings.			
Option	Description									
<i>enable</i>	Override global STP settings.									
<i>disable</i>	Use global STP settings.									
name	Name of local STP settings configuration.	string	Maximum length: 31							
revision	STP revision number .	integer	Minimum value: 0 Maximum value: 65535	0						
hello-time	Period of time between successive STP frame Bridge Protocol Data Units .	integer	Minimum value: 1 Maximum value: 10	2						
forward-time	Period of time a port is in listening and learning state .	integer	Minimum value: 4 Maximum value: 30	15						
max-age	Maximum time before a bridge port saves its configuration BPDU information .	integer	Minimum value: 6 Maximum value: 40	20						
max-hops	Maximum number of hops between the root bridge and the furthest bridge .	integer	Minimum value: 1 Maximum value: 40	20						

Parameter	Description	Type	Size	Default
pending-timer	Pending time .	integer	Minimum value: 1 Maximum value: 15	4

### config stp-instance

Parameter	Description	Type	Size	Default																																		
priority	Priority.	option	-	32768																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>0</td><td>0.</td></tr> <tr><td>4096</td><td>4096.</td></tr> <tr><td>8192</td><td>8192.</td></tr> <tr><td>12288</td><td>12288.</td></tr> <tr><td>16384</td><td>16384.</td></tr> <tr><td>20480</td><td>20480.</td></tr> <tr><td>24576</td><td>24576.</td></tr> <tr><td>28672</td><td>28672.</td></tr> <tr><td>32768</td><td>32768.</td></tr> <tr><td>36864</td><td>36864.</td></tr> <tr><td>40960</td><td>40960.</td></tr> <tr><td>45056</td><td>45056.</td></tr> <tr><td>49152</td><td>49152.</td></tr> <tr><td>53248</td><td>53248.</td></tr> <tr><td>57344</td><td>57344.</td></tr> <tr><td>61440</td><td>61440.</td></tr> </tbody> </table>	Option	Description	0	0.	4096	4096.	8192	8192.	12288	12288.	16384	16384.	20480	20480.	24576	24576.	28672	28672.	32768	32768.	36864	36864.	40960	40960.	45056	45056.	49152	49152.	53248	53248.	57344	57344.	61440	61440.			
Option	Description																																					
0	0.																																					
4096	4096.																																					
8192	8192.																																					
12288	12288.																																					
16384	16384.																																					
20480	20480.																																					
24576	24576.																																					
28672	28672.																																					
32768	32768.																																					
36864	36864.																																					
40960	40960.																																					
45056	45056.																																					
49152	49152.																																					
53248	53248.																																					
57344	57344.																																					
61440	61440.																																					

### config snmp-sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP.	<i>enable</i>	Enable SNMP.			
Option	Description									
<i>disable</i>	Disable SNMP.									
<i>enable</i>	Enable SNMP.									
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24							
description	System description.	string	Maximum length: 35							
contact-info	Contact information.	string	Maximum length: 35							
location	System location.	string	Maximum length: 35							

### config snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90

### config snmp-community

Parameter	Description	Type	Size	Default
name	SNMP community name.	string	Maximum length: 35	
status	Enable/disable this SNMP community.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP community.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP community.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP community.	<i>enable</i>	Enable SNMP community.			
Option	Description									
<i>disable</i>	Disable SNMP community.									
<i>enable</i>	Enable SNMP community.									
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v1 queries.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v1 queries.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v1 queries.	<i>enable</i>	Enable SNMP v1 queries.			
Option	Description									
<i>disable</i>	Disable SNMP v1 queries.									
<i>enable</i>	Enable SNMP v1 queries.									
query-v1-port	SNMP v1 query port .	integer	Minimum value: 0 Maximum value: 65535	161						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v2c queries.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v2c queries.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v2c queries.	<i>enable</i>	Enable SNMP v2c queries.			
Option	Description									
<i>disable</i>	Disable SNMP v2c queries.									
<i>enable</i>	Enable SNMP v2c queries.									
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535	161						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v1 traps.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v1 traps.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v1 traps.	<i>enable</i>	Enable SNMP v1 traps.			
Option	Description									
<i>disable</i>	Disable SNMP v1 traps.									
<i>enable</i>	Enable SNMP v1 traps.									
trap-v1-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162						

Parameter	Description	Type	Size	Default												
trap-v1-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162												
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v2c traps.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v2c traps.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v2c traps.	<i>enable</i>	Enable SNMP v2c traps.									
Option	Description															
<i>disable</i>	Disable SNMP v2c traps.															
<i>enable</i>	Enable SNMP v2c traps.															
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162												
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162												
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip ent-conf-change												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>cpu-high</i></td> <td>Send a trap when CPU usage too high.</td> </tr> <tr> <td><i>mem-low</i></td> <td>Send a trap when available memory is low.</td> </tr> <tr> <td><i>log-full</i></td> <td>Send a trap when log disk space becomes low.</td> </tr> <tr> <td><i>intf-ip</i></td> <td>Send a trap when an interface IP address is changed.</td> </tr> <tr> <td><i>ent-conf-change</i></td> <td>Send a trap when an entity MIB change occurs (RFC4133).</td> </tr> </tbody> </table>	Option	Description	<i>cpu-high</i>	Send a trap when CPU usage too high.	<i>mem-low</i>	Send a trap when available memory is low.	<i>log-full</i>	Send a trap when log disk space becomes low.	<i>intf-ip</i>	Send a trap when an interface IP address is changed.	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).			
Option	Description															
<i>cpu-high</i>	Send a trap when CPU usage too high.															
<i>mem-low</i>	Send a trap when available memory is low.															
<i>log-full</i>	Send a trap when log disk space becomes low.															
<i>intf-ip</i>	Send a trap when an interface IP address is changed.															
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).															

### config hosts

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

## config snmp-user

Parameter	Description	Type	Size	Default								
queries	Enable/disable SNMP queries for this user.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP queries for this user.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP queries for this user.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP queries for this user.	<i>enable</i>	Enable SNMP queries for this user.					
Option	Description											
<i>disable</i>	Disable SNMP queries for this user.											
<i>enable</i>	Enable SNMP queries for this user.											
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161								
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-auth-no-priv</i></td> <td>Message with no authentication and no privacy (encryption).</td> </tr> <tr> <td><i>auth-no-priv</i></td> <td>Message with authentication but no privacy (encryption).</td> </tr> <tr> <td><i>auth-priv</i></td> <td>Message with authentication and privacy (encryption).</td> </tr> </tbody> </table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).			
Option	Description											
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).											
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).											
<i>auth-priv</i>	Message with authentication and privacy (encryption).											
auth-proto	Authentication protocol.	option	-	sha								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>HMAC-MD5-96 authentication protocol.</td> </tr> <tr> <td><i>sha</i></td> <td>HMAC-SHA-96 authentication protocol.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	HMAC-MD5-96 authentication protocol.	<i>sha</i>	HMAC-SHA-96 authentication protocol.					
Option	Description											
<i>md5</i>	HMAC-MD5-96 authentication protocol.											
<i>sha</i>	HMAC-SHA-96 authentication protocol.											
auth-pwd	Password for authentication protocol.	password	Not Specified									
priv-proto	Privacy (encryption) protocol.	option	-	aes								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes</i></td> <td>CFB128-AES-128 symmetric encryption protocol.</td> </tr> <tr> <td><i>des</i></td> <td>CBC-DES symmetric encryption protocol.</td> </tr> </tbody> </table>	Option	Description	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	<i>des</i>	CBC-DES symmetric encryption protocol.					
Option	Description											
<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.											
<i>des</i>	CBC-DES symmetric encryption protocol.											
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified									

## config switch-log

Parameter	Description	Type	Size	Default																		
local-override	Enable to configure local logging settings that override global logging settings.	option	-	disable																		
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Override global logging settings.</td></tr><tr><td><i>disable</i></td><td>Use global logging settings.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Override global logging settings.	<i>disable</i>	Use global logging settings.															
Option	Description																					
<i>enable</i>	Override global logging settings.																					
<i>disable</i>	Use global logging settings.																					
status	Enable/disable adding FortiSwitch logs to the FortiGate event log.	option	-	enable																		
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Add FortiSwitch logs to the FortiGate event log.</td></tr><tr><td><i>disable</i></td><td>Do not add FortiSwitch logs to the FortiGate event log.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Add FortiSwitch logs to the FortiGate event log.	<i>disable</i>	Do not add FortiSwitch logs to the FortiGate event log.															
Option	Description																					
<i>enable</i>	Add FortiSwitch logs to the FortiGate event log.																					
<i>disable</i>	Do not add FortiSwitch logs to the FortiGate event log.																					
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	information																		
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></tbody></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

## config remote-log

Parameter	Description	Type	Size	Default						
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable logging by FortiSwitch device to a remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Disable logging by FortiSwitch device to a remote syslog server.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.			
Option	Description									
<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.									
<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.									

Parameter	Description	Type	Size	Default																		
server	IPv4 address of the remote syslog server.	string	Maximum length: 63																			
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514																		
severity	Severity of logs to be transferred to remote log server.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable comma-separated value (CSV) strings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable comma-separated value (CSV) strings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable comma-separated value (CSV) strings.	<i>disable</i>	Disable comma-separated value (CSV) strings.															
Option	Description																					
<i>enable</i>	Enable comma-separated value (CSV) strings.																					
<i>disable</i>	Disable comma-separated value (CSV) strings.																					
facility	Facility to log to remote syslog server.	option	-	local7																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> <tr> <td><i>auth</i></td> <td>Security/authorization messages.</td> </tr> <tr> <td><i>syslog</i></td> <td>Messages generated internally by syslogd.</td> </tr> <tr> <td><i>lpr</i></td> <td>Line printer subsystem.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslogd.	<i>lpr</i>	Line printer subsystem.					
Option	Description																					
<i>kernel</i>	Kernel messages.																					
<i>user</i>	Random user-level messages.																					
<i>mail</i>	Mail system.																					
<i>daemon</i>	System daemons.																					
<i>auth</i>	Security/authorization messages.																					
<i>syslog</i>	Messages generated internally by syslogd.																					
<i>lpr</i>	Line printer subsystem.																					

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>news</i></td> <td>Network news subsystem.</td> </tr> <tr> <td><i>uucp</i></td> <td>UUCP server messages.</td> </tr> <tr> <td><i>cron</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>authpriv</i></td> <td>Security/authorization messages (private).</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP daemon.</td> </tr> <tr> <td><i>ntp</i></td> <td>NTP daemon.</td> </tr> <tr> <td><i>audit</i></td> <td>Log audit.</td> </tr> <tr> <td><i>alert</i></td> <td>Log alert.</td> </tr> <tr> <td><i>clock</i></td> <td>Clock daemon.</td> </tr> <tr> <td><i>local0</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local1</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local2</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local3</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local4</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local5</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local6</i></td> <td>Reserved for local use.</td> </tr> <tr> <td><i>local7</i></td> <td>Reserved for local use.</td> </tr> </tbody> </table>	Option	Description	<i>news</i>	Network news subsystem.	<i>uucp</i>	UUCP server messages.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
Option	Description																																							
<i>news</i>	Network news subsystem.																																							
<i>uucp</i>	UUCP server messages.																																							
<i>cron</i>	Clock daemon.																																							
<i>authpriv</i>	Security/authorization messages (private).																																							
<i>ftp</i>	FTP daemon.																																							
<i>ntp</i>	NTP daemon.																																							
<i>audit</i>	Log audit.																																							
<i>alert</i>	Log alert.																																							
<i>clock</i>	Clock daemon.																																							
<i>local0</i>	Reserved for local use.																																							
<i>local1</i>	Reserved for local use.																																							
<i>local2</i>	Reserved for local use.																																							
<i>local3</i>	Reserved for local use.																																							
<i>local4</i>	Reserved for local use.																																							
<i>local5</i>	Reserved for local use.																																							
<i>local6</i>	Reserved for local use.																																							
<i>local7</i>	Reserved for local use.																																							

### config storm-control

Parameter	Description	Type	Size	Default						
local-override	Enable to override global FortiSwitch storm control settings for this FortiSwitch.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override global storm control settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use global storm control settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override global storm control settings.	<i>disable</i>	Use global storm control settings.			
Option	Description									
<i>enable</i>	Override global storm control settings.									
<i>disable</i>	Use global storm control settings.									
rate	Rate in packets per second at which storm traffic is controlled . Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000	500						

Parameter	Description	Type	Size	Default						
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Drop unknown unicast traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow unknown unicast traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Drop unknown unicast traffic.	<i>disable</i>	Allow unknown unicast traffic.			
Option	Description									
<i>enable</i>	Drop unknown unicast traffic.									
<i>disable</i>	Allow unknown unicast traffic.									
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Drop unknown multicast traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow unknown multicast traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Drop unknown multicast traffic.	<i>disable</i>	Allow unknown multicast traffic.			
Option	Description									
<i>enable</i>	Drop unknown multicast traffic.									
<i>disable</i>	Allow unknown multicast traffic.									
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Drop broadcast traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow broadcast traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Drop broadcast traffic.	<i>disable</i>	Allow broadcast traffic.			
Option	Description									
<i>enable</i>	Drop broadcast traffic.									
<i>disable</i>	Allow broadcast traffic.									

## config mirror

Parameter	Description	Type	Size	Default						
status	Active/inactive mirror configuration.	option	-	inactive						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>active</i></td> <td>Activate mirror configuration.</td> </tr> <tr> <td><i>inactive</i></td> <td>Deactivate mirror configuration.</td> </tr> </tbody> </table>	Option	Description	<i>active</i>	Activate mirror configuration.	<i>inactive</i>	Deactivate mirror configuration.			
Option	Description									
<i>active</i>	Activate mirror configuration.									
<i>inactive</i>	Deactivate mirror configuration.									
switching-packet	Enable/disable switching functionality when mirroring.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable switching functionality when mirroring.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable switching functionality when mirroring.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable switching functionality when mirroring.	<i>disable</i>	Disable switching functionality when mirroring.			
Option	Description									
<i>enable</i>	Enable switching functionality when mirroring.									
<i>disable</i>	Disable switching functionality when mirroring.									
dst	Destination port.	string	Maximum length: 63							
src-ingress <name>	Source ingress interfaces. Interface name.	string	Maximum length: 79							



Parameter	Description	Type	Size	Default
src-egress <name>	Source egress interfaces. Interface name.	string	Maximum length: 79	

### config static-mac

Parameter	Description	Type	Size	Default						
type	Type.	option	-	static						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Static MAC.</td> </tr> <tr> <td><i>sticky</i></td> <td>Sticky MAC.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Static MAC.	<i>sticky</i>	Sticky MAC.			
Option	Description									
<i>static</i>	Static MAC.									
<i>sticky</i>	Sticky MAC.									
vlan	Vlan.	string	Maximum length: 15							
mac	MAC address.	mac- address	Not Specified	00:00:00:00:00:00						
interface	Interface name.	string	Maximum length: 35							
description	Description.	string	Maximum length: 63							

### config custom-command

Parameter	Description	Type	Size	Default
command- name	Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller custom-command.	string	Maximum length: 35	

### config igmp-snooping

Parameter	Description	Type	Size	Default						
local-override	Enable/disable overriding the global IGMP snooping configuration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the global IGMP snooping configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the global IGMP snooping configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the global IGMP snooping configuration.	<i>disable</i>	Use the global IGMP snooping configuration.			
Option	Description									
<i>enable</i>	Override the global IGMP snooping configuration.									
<i>disable</i>	Use the global IGMP snooping configuration.									

Parameter	Description	Type	Size	Default						
aging-time	Maximum time to retain a multicast snooping entry for which no packets have been seen .	integer	Minimum value: 15 Maximum value: 3600	300						
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable unknown multicast flooding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable unknown multicast flooding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable unknown multicast flooding.	<i>disable</i>	Disable unknown multicast flooding.			
Option	Description									
<i>enable</i>	Enable unknown multicast flooding.									
<i>disable</i>	Disable unknown multicast flooding.									

### config 802-1X-settings

Parameter	Description	Type	Size	Default						
local-override	Enable to override global 802.1X settings on individual FortiSwitches.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override global 802.1X settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use global 802.1X settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override global 802.1X settings.	<i>disable</i>	Use global 802.1X settings.			
Option	Description									
<i>enable</i>	Override global 802.1X settings.									
<i>disable</i>	Use global 802.1X settings.									
link-down-auth	Authentication state to set if a link is down.	option	-	set-unauth						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>set-unauth</i></td> <td>Interface set to unauth when down. Reauthentication is needed.</td> </tr> <tr> <td><i>no-action</i></td> <td>Interface reauthentication is not needed.</td> </tr> </tbody> </table>	Option	Description	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.	<i>no-action</i>	Interface reauthentication is not needed.			
Option	Description									
<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.									
<i>no-action</i>	Interface reauthentication is not needed.									
reauth-period	Reauthentication time interval .	integer	Minimum value: 0 Maximum value: 1440	60						
max-reauth-attempt	Maximum number of authentication attempts .	integer	Minimum value: 0 Maximum value: 15	3						
tx-period	802.1X Tx period .	integer	Minimum value: 4 Maximum value: 60	30						

---

## config switch-controller switch-group

Configure FortiSwitch switch groups.

```
config switch-controller switch-group
  Description: Configure FortiSwitch switch groups.
  edit <name>
    set description {string}
    set fortilink {string}
    set members <switch-id1>, <switch-id2>, ...
  next
end
```

## config switch-controller switch-group

Parameter	Description	Type	Size	Default
description	Optional switch group description.	string	Maximum length: 63	
fortilink	FortiLink interface to which switch group members belong.	string	Maximum length: 15	
members <switch-id>	FortiSwitch members belonging to this switch group. Managed device ID.	string	Maximum length: 79	

## config switch-controller stp-settings

Configure FortiSwitch spanning tree protocol (STP).

```
config switch-controller stp-settings
  Description: Configure FortiSwitch spanning tree protocol (STP).
  set name {string}
  set revision {integer}
  set hello-time {integer}
  set forward-time {integer}
  set max-age {integer}
  set max-hops {integer}
  set pending-timer {integer}
end
```

## config switch-controller stp-settings

Parameter	Description	Type	Size	Default
name	Name of global STP settings configuration.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
revision	STP revision number .	integer	Minimum value: 0 Maximum value: 65535	0
hello-time	Period of time between successive STP frame Bridge Protocol Data Units .	integer	Minimum value: 1 Maximum value: 10	2
forward-time	Period of time a port is in listening and learning state .	integer	Minimum value: 4 Maximum value: 30	15
max-age	Maximum time before a bridge port saves its configuration BPDU information .	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops between the root bridge and the furthest bridge .	integer	Minimum value: 1 Maximum value: 40	20
pending-timer	Pending time .	integer	Minimum value: 1 Maximum value: 15	4

## config switch-controller stp-instance

Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.

```
config switch-controller stp-instance
  Description: Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.
  edit <id>
    set vlan-range <vlan-name1>, <vlan-name2>, ...
  next
end
```

## config switch-controller stp-instance

Parameter	Description	Type	Size	Default
vlan-range <vlan-name>	Configure VLAN range for STP instance. VLAN name.	string	Maximum length: 79	

## config switch-controller storm-control

Configure FortiSwitch storm control.

```
config switch-controller storm-control
  Description: Configure FortiSwitch storm control.
  set rate {integer}
  set unknown-unicast [enable|disable]
  set unknown-multicast [enable|disable]
  set broadcast [enable|disable]
end
```

## config switch-controller storm-control

Parameter	Description	Type	Size	Default						
rate	Rate in packets per second at which storm traffic is controlled . Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000	500						
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable unknown unicast storm control.</td></tr><tr><td><i>disable</i></td><td>Disable unknown unicast storm control.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable unknown unicast storm control.	<i>disable</i>	Disable unknown unicast storm control.			
Option	Description									
<i>enable</i>	Enable unknown unicast storm control.									
<i>disable</i>	Disable unknown unicast storm control.									
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable unknown multicast storm control.</td></tr><tr><td><i>disable</i></td><td>Disable unknown multicast storm control.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable unknown multicast storm control.	<i>disable</i>	Disable unknown multicast storm control.			
Option	Description									
<i>enable</i>	Enable unknown multicast storm control.									
<i>disable</i>	Disable unknown multicast storm control.									
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable broadcast storm control.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast storm control.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable broadcast storm control.	<i>disable</i>	Disable broadcast storm control.			
Option	Description									
<i>enable</i>	Enable broadcast storm control.									
<i>disable</i>	Disable broadcast storm control.									

## config switch-controller global

Configure FortiSwitch global settings.

```
config switch-controller global
  Description: Configure FortiSwitch global settings.
```

```

set mac-aging-interval {integer}
set https-image-push [enable|disable]
set vlan-all-mode [all|defined]
set vlan-optimization [enable|disable]
set disable-discovery <name1>, <name2>, ...
set mac-retention-period {integer}
set default-virtual-switch-vlan {string}
set log-mac-limit-violations [enable|disable]
set mac-violation-timer {integer}
set sn-dns-resolution [enable|disable]
set mac-event-logging [enable|disable]
set bounce-quarantined-link [disable|enable]
set quarantine-mode [by-vlan|by-redirect]
set update-user-device {option1}, {option2}, ...
config custom-command
    Description: List of custom commands to be pushed to all FortiSwitches in the VDOM.
    edit <command-entry>
        set command-name {string}
    next
end
end
end

```

## config switch-controller global

Parameter	Description	Type	Size	Default						
mac-aging-interval	Time after which an inactive MAC is aged out .	integer	Minimum value: 10 Maximum value: 1000000	300						
https-image-push	Enable/disable image push to FortiSwitch using HTTPS.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable image push to FortiSwitch using HTTPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable image push to FortiSwitch using HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable image push to FortiSwitch using HTTPS.	<i>disable</i>	Disable image push to FortiSwitch using HTTPS.			
Option	Description									
<i>enable</i>	Enable image push to FortiSwitch using HTTPS.									
<i>disable</i>	Disable image push to FortiSwitch using HTTPS.									
vlan-all-mode	VLAN configuration mode, user-defined-vlans or all-possible-vlans.	option	-	defined						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Include all possible VLANs (1-4093).</td> </tr> <tr> <td><i>defined</i></td> <td>Include user defined VLANs.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Include all possible VLANs (1-4093).	<i>defined</i>	Include user defined VLANs.			
Option	Description									
<i>all</i>	Include all possible VLANs (1-4093).									
<i>defined</i>	Include user defined VLANs.									
vlan-optimization	FortiLink VLAN optimization.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VLAN optimization on FortiSwitch units for auto-generated trunks.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VLAN optimization on FortiSwitch units for auto-generated trunks.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VLAN optimization on FortiSwitch units for auto-generated trunks.	<i>disable</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.			
Option	Description									
<i>enable</i>	Enable VLAN optimization on FortiSwitch units for auto-generated trunks.									
<i>disable</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.									
disable-discovery <name>	Prevent this FortiSwitch from discovering Managed device ID.	string	Maximum length: 79							
mac-retention-period	Time in hours after which an inactive MAC is removed from client DB (0 = aged out based on mac-aging-interval).	integer	Minimum value: 0 Maximum value: 168	24						
default-virtual-switch-vlan	Default VLAN for ports when added to the virtual-switch.	string	Maximum length: 15							
log-mac-limit-violations	Enable/disable logs for Learning Limit Violations.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Learn Limit Violation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Learn Limit Violation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Learn Limit Violation.	<i>disable</i>	Disable Learn Limit Violation.			
Option	Description									
<i>enable</i>	Enable Learn Limit Violation.									
<i>disable</i>	Disable Learn Limit Violation.									
mac-violation-timer	Set timeout for Learning Limit Violations (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0						
sn-dns-resolution	Enable/disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	<i>disable</i>	Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.			
Option	Description									
<i>enable</i>	Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.									
<i>disable</i>	Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.									
mac-event-logging	Enable/disable MAC address event logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MAC address event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MAC address event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MAC address event logging.	<i>disable</i>	Disable MAC address event logging.			
Option	Description									
<i>enable</i>	Enable MAC address event logging.									
<i>disable</i>	Disable MAC address event logging.									

Parameter	Description	Type	Size	Default												
bounce-quarantined-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last. Helps to re-initiate the DHCP process for a device.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.									
Option	Description															
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.															
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.															
quarantine-mode	Quarantine mode.	option	-	by-vlan												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>by-vlan</i></td> <td>Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.</td> </tr> <tr> <td><i>by-redirect</i></td> <td>Quarantined device traffic is redirected only to the FortiGate on the received VLAN.</td> </tr> </tbody> </table>	Option	Description	<i>by-vlan</i>	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.	<i>by-redirect</i>	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.									
Option	Description															
<i>by-vlan</i>	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.															
<i>by-redirect</i>	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.															
update-user-device	Control which sources update the device user list.	option	-	mac-cache lldp dhcp-snooping l2-db l3-db												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mac-cache</i></td> <td>Update MAC address from switch-controller mac-cache.</td> </tr> <tr> <td><i>lldp</i></td> <td>Update from FortiSwitch LLDP neighbor database.</td> </tr> <tr> <td><i>dhcp-snooping</i></td> <td>Update from FortiSwitch DHCP snooping client and server databases.</td> </tr> <tr> <td><i>l2-db</i></td> <td>Update from FortiSwitch Network-monitor Layer 2 tracking database.</td> </tr> <tr> <td><i>l3-db</i></td> <td>Update from FortiSwitch Network-monitor Layer 3 tracking database.</td> </tr> </tbody> </table>	Option	Description	<i>mac-cache</i>	Update MAC address from switch-controller mac-cache.	<i>lldp</i>	Update from FortiSwitch LLDP neighbor database.	<i>dhcp-snooping</i>	Update from FortiSwitch DHCP snooping client and server databases.	<i>l2-db</i>	Update from FortiSwitch Network-monitor Layer 2 tracking database.	<i>l3-db</i>	Update from FortiSwitch Network-monitor Layer 3 tracking database.			
Option	Description															
<i>mac-cache</i>	Update MAC address from switch-controller mac-cache.															
<i>lldp</i>	Update from FortiSwitch LLDP neighbor database.															
<i>dhcp-snooping</i>	Update from FortiSwitch DHCP snooping client and server databases.															
<i>l2-db</i>	Update from FortiSwitch Network-monitor Layer 2 tracking database.															
<i>l3-db</i>	Update from FortiSwitch Network-monitor Layer 3 tracking database.															

### config custom-command

Parameter	Description	Type	Size	Default
command-name	Name of custom command to push to all FortiSwitches in VDOM.	string	Maximum length: 35	

### config switch-controller system

Configure system-wide switch controller settings.



```

config switch-controller system
  Description: Configure system-wide switch controller settings.
  set parallel-process-override [disable|enable]
  set parallel-process {integer}
  set data-sync-interval {integer}
  set iot-weight-threshold {integer}
  set iot-scan-interval {integer}
  set iot-holdoff {integer}
  set iot-mac-idle {integer}
end

```

## config switch-controller system

Parameter	Description	Type	Size	Default						
parallel-process-override	Enable/disable parallel process override.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable maximum parallel process override.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable maximum parallel process override.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable maximum parallel process override.	<i>enable</i>	Enable maximum parallel process override.			
Option	Description									
<i>disable</i>	Disable maximum parallel process override.									
<i>enable</i>	Enable maximum parallel process override.									
parallel-process	Maximum number of parallel processes.	integer	Minimum value: 1 Maximum value: 16 **	1						
data-sync-interval	Time interval between collection of switch data .	integer	Minimum value: 30 Maximum value: 1800	60						
iot-weight-threshold	MAC entry's confidence value. Value is re-queried when below this value .	integer	Minimum value: 0 Maximum value: 255	1						
iot-scan-interval	IoT scan interval .	integer	Minimum value: 2 Maximum value: 10080	60						
iot-holdoff	MAC entry's creation time. Time must be greater than this value for an entry to be created .	integer	Minimum value: 0 Maximum value: 10080	5						

Parameter	Description	Type	Size	Default
iot-mac-idle	MAC entry's idle time. MAC entry is removed after this value .	integer	Minimum value: 0 Maximum value: 10080	1440

\*\* Values may differ between models.

## config switch-controller switch-log

Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log).

```
config switch-controller switch-log
  Description: Configure FortiSwitch logging (logs are transferred to and inserted into
  FortiGate event log).
  set status [enable|disable]
  set severity [emergency|alert|...]
end
```

## config switch-controller switch-log

Parameter	Description	Type	Size	Default																		
status	Enable/disable adding FortiSwitch logs to FortiGate event log.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Add FortiSwitch logs to FortiGate event log.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not add FortiSwitch logs to FortiGate event log.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Add FortiSwitch logs to FortiGate event log.	<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.															
Option	Description																					
<i>enable</i>	Add FortiSwitch logs to FortiGate event log.																					
<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.																					
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

## config switch-controller igmp-snooping

Configure FortiSwitch IGMP snooping global settings.

```
config switch-controller igmp-snooping
  Description: Configure FortiSwitch IGMP snooping global settings.
  set aging-time {integer}
  set flood-unknown-multicast [enable|disable]
end
```

## config switch-controller igmp-snooping

Parameter	Description	Type	Size	Default
aging-time	Maximum number of seconds to retain a multicast snooping entry for which no packets have been seen .	integer	Minimum value: 15 Maximum value: 3600	300
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable

Option	Description
<i>enable</i>	Enable unknown multicast flooding.
<i>disable</i>	Disable unknown multicast flooding.

## config switch-controller sflow

Configure FortiSwitch sFlow.

```
config switch-controller sflow
  Description: Configure FortiSwitch sFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
end
```

## config switch-controller sflow

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0
collector-port	SFlow collector port .	integer	Minimum value: 0 Maximum value: 65535	6343

## config switch-controller quarantine

Configure FortiSwitch quarantine support.

```
config switch-controller quarantine
  Description: Configure FortiSwitch quarantine support.
  set quarantine [enable|disable]
  config targets
    Description: Quarantine MACs.
    edit <mac>
      set description {string}
      set tag <tags1>, <tags2>, ...
    next
  end
end
```

## config switch-controller quarantine

Parameter	Description	Type	Size	Default						
quarantine	Enable/disable quarantine.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable quarantine.</td></tr><tr><td><i>disable</i></td><td>Disable quarantine.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable quarantine.	<i>disable</i>	Disable quarantine.			
Option	Description									
<i>enable</i>	Enable quarantine.									
<i>disable</i>	Disable quarantine.									

## config targets

Parameter	Description	Type	Size	Default
description	Description for the quarantine MAC.	string	Maximum length: 63	
tag <tags>	Tags for the quarantine MAC. Tag string(eg. string1 string2 string3).	string	Maximum length: 63	

## config switch-controller network-monitor-settings

Configure network monitor settings.

```
config switch-controller network-monitor-settings
  Description: Configure network monitor settings.
  set network-monitoring [enable|disable]
end
```

## config switch-controller network-monitor-settings

Parameter	Description	Type	Size	Default						
network-monitoring	Enable/disable passive gathering of information by FortiSwitch units concerning other network devices.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable network monitoring on FortiSwitch.</td></tr><tr><td><i>disable</i></td><td>Disable network monitoring on FortiSwitch.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable network monitoring on FortiSwitch.	<i>disable</i>	Disable network monitoring on FortiSwitch.			
Option	Description									
<i>enable</i>	Enable network monitoring on FortiSwitch.									
<i>disable</i>	Disable network monitoring on FortiSwitch.									

## config switch-controller flow-tracking

Configure FortiSwitch flow tracking and export via ipfix/netflow.

```
config switch-controller flow-tracking
  Description: Configure FortiSwitch flow tracking and export via ipfix/netflow.
  set sample-mode [local|perimeter|...]
  set sample-rate {integer}
  set format [netflow1|netflow5|...]
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set transport [udp|tcp|...]
  set level [vlan|ip|...]
  set max-export-pkt-size {integer}
  set timeout-general {integer}
  set timeout-icmp {integer}
  set timeout-max {integer}
  set timeout-tcp {integer}
  set timeout-tcp-fin {integer}
  set timeout-tcp-rst {integer}
  set timeout-udp {integer}
config aggregates
  Description: Configure aggregates in which all traffic sessions matching the IP
  Address will be grouped into the same flow.
  edit <id>
    set ip {ipv4-classnet}
  next
end
end
```

## config switch-controller flow-tracking

Parameter	Description	Type	Size	Default
sample-mode	Configure sample mode for the flow tracking.	option	-	perimeter

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>local</i></td> <td>Set local mode which samples on the specific switch port.</td> </tr> <tr> <td><i>perimeter</i></td> <td>Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.</td> </tr> <tr> <td><i>device-ingress</i></td> <td>Set device -ingress mode which samples across all switch ports at the ingress.</td> </tr> </tbody> </table>	Option	Description	<i>local</i>	Set local mode which samples on the specific switch port.	<i>perimeter</i>	Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.	<i>device-ingress</i>	Set device -ingress mode which samples across all switch ports at the ingress.							
Option	Description															
<i>local</i>	Set local mode which samples on the specific switch port.															
<i>perimeter</i>	Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.															
<i>device-ingress</i>	Set device -ingress mode which samples across all switch ports at the ingress.															
sample-rate	Configure sample rate for the perimeter and device-ingress sampling.	integer	Minimum value: 0 Maximum value: 99999	512												
format	Configure flow tracking protocol.	option	-	netflow9												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>netflow1</i></td> <td>Netflow version 1 sampling.</td> </tr> <tr> <td><i>netflow5</i></td> <td>Netflow version 5 sampling.</td> </tr> <tr> <td><i>netflow9</i></td> <td>Netflow version 9 sampling.</td> </tr> <tr> <td><i>ipfix</i></td> <td>Ipfix sampling.</td> </tr> </tbody> </table>	Option	Description	<i>netflow1</i>	Netflow version 1 sampling.	<i>netflow5</i>	Netflow version 5 sampling.	<i>netflow9</i>	Netflow version 9 sampling.	<i>ipfix</i>	Ipfix sampling.					
Option	Description															
<i>netflow1</i>	Netflow version 1 sampling.															
<i>netflow5</i>	Netflow version 5 sampling.															
<i>netflow9</i>	Netflow version 9 sampling.															
<i>ipfix</i>	Ipfix sampling.															
collector-ip	Configure collector ip address.	ipv4-address	Not Specified	0.0.0.0												
collector-port	Configure collector port number.	integer	Minimum value: 0 Maximum value: 65535	0												
transport	Configure L4 transport protocol for exporting packets.	option	-	udp												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>UDP protocol.</td> </tr> <tr> <td><i>tcp</i></td> <td>TCP protocol.</td> </tr> <tr> <td><i>sctp</i></td> <td>SCTP protocol.</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	UDP protocol.	<i>tcp</i>	TCP protocol.	<i>sctp</i>	SCTP protocol.							
Option	Description															
<i>udp</i>	UDP protocol.															
<i>tcp</i>	TCP protocol.															
<i>sctp</i>	SCTP protocol.															
level	Configure flow tracking level.	option	-	ip												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>vlan</i></td> <td>Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.</td> </tr> <tr> <td><i>ip</i></td> <td>Collects srcip/dstip from the sample packet.</td> </tr> <tr> <td><i>port</i></td> <td>Collects srcip/dstip/srcport/dstport/protocol from the sample packet.</td> </tr> <tr> <td><i>proto</i></td> <td>Collects srcip/dstip/protocol from the sample packet.</td> </tr> <tr> <td><i>mac</i></td> <td>Collects smac/dmac from the sample packet.</td> </tr> </tbody> </table>	Option	Description	<i>vlan</i>	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.	<i>ip</i>	Collects srcip/dstip from the sample packet.	<i>port</i>	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.	<i>proto</i>	Collects srcip/dstip/protocol from the sample packet.	<i>mac</i>	Collects smac/dmac from the sample packet.			
Option	Description															
<i>vlan</i>	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.															
<i>ip</i>	Collects srcip/dstip from the sample packet.															
<i>port</i>	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.															
<i>proto</i>	Collects srcip/dstip/protocol from the sample packet.															
<i>mac</i>	Collects smac/dmac from the sample packet.															

Parameter	Description	Type	Size	Default
max-export-pkt-size	Configure flow max export packet size .	integer	Minimum value: 512 512 Maximum value: 9216	512
timeout-general	Configure flow session general timeout .	integer	Minimum value: 60 Maximum value: 604800	3600
timeout-icmp	Configure flow session ICMP timeout .	integer	Minimum value: 60 Maximum value: 604800	300
timeout-max	Configure flow session max timeout .	integer	Minimum value: 60 Maximum value: 604800	604800
timeout-tcp	Configure flow session TCP timeout .	integer	Minimum value: 60 Maximum value: 604800	3600
timeout-tcp-fin	Configure flow session TCP FIN timeout .	integer	Minimum value: 60 Maximum value: 604800	300
timeout-tcp-rst	Configure flow session TCP RST timeout .	integer	Minimum value: 60 Maximum value: 604800	120
timeout-udp	Configure flow session UDP timeout .	integer	Minimum value: 60 Maximum value: 604800	300

## config aggregates

Parameter	Description	Type	Size	Default
ip	IP address to group all matching traffic sessions to a flow.	ipv4-classnet	Not Specified	0.0.0.0

## config switch-controller snmp-sysinfo

Configure FortiSwitch SNMP system information globally.

```

config switch-controller snmp-sysinfo
  Description: Configure FortiSwitch SNMP system information globally.
  set status [disable|enable]
  set engine-id {string}
  set description {string}
  set contact-info {string}
  set location {string}
end

```

## config switch-controller snmp-sysinfo

Parameter	Description	Type	Size	Default						
status	Enable/disable SNMP.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable SNMP.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable SNMP.	<i>enable</i>	Enable SNMP.			
Option	Description									
<i>disable</i>	Disable SNMP.									
<i>enable</i>	Enable SNMP.									
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24							
description	System description.	string	Maximum length: 35							
contact-info	Contact information.	string	Maximum length: 35							
location	System location.	string	Maximum length: 35							

## config switch-controller snmp-trap-threshold

Configure FortiSwitch SNMP trap threshold values globally.

```
config switch-controller snmp-trap-threshold
  Description: Configure FortiSwitch SNMP trap threshold values globally.
  set trap-high-cpu-threshold {integer}
  set trap-low-memory-threshold {integer}
  set trap-log-full-threshold {integer}
end
```

## config switch-controller snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80



Parameter	Description	Type	Size	Default
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90

## config switch-controller snmp-community

Configure FortiSwitch SNMP v1/v2c communities globally.

```
config switch-controller snmp-community
  Description: Configure FortiSwitch SNMP v1/v2c communities globally.
  edit <id>
    set name {string}
    set status [disable|enable]
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ip {user}
      next
    end
    set query-v1-status [disable|enable]
    set query-v1-port {integer}
    set query-v2c-status [disable|enable]
    set query-v2c-port {integer}
    set trap-v1-status [disable|enable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v2c-status [disable|enable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set events {option1}, {option2}, ...
  next
end
```

## config switch-controller snmp-community

Parameter	Description	Type	Size	Default						
name	SNMP community name.	string	Maximum length: 35							
status	Enable/disable this SNMP community.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP community.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP community.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP community.	<i>enable</i>	Enable SNMP community.			
Option	Description									
<i>disable</i>	Disable SNMP community.									
<i>enable</i>	Enable SNMP community.									

Parameter	Description	Type	Size	Default						
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v1 queries.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v1 queries.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v1 queries.	<i>enable</i>	Enable SNMP v1 queries.			
Option	Description									
<i>disable</i>	Disable SNMP v1 queries.									
<i>enable</i>	Enable SNMP v1 queries.									
query-v1-port	SNMP v1 query port .	integer	Minimum value: 0 Maximum value: 65535	161						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v2c queries.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v2c queries.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v2c queries.	<i>enable</i>	Enable SNMP v2c queries.			
Option	Description									
<i>disable</i>	Disable SNMP v2c queries.									
<i>enable</i>	Enable SNMP v2c queries.									
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535	161						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v1 traps.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v1 traps.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v1 traps.	<i>enable</i>	Enable SNMP v1 traps.			
Option	Description									
<i>disable</i>	Disable SNMP v1 traps.									
<i>enable</i>	Enable SNMP v1 traps.									
trap-v1-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162						
trap-v1-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162						
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP v2c traps.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP v2c traps.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP v2c traps.	<i>enable</i>	Enable SNMP v2c traps.									
Option	Description															
<i>disable</i>	Disable SNMP v2c traps.															
<i>enable</i>	Enable SNMP v2c traps.															
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162												
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162												
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip ent-conf-change												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>cpu-high</i></td> <td>Send a trap when CPU usage too high.</td> </tr> <tr> <td><i>mem-low</i></td> <td>Send a trap when available memory is low.</td> </tr> <tr> <td><i>log-full</i></td> <td>Send a trap when log disk space becomes low.</td> </tr> <tr> <td><i>intf-ip</i></td> <td>Send a trap when an interface IP address is changed.</td> </tr> <tr> <td><i>ent-conf-change</i></td> <td>Send a trap when an entity MIB change occurs (RFC4133).</td> </tr> </tbody> </table>	Option	Description	<i>cpu-high</i>	Send a trap when CPU usage too high.	<i>mem-low</i>	Send a trap when available memory is low.	<i>log-full</i>	Send a trap when log disk space becomes low.	<i>intf-ip</i>	Send a trap when an interface IP address is changed.	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).			
Option	Description															
<i>cpu-high</i>	Send a trap when CPU usage too high.															
<i>mem-low</i>	Send a trap when available memory is low.															
<i>log-full</i>	Send a trap when log disk space becomes low.															
<i>intf-ip</i>	Send a trap when an interface IP address is changed.															
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).															

## config hosts

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

## config switch-controller snmp-user

Configure FortiSwitch SNMP v3 users globally.

```
config switch-controller snmp-user
  Description: Configure FortiSwitch SNMP v3 users globally.
  edit <name>
    set queries [disable|enable]
    set query-port {integer}
```

```

set security-level [no-auth-no-priv|auth-no-priv|...]
set auth-proto [md5|sha]
set auth-pwd {password}
set priv-proto [aes|des]
set priv-pwd {password}
next
end

```

## config switch-controller snmp-user

Parameter	Description	Type	Size	Default								
queries	Enable/disable SNMP queries for this user.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SNMP queries for this user.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SNMP queries for this user.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SNMP queries for this user.	<i>enable</i>	Enable SNMP queries for this user.					
Option	Description											
<i>disable</i>	Disable SNMP queries for this user.											
<i>enable</i>	Enable SNMP queries for this user.											
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161								
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-auth-no-priv</i></td> <td>Message with no authentication and no privacy (encryption).</td> </tr> <tr> <td><i>auth-no-priv</i></td> <td>Message with authentication but no privacy (encryption).</td> </tr> <tr> <td><i>auth-priv</i></td> <td>Message with authentication and privacy (encryption).</td> </tr> </tbody> </table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).			
Option	Description											
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).											
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).											
<i>auth-priv</i>	Message with authentication and privacy (encryption).											
auth-proto	Authentication protocol.	option	-	sha								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>HMAC-MD5-96 authentication protocol.</td> </tr> <tr> <td><i>sha</i></td> <td>HMAC-SHA-96 authentication protocol.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	HMAC-MD5-96 authentication protocol.	<i>sha</i>	HMAC-SHA-96 authentication protocol.					
Option	Description											
<i>md5</i>	HMAC-MD5-96 authentication protocol.											
<i>sha</i>	HMAC-SHA-96 authentication protocol.											
auth-pwd	Password for authentication protocol.	password	Not Specified									
priv-proto	Privacy (encryption) protocol.	option	-	aes								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes</i></td> <td>CFB128-AES-128 symmetric encryption protocol.</td> </tr> <tr> <td><i>des</i></td> <td>CBC-DES symmetric encryption protocol.</td> </tr> </tbody> </table>	Option	Description	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	<i>des</i>	CBC-DES symmetric encryption protocol.					
Option	Description											
<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.											
<i>des</i>	CBC-DES symmetric encryption protocol.											

Parameter	Description	Type	Size	Default
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

## config switch-controller traffic-sniffer

Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.

```

config switch-controller traffic-sniffer
  Description: Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.
  set mode [erspan-auto|rspan|...]
  set erspan-ip {ipv4-address}
  config target-mac
    Description: Sniffer MACs to filter.
    edit <mac>
      set description {string}
    next
  end
  config target-ip
    Description: Sniffer IPs to filter.
    edit <ip>
      set description {string}
    next
  end
  config target-port
    Description: Sniffer ports to filter.
    edit <switch-id>
      set description {string}
      set in-ports <name1>, <name2>, ...
      set out-ports <name1>, <name2>, ...
    next
  end
end
end

```

## config switch-controller traffic-sniffer

Parameter	Description	Type	Size	Default								
mode	Configure traffic sniffer mode.	option	-	erspan-auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>erspan-auto</i></td> <td>Mirror traffic using a GRE tunnel.</td> </tr> <tr> <td><i>rspan</i></td> <td>Mirror traffic on a layer2 VLAN.</td> </tr> <tr> <td><i>none</i></td> <td>Disable traffic mirroring (sniffer).</td> </tr> </tbody> </table>	Option	Description	<i>erspan-auto</i>	Mirror traffic using a GRE tunnel.	<i>rspan</i>	Mirror traffic on a layer2 VLAN.	<i>none</i>	Disable traffic mirroring (sniffer).			
Option	Description											
<i>erspan-auto</i>	Mirror traffic using a GRE tunnel.											
<i>rspan</i>	Mirror traffic on a layer2 VLAN.											
<i>none</i>	Disable traffic mirroring (sniffer).											
erspan-ip	Configure ERSPAN collector IP address.	ipv4-address	Not Specified	0.0.0.0								

## config target-mac

Parameter	Description	Type	Size	Default
description	Description for the sniffer MAC.	string	Maximum length: 63	

## config target-ip

Parameter	Description	Type	Size	Default
description	Description for the sniffer IP.	string	Maximum length: 63	

## config target-port

Parameter	Description	Type	Size	Default
description	Description for the sniffer port entry.	string	Maximum length: 63	
in-ports <name>	Configure source ingress port interfaces. Interface name.	string	Maximum length: 79	
out-ports <name>	Configure source egress port interfaces. Interface name.	string	Maximum length: 79	

## config switch-controller remote-log

Configure logging by FortiSwitch device to a remote syslog server.

```
config switch-controller remote-log
  Description: Configure logging by FortiSwitch device to a remote syslog server.
  edit <name>
    set status [enable|disable]
    set server {string}
    set port {integer}
    set severity [emergency|alert|...]
    set csv [enable|disable]
    set facility [kernel|user|...]
  next
end
```

## config switch-controller remote-log

Parameter	Description	Type	Size	Default
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging by FortiSwitch device to a remote syslog server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging by FortiSwitch device to a remote syslog server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.															
Option	Description																					
<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.																					
<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.																					
server	IPv4 address of the remote syslog server.	string	Maximum length: 63																			
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514																		
severity	Severity of logs to be transferred to remote log server.	option	-	information																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable comma-separated value (CSV) strings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable comma-separated value (CSV) strings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable comma-separated value (CSV) strings.	<i>disable</i>	Disable comma-separated value (CSV) strings.															
Option	Description																					
<i>enable</i>	Enable comma-separated value (CSV) strings.																					
<i>disable</i>	Disable comma-separated value (CSV) strings.																					
facility	Facility to log to remote syslog server.	option	-	local7																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kernel</i></td> <td>Kernel messages.</td> </tr> <tr> <td><i>user</i></td> <td>Random user-level messages.</td> </tr> <tr> <td><i>mail</i></td> <td>Mail system.</td> </tr> <tr> <td><i>daemon</i></td> <td>System daemons.</td> </tr> </tbody> </table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.											
Option	Description																					
<i>kernel</i>	Kernel messages.																					
<i>user</i>	Random user-level messages.																					
<i>mail</i>	Mail system.																					
<i>daemon</i>	System daemons.																					

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslogd.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	UUCP server messages.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		
	<i>local4</i>	Reserved for local use.		
	<i>local5</i>	Reserved for local use.		
	<i>local6</i>	Reserved for local use.		
	<i>local7</i>	Reserved for local use.		

## config switch-controller vlan-policy

Configure VLAN policy to be applied on the managed FortiSwitch ports through port-policy.

```

config switch-controller vlan-policy
  Description: Configure VLAN policy to be applied on the managed FortiSwitch ports through
  port-policy.
  edit <name>
    set description {string}
    set fortilink {string}
    set vlan {string}
    set allowed-vlans <vlan-name1>, <vlan-name2>, ...
    set untagged-vlans <vlan-name1>, <vlan-name2>, ...
    set allowed-vlans-all [enable|disable]
    set discard-mode [none|all-untagged|...]
  next

```



end

## config switch-controller vlan-policy

Parameter	Description	Type	Size	Default								
description	Description for the VLAN policy.	string	Maximum length: 63									
fortilink	FortiLink interface for which this VLAN policy belongs to.	string	Maximum length: 15									
vlan	Native VLAN to be applied when using this VLAN policy.	string	Maximum length: 15									
allowed-vlans <vlan-name>	Allowed VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79									
untagged-vlans <vlan-name>	Untagged VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79									
allowed-vlans-all	Enable/disable all defined VLANs when using this VLAN policy.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable all defined VLANs.</td></tr><tr><td><i>disable</i></td><td>Disable all defined VLANs.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable all defined VLANs.	<i>disable</i>	Disable all defined VLANs.					
Option	Description											
<i>enable</i>	Enable all defined VLANs.											
<i>disable</i>	Disable all defined VLANs.											
discard-mode	Discard mode to be applied when using this VLAN policy.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>Discard disabled.</td></tr><tr><td><i>all-untagged</i></td><td>Discard all frames that are untagged.</td></tr><tr><td><i>all-tagged</i></td><td>Discard all frames that are tagged.</td></tr></tbody></table>	Option	Description	<i>none</i>	Discard disabled.	<i>all-untagged</i>	Discard all frames that are untagged.	<i>all-tagged</i>	Discard all frames that are tagged.			
Option	Description											
<i>none</i>	Discard disabled.											
<i>all-untagged</i>	Discard all frames that are untagged.											
<i>all-tagged</i>	Discard all frames that are tagged.											

## config switch-controller port-policy

Configure port policy to be applied on the managed FortiSwitch ports through NAC device.

```
config switch-controller port-policy
  Description: Configure port policy to be applied on the managed FortiSwitch ports through
  NAC device.
  edit <name>
    set description {string}
    set fortilink {string}
    set lldp-profile {string}
    set qos-policy {string}
```

```

    set 802-1x {string}
    set vlan-policy {string}
    set bounce-port-link [disable|enable]
  next
end

```

## config switch-controller port-policy

Parameter	Description	Type	Size	Default
description	Description for the port policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this port policy belongs to.	string	Maximum length: 15	
lldp-profile	LLDP profile to be applied when using this port-policy.	string	Maximum length: 63	
qos-policy	QoS policy to be applied when using this port-policy.	string	Maximum length: 63	
802-1x	802.1x security policy to be applied when using this port-policy.	string	Maximum length: 31	
vlan-policy	VLAN policy to be applied when using this port-policy.	string	Maximum length: 63	
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this port policy is applied. Helps to clear and reassign VLAN from lldp-profile.	option	-	enable

Option	Description
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this port policy is applied.
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this port policy is applied.

## config switch-controller mac-policy

Configure MAC policy to be applied on the managed FortiSwitch devices through NAC device.

```

config switch-controller mac-policy
  Description: Configure MAC policy to be applied on the managed FortiSwitch devices
              through NAC device.
  edit <name>
    set description {string}
    set fortilink {string}
    set vlan {string}
    set traffic-policy {string}
    set count [disable|enable]
  end
end

```

```
next
end
```

## config switch-controller mac-policy

Parameter	Description	Type	Size	Default
description	Description for the MAC policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this MAC policy belongs to.	string	Maximum length: 15	
vlan	Ingress traffic VLAN assignment for the MAC address matching this MAC policy.	string	Maximum length: 15	
traffic-policy	Traffic policy to be applied when using this MAC policy.	string	Maximum length: 63	
count	Enable/Disable packet count on the NAC device.	option	-	disable

Option	Description
<i>disable</i>	Enable packet count on the NAC device.
<i>enable</i>	Disable packet count on the NAC device.

## config switch-controller nac-device

Configure/list NAC devices learned on the managed FortiSwitch ports which matches NAC policy.

```
config switch-controller nac-device
  Description: Configure/list NAC devices learned on the managed FortiSwitch ports which
              matches NAC policy.
  edit <id>
    set description {string}
    set status [enable|disable]
    set mac {mac-address}
    set last-known-switch {string}
    set last-known-port {string}
    set matched-nac-policy {string}
    set port-policy {string}
    set mac-policy {string}
    set last-seen {integer}
  next
end
```

## config switch-controller nac-device

Parameter	Description	Type	Size	Default						
description	Description for the learned NAC device.	string	Maximum length: 127							
status	Status of the learned NAC device. Set enable to authorize the NAC device.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the NAC device.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the NAC device.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the NAC device.	<i>disable</i>	Disable the NAC device.			
Option	Description									
<i>enable</i>	Enable the NAC device.									
<i>disable</i>	Disable the NAC device.									
mac	MAC address of the learned NAC device.	mac-address	Not Specified	00:00:00:00:00:00						
last-known-switch	Managed FortiSwitch where NAC device is last learned.	string	Maximum length: 63							
last-known-port	Managed FortiSwitch port where NAC device is last learned.	string	Maximum length: 35							
matched-nac-policy	Matched NAC policy for the learned NAC device.	string	Maximum length: 63							
port-policy	Port policy to be applied on this learned NAC device.	string	Maximum length: 63							
mac-policy	MAC policy to be applied on this learned NAC device.	string	Maximum length: 63							
last-seen	Device last seen.	integer	Minimum value: 0 Maximum value: 4294967295	0						

# system

This section includes syntax for the following commands:

- [config system vdom-netflow on page 921](#)
- [config system resource-limits on page 1026](#)
- [config system ipsec-aggregate on page 1014](#)
- [config system nat64 on page 1091](#)
- [config system replacemsg mail on page 924](#)
- [config system probe-response on page 1077](#)
- [config system fortiguard-log-service on page 989](#)
- [config system gre-tunnel on page 1011](#)
- [config system sflow on page 918](#)
- [config system cmdb on page 988](#)
- [config system password-policy-guest-admin on page 862](#)
- [config system ipip-tunnel on page 1014](#)
- [config system ha on page 899](#)
- [config system lte-modem on page 809](#)
- [config system saml on page 1115](#)
- [config system geneve on page 1021](#)
- [config system replacemsg traffic-quota on page 933](#)
- [config system sms-server on page 864](#)
- [config system link-monitor on page 1078](#)
- [config system replacemsg spam on page 929](#)
- [config system automation-trigger on page 1104](#)
- [config system geoip-override on page 1096](#)
- [config system startup-error-log on page 1094](#)
- [config system alarm on page 1070](#)
- [config system alias on page 989](#)
- [config system mobile-tunnel on page 1015](#)
- [config system dns-server on page 1025](#)
- [config system replacemsg alertmail on page 929](#)
- [config system info admin ssh on page 990](#)
- [config system api-user on page 871](#)
- [config system ipv6-tunnel on page 1006](#)
- [config system autoupdate push-update on page 960](#)
- [config system fortiguard on page 1061](#)
- [config system global on page 761](#)
- [config system auto-update status on page 1094](#)
- [config system vdom-sflow on page 919](#)
- [config system fips-cc on page 1075](#)
- [config system dscp-based-priority on page 1077](#)
- [config system session-info ttl on page 1095](#)

- 
- [config system sdwan on page 1030](#)
  - [config system session-info list on page 1094](#)
  - [config system object-tagging on page 808](#)
  - [config system replacemsg ftp on page 927](#)
  - [config system netflow on page 920](#)
  - [config system vdom-dns on page 922](#)
  - [config system session6 on page 987](#)
  - [config system replacemsg webproxy on page 926](#)
  - [config system replacemsg admin on page 930](#)
  - [config system auto-update versions on page 1094](#)
  - [config system mac-address-table on page 1073](#)
  - [config system admin on page 865](#)
  - [config system replacemsg utm on page 934](#)
  - [config system ntp on page 1084](#)
  - [config system vdom on page 760](#)
  - [config system ha-nonsync-csum on page 988](#)
  - [config system sit-tunnel on page 892](#)
  - [config system ptp on page 1087](#)
  - [config system fortianalyzer-connectivity on page 988](#)
  - [config system ftm-push on page 1095](#)
  - [config system replacemsg sslvpn on page 932](#)
  - [config system cluster-sync on page 1058](#)
  - [config system ha-monitor on page 909](#)
  - [config system virtual-wire-pair on page 1022](#)
  - [config system pppoe-interface on page 1017](#)
  - [config system snmp sysinfo on page 946](#)
  - [config system accprofile on page 796](#)
  - [config system fortisandbox on page 1097](#)
  - [config system performance top on page 987](#)
  - [config system replacemsg auth on page 931](#)
  - [config system central-mgmt on page 989](#)
  - [config system ipv6-neighbor-cache on page 913](#)
  - [config system replacemsg fortiguard-wf on page 928](#)
  - [config system vxlan on page 1019](#)
  - [config system session-helper-info list on page 1095](#)
  - [config system replacemsg-image on page 924](#)
  - [config system session-info statistics on page 1095](#)
  - [config system vne-tunnel on page 1118](#)
  - [config system custom-language on page 864](#)
  - [config system virtual-switch on page 857](#)
  - [config system ips-urlfilter-dns on page 1009](#)
  - [config system vdom-radius-server on page 1093](#)
  - [config system vdom-exception on page 1099](#)
  - [config system external-resource on page 1007](#)
  - [config system replacemsg nac-quar on page 933](#)

- 
- [config system csf on page 1100](#)
  - [config system checksum status on page 988](#)
  - [config system wccp on page 1088](#)
  - [config system session on page 987](#)
  - [config system switch-interface on page 806](#)
  - [config system npu on page 893](#)
  - [config system vdom-property on page 1028](#)
  - [config system replacemsg http on page 925](#)
  - [config system ddns on page 915](#)
  - [config system performance firewall packet-distribution on page 987](#)
  - [config system nd-proxy on page 1114](#)
  - [config system console on page 1083](#)
  - [config system performance firewall statistics on page 987](#)
  - [config system central-management on page 994](#)
  - [config system replacemsg icap on page 935](#)
  - [config system dhcp6 server on page 975](#)
  - [config system performance status on page 986](#)
  - [config system password-policy on page 860](#)
  - [config system ips-urlfilter-dns6 on page 1009](#)
  - [config system vdom-link on page 805](#)
  - [config system lldp network-policy on page 1050](#)
  - [config system auto-install on page 1082](#)
  - [config system session-info full-stat on page 1095](#)
  - [config system ips on page 1067](#)
  - [config system session-ttl on page 963](#)
  - [config system dns-database on page 1022](#)
  - [config system session-info expectation on page 1094](#)
  - [config system replacemsg-group on page 936](#)
  - [config system dhcp server on page 964](#)
  - [config system snmp user on page 954](#)
  - [config system 3g-modem custom on page 985](#)
  - [config system email-server on page 1068](#)
  - [config system zone on page 999](#)
  - [config system tos-based-priority on page 1076](#)
  - [config system network-visibility on page 1010](#)
  - [config system autoupdate schedule on page 961](#)
  - [config system fortiguard-service on page 988](#)
  - [config system dedicated-mgmt on page 911](#)
  - [config system settings on page 873](#)
  - [config system snmp community on page 947](#)
  - [config system automation-destination on page 1113](#)
  - [config system proxy-arp on page 1074](#)
  - [config system speed-test-server on page 1049](#)
  - [config system arp on page 1068](#)
  - [config system fm on page 993](#)

- [config system info admin status on page 990](#)
- [config system fsso-polling on page 898](#)
- [config system session-helper on page 1073](#)
- [config system sso-admin on page 873](#)
- [config system fortimanager on page 992](#)
- [config system interface on page 811](#)
- [config system stp on page 858](#)
- [config system geoip-country on page 1000](#)
- [config system arp-table on page 912](#)
- [config system standalone-cluster on page 1057](#)
- [config system auto-script on page 989](#)
- [config system source-ip status on page 1094](#)
- [config system management-tunnel on page 991](#)
- [config system dns on page 913](#)
- [config system physical-switch on page 856](#)
- [config system status on page 986](#)
- [config system ip-conflict status on page 1095](#)
- [config system storage on page 910](#)
- [config system sdn-connector on page 1000](#)
- [config system modem on page 978](#)
- [config system mgmt-csum on page 988](#)
- [config system autoupdate tunneling on page 962](#)
- [config system automation-stitch on page 1113](#)
- [config system automation-action on page 1107](#)

## config system vdom

Configure virtual domain.

```
config system vdom
  Description: Configure virtual domain.
  edit <name>
    set short-name {string}
    set vcluster-id {integer}
    set flag {integer}
  next
end
```

## config system vdom

Parameter	Description	Type	Size	Default
short-name	VDOM short name.	string	Maximum length: 11	



Parameter	Description	Type	Size	Default
vcluster-id	Virtual cluster ID .	integer	Minimum value: 0 Maximum value: 4294967295	0
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config system global

Configure global attributes.

```

config system global
  Description: Configure global attributes.
  set language [english|french|...]
  set gui-ipv6 [enable|disable]
  set gui-certificates [enable|disable]
  set gui-custom-language [enable|disable]
  set gui-wireless-opensecurity [enable|disable]
  set gui-display-hostname [enable|disable]
  set gui-fortisandbox-cloud [enable|disable]
  set gui-firmware-upgrade-warning [enable|disable]
  set gui-allow-default-hostname [enable|disable]
  set gui-forticare-registration-setup-warning [enable|disable]
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admintimeout {integer}
  set admin-console-timeout {integer}
  set admin-concurrent [enable|disable]
  set admin-lockout-threshold {integer}
  set admin-lockout-duration {integer}
  set refresh {integer}
  set interval {integer}
  set failtime {integer}
  set daily-restart [enable|disable]
  set restart-time {user}
  set radius-port {integer}
  set admin-login-max {integer}
  set remoteauthtimeout {integer}
  set ldapconntimeout {integer}
  set batch-cmdb [enable|disable]
  set multi-factor-authentication [optional|mandatory]
  set ssl-min-proto-version [SSLv3|TLSv1|...]
  set autorun-log-fsck [enable|disable]
  set dst [enable|disable]
  set timezone [01|02|...]
  set traffic-priority [tos|dscp]
  set traffic-priority-level [low|medium|...]
  set anti-replay [disable|loose|...]
  set send-pmtu-icmp [enable|disable]

```

---

```
set honor-df [enable|disable]
set pmtu-discovery [enable|disable]
set revision-image-auto-backup [enable|disable]
set revision-backup-on-logout [enable|disable]
set management-vdom {string}
set hostname {string}
set alias {string}
set strong-crypto [enable|disable]
set ssh-cbc-cipher [enable|disable]
set ssh-hmac-md5 [enable|disable]
set ssh-kex-sha1 [enable|disable]
set ssh-mac-weak [enable|disable]
set ssl-static-key-ciphers [enable|disable]
set snat-route-change [enable|disable]
set cli-audit-log [enable|disable]
set dh-params [1024|1536|...]
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set tcp-option [enable|disable]
set lldp-transmission [enable|disable]
set lldp-reception [enable|disable]
set proxy-auth-timeout {integer}
set proxy-re-authentication-mode [session|traffic|...]
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
set sys-perf-log-interval {integer}
set check-protocol-header [loose|strict]
set vip-arp-range [unlimited|restricted]
set reset-sessionless-tcp [enable|disable]
set allow-traffic-redirect [enable|disable]
set strict-dirty-session-check [enable|disable]
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-timewait-timer {integer}
set udp-idle-timer {integer}
set block-session-timer {integer}
set ip-src-port-range {user}
set pre-login-banner [enable|disable]
set post-login-banner [disable|enable]
set tftp [enable|disable]
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set memory-use-threshold-extreme {integer}
set memory-use-threshold-red {integer}
set memory-use-threshold-green {integer}
set cpu-use-threshold {integer}
set check-reset-range [strict|disable]
set vdom-mode [no-vdom|split-vdom|...]
set long-vdom-name [enable|disable]
set edit-vdom-prompt [enable|disable]
set admin-port {integer}
set admin-sport {integer}
set admin-https-redirect [enable|disable]
set admin-hsts-max-age {integer}
set admin-ssh-password [enable|disable]
set admin-restrict-local [enable|disable]
set admin-ssh-port {integer}
```

---

```
set admin-ssh-grace-time {integer}
set admin-ssh-v1 [enable|disable]
set admin-telnet [enable|disable]
set admin-telnet-port {integer}
set default-service-source-port {user}
set admin-maintainer [enable|disable]
set admin-reset-button [enable|disable]
set admin-server-cert {string}
set user-server-cert {string}
set admin-https-pki-required [enable|disable]
set wifi-certificate {string}
set wifi-ca-certificate {string}
set auth-http-port {integer}
set auth-https-port {integer}
set auth-keepalive [enable|disable]
set policy-auth-concurrent {integer}
set auth-session-limit [block-new|logout-inactive]
set auth-cert {string}
set clt-cert-req [enable|disable]
set fortiservice-port {integer}
set cfg-save [automatic|manual|...]
set cfg-revert-timeout {integer}
set reboot-upon-config-restore [enable|disable]
set admin-scp [enable|disable]
set security-rating-result-submission [enable|disable]
set security-rating-run-on-schedule [enable|disable]
set wireless-controller [enable|disable]
set wireless-controller-port {integer}
set fortiextender-data-port {integer}
set fortiextender [disable|enable]
set fortiextender-vlan-mode [enable|disable]
set switch-controller [disable|enable]
set switch-controller-reserved-network {ipv4-classnet}
set dnsproxy-worker-count {integer}
set url-filter-count {integer}
set proxy-worker-count {integer}
set scanunit-count {integer}
set proxy-hardware-acceleration [disable|enable]
set fgd-alert-subscription {option1}, {option2}, ...
set ipsec-hmac-offload [enable|disable]
set ipv6-accept-dad {integer}
set ipv6-allow-anycast-probe [enable|disable]
set csr-ca-attribute [enable|disable]
set wimax-4g-usb [enable|disable]
set cert-chain-max {integer}
set sslvpn-max-worker-count {integer}
set sslvpn-kxp-hardware-acceleration [enable|disable]
set sslvpn-cipher-hardware-acceleration [enable|disable]
set sslvpn-ems-sn-check [enable|disable]
set sslvpn-plugin-version-check [enable|disable]
set two-factor-ftk-expiry {integer}
set two-factor-email-expiry {integer}
set two-factor-sms-expiry {integer}
set two-factor-fac-expiry {integer}
set two-factor-ftm-expiry {integer}
set wad-worker-count {integer}
set wad-csvc-cs-count {integer}
```

```

set wad-csvc-db-count {integer}
set wad-source-affinity [disable|enable]
set wad-memory-change-granularity {integer}
set login-timestamp [enable|disable]
set miglogd-children {integer}
set special-file-23-support [disable|enable]
set log-uuid-address [enable|disable]
set log-ssl-connection [enable|disable]
set arp-max-entry {integer}
set ndp-max-entry {integer}
set br-fdb-max-entry {integer}
set max-route-cache-size {integer}
set ipsec-asic-offload [enable|disable]
set ipsec-soft-dec-async [enable|disable]
set device-idle-timeout {integer}
set user-device-store-max-devices {integer}
set user-device-store-max-users {integer}
set gui-device-latitude {string}
set gui-device-longitude {string}
set private-data-encryption [disable|enable]
set auto-auth-extension-device [enable|disable]
set gui-theme [green|neutrino|...]
set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
set gui-date-time-source [system|browser]
set igmp-state-limit {integer}
set legacy-poe-device-support [enable|disable]
set cloud-communication [enable|disable]
set fec-port {integer}
set fortitoken-cloud [enable|disable]
set faz-disk-buffer-size {integer}
set irq-time-accounting [auto|force]
set fortiipam-integration [enable|disable]
set early-tcp-npu-session [enable|disable]

```

end

## config system global

Parameter	Description	Type	Size	Default														
language	GUI display language.	option	-	english														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>english</i></td> <td>English.</td> </tr> <tr> <td><i>french</i></td> <td>French.</td> </tr> <tr> <td><i>spanish</i></td> <td>Spanish.</td> </tr> <tr> <td><i>portuguese</i></td> <td>Portuguese.</td> </tr> <tr> <td><i>japanese</i></td> <td>Japanese.</td> </tr> <tr> <td><i>trach</i></td> <td>Traditional Chinese.</td> </tr> </tbody> </table>	Option	Description	<i>english</i>	English.	<i>french</i>	French.	<i>spanish</i>	Spanish.	<i>portuguese</i>	Portuguese.	<i>japanese</i>	Japanese.	<i>trach</i>	Traditional Chinese.			
Option	Description																	
<i>english</i>	English.																	
<i>french</i>	French.																	
<i>spanish</i>	Spanish.																	
<i>portuguese</i>	Portuguese.																	
<i>japanese</i>	Japanese.																	
<i>trach</i>	Traditional Chinese.																	

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>simch</i></td> <td>Simplified Chinese.</td> </tr> <tr> <td><i>korean</i></td> <td>Korean.</td> </tr> </tbody> </table>	Option	Description	<i>simch</i>	Simplified Chinese.	<i>korean</i>	Korean.			
Option	Description									
<i>simch</i>	Simplified Chinese.									
<i>korean</i>	Korean.									
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-certificates	Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.	option	-	disable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-custom-language	Enable/disable custom languages in GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-wireless-opensecurity	Enable/disable wireless open security option on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-display-hostname	Enable/disable displaying the FortiGate's hostname on the GUI login page.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-fortisandbox-cloud	Enable/disable displaying FortiSandbox Cloud on the GUI.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.					
Option	Description											
<i>enable</i>	Display the feature in GUI.											
<i>disable</i>	Do not display the feature in GUI.											
gui-firmware-upgrade-warning	Enable/disable the firmware upgrade warning on the GUI.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.					
Option	Description											
<i>enable</i>	Display the feature in GUI.											
<i>disable</i>	Do not display the feature in GUI.											
gui-allow-default-hostname	Enable/disable the factory default hostname warning on the GUI setup wizard.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.					
Option	Description											
<i>enable</i>	Display the feature in GUI.											
<i>disable</i>	Do not display the feature in GUI.											
gui-forticare-registration-setup-warning	Enable/disable the FortiCare registration setup warning on the GUI.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display the feature in GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display the feature in GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.					
Option	Description											
<i>enable</i>	Display the feature in GUI.											
<i>disable</i>	Do not display the feature in GUI.											
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-	tlsv1-1 tlsv1-2 tlsv1-3								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tlsv1-1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tlsv1-2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tlsv1-3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>tlsv1-1</i>	TLS 1.1.	<i>tlsv1-2</i>	TLS 1.2.	<i>tlsv1-3</i>	TLS 1.3.			
Option	Description											
<i>tlsv1-1</i>	TLS 1.1.											
<i>tlsv1-2</i>	TLS 1.2.											
<i>tlsv1-3</i>	TLS 1.3.											
admintimeout	Number of minutes before an idle administrator session times out . A shorter idle timeout is more secure.	integer	Minimum value: 1 Maximum value: 480	5								

Parameter	Description	Type	Size	Default						
admin-console-timeout	Console login timeout that overrides the admintimeout value. . 0 the default, disables this timeout.	integer	Minimum value: 15 Maximum value: 300	0						
admin-concurrent	Enable/disable concurrent administrator logins. (Use policy-auth-concurrent for firewall authenticated users.)	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable admin concurrent login.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable admin concurrent login.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable admin concurrent login.	<i>disable</i>	Disable admin concurrent login.			
Option	Description									
<i>enable</i>	Enable admin concurrent login.									
<i>disable</i>	Disable admin concurrent login.									
admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 1 Maximum value: 10	3						
admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 1 Maximum value: 2147483647	60						
refresh	Statistics refresh interval second(s) in GUI.	integer	Minimum value: 0 Maximum value: 4294967295	0						
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295	5						
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295	5						
daily-restart	Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable daily reboot of the FortiGate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable daily reboot of the FortiGate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable daily reboot of the FortiGate.	<i>disable</i>	Disable daily reboot of the FortiGate.			
Option	Description									
<i>enable</i>	Enable daily reboot of the FortiGate.									
<i>disable</i>	Disable daily reboot of the FortiGate.									
restart-time	Daily restart time (hh:mm).	user	Not Specified							
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812						
admin-login-max	Maximum number of administrators who can be logged in at the same time	integer	Minimum value: 1 Maximum value: 100	100						
remoteauthtimeout	Number of seconds that the FortiGate waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. .	integer	Minimum value: 1 Maximum value: 300	5						
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds .	integer	Minimum value: 1 Maximum value: 300000	500						
batch-cmdb	Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable batch mode to execute in CMDB server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable batch mode to execute in CMDB server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable batch mode to execute in CMDB server.	<i>disable</i>	Disable batch mode to execute in CMDB server.			
Option	Description									
<i>enable</i>	Enable batch mode to execute in CMDB server.									
<i>disable</i>	Disable batch mode to execute in CMDB server.									
multi-factor-authentication	Enforce all login methods to require an additional authentication factor .	option	-	optional						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>optional</i></td> <td>Do not enforce all login methods to require an additional authentication factor (controlled by user settings).</td> </tr> <tr> <td><i>mandatory</i></td> <td>Enforce all login methods to require an additional authentication factor.</td> </tr> </tbody> </table>	Option	Description	<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).	<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.			
Option	Description									
<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).									
<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.									
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	TLSv1-2						



Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> <tr> <td><i>TLSv1-3</i></td> <td>TLSv1.3.</td> </tr> </tbody> </table>	Option	Description	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.													
Option	Description																									
<i>SSLv3</i>	SSLv3.																									
<i>TLSv1</i>	TLSv1.																									
<i>TLSv1-1</i>	TLSv1.1.																									
<i>TLSv1-2</i>	TLSv1.2.																									
<i>TLSv1-3</i>	TLSv1.3.																									
autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-	disable																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic log partition check after ungraceful shutdown.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic log partition check after ungraceful shutdown.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.	<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.																			
Option	Description																									
<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.																									
<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.																									
dst	Enable/disable daylight saving time.	option	-	enable																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable daylight saving time.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable daylight saving time.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable daylight saving time.	<i>disable</i>	Disable daylight saving time.																			
Option	Description																									
<i>enable</i>	Enable daylight saving time.																									
<i>disable</i>	Disable daylight saving time.																									
timezone	Number corresponding to your time zone from 00 to 86. Enter set timezone ? to view the list of time zones and the numbers that represent them.	option	-	00																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>01</i></td> <td>(GMT-11:00) Midway Island, Samoa</td> </tr> <tr> <td><i>02</i></td> <td>(GMT-10:00) Hawaii</td> </tr> <tr> <td><i>03</i></td> <td>(GMT-9:00) Alaska</td> </tr> <tr> <td><i>04</i></td> <td>(GMT-8:00) Pacific Time (US &amp; Canada)</td> </tr> <tr> <td><i>05</i></td> <td>(GMT-7:00) Arizona</td> </tr> <tr> <td><i>81</i></td> <td>(GMT-7:00) Baja California Sur, Chihuahua</td> </tr> <tr> <td><i>06</i></td> <td>(GMT-7:00) Mountain Time (US &amp; Canada)</td> </tr> <tr> <td><i>07</i></td> <td>(GMT-6:00) Central America</td> </tr> <tr> <td><i>08</i></td> <td>(GMT-6:00) Central Time (US &amp; Canada)</td> </tr> <tr> <td><i>09</i></td> <td>(GMT-6:00) Mexico City</td> </tr> </tbody> </table>	Option	Description	<i>01</i>	(GMT-11:00) Midway Island, Samoa	<i>02</i>	(GMT-10:00) Hawaii	<i>03</i>	(GMT-9:00) Alaska	<i>04</i>	(GMT-8:00) Pacific Time (US & Canada)	<i>05</i>	(GMT-7:00) Arizona	<i>81</i>	(GMT-7:00) Baja California Sur, Chihuahua	<i>06</i>	(GMT-7:00) Mountain Time (US & Canada)	<i>07</i>	(GMT-6:00) Central America	<i>08</i>	(GMT-6:00) Central Time (US & Canada)	<i>09</i>	(GMT-6:00) Mexico City			
Option	Description																									
<i>01</i>	(GMT-11:00) Midway Island, Samoa																									
<i>02</i>	(GMT-10:00) Hawaii																									
<i>03</i>	(GMT-9:00) Alaska																									
<i>04</i>	(GMT-8:00) Pacific Time (US & Canada)																									
<i>05</i>	(GMT-7:00) Arizona																									
<i>81</i>	(GMT-7:00) Baja California Sur, Chihuahua																									
<i>06</i>	(GMT-7:00) Mountain Time (US & Canada)																									
<i>07</i>	(GMT-6:00) Central America																									
<i>08</i>	(GMT-6:00) Central Time (US & Canada)																									
<i>09</i>	(GMT-6:00) Mexico City																									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	10	(GMT-6:00) Saskatchewan		
	11	(GMT-5:00) Bogota, Lima, Quito		
	12	(GMT-5:00) Eastern Time (US & Canada)		
	13	(GMT-5:00) Indiana (East)		
	74	(GMT-4:00) Caracas		
	14	(GMT-4:00) Atlantic Time (Canada)		
	77	(GMT-4:00) Georgetown		
	15	(GMT-4:00) La Paz		
	87	(GMT-4:00) Paraguay		
	16	(GMT-3:00) Santiago		
	17	(GMT-3:30) Newfoundland		
	18	(GMT-3:00) Brasilia		
	19	(GMT-3:00) Buenos Aires		
	20	(GMT-3:00) Nuuk (Greenland)		
	75	(GMT-3:00) Uruguay		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Athens, Sofia, Vilnius		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	44	(GMT+4:30) Kabul		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepara		
	48	(GMT+5:45) Kathmandu		
	45	(GMT+5:00) Ekaterinburg		
	49	(GMT+6:00) Almaty, Novosibirsk		
	50	(GMT+6:00) Astana, Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		

Parameter	Description	Type	Size	Default																																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>58</td> <td>(GMT+8:00) Perth</td> </tr> <tr> <td>59</td> <td>(GMT+8:00) Taipei</td> </tr> <tr> <td>60</td> <td>(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul</td> </tr> <tr> <td>62</td> <td>(GMT+9:30) Adelaide</td> </tr> <tr> <td>63</td> <td>(GMT+9:30) Darwin</td> </tr> <tr> <td>61</td> <td>(GMT+9:00) Yakutsk</td> </tr> <tr> <td>64</td> <td>(GMT+10:00) Brisbane</td> </tr> <tr> <td>65</td> <td>(GMT+10:00) Canberra, Melbourne, Sydney</td> </tr> <tr> <td>66</td> <td>(GMT+10:00) Guam, Port Moresby</td> </tr> <tr> <td>67</td> <td>(GMT+10:00) Hobart</td> </tr> <tr> <td>68</td> <td>(GMT+10:00) Vladivostok</td> </tr> <tr> <td>69</td> <td>(GMT+10:00) Magadan</td> </tr> <tr> <td>70</td> <td>(GMT+11:00) Solomon Is., New Caledonia</td> </tr> <tr> <td>71</td> <td>(GMT+12:00) Auckland, Wellington</td> </tr> <tr> <td>72</td> <td>(GMT+12:00) Fiji, Kamchatka, Marshall Is.</td> </tr> <tr> <td>00</td> <td>(GMT+12:00) Eniwetok, Kwajalein</td> </tr> <tr> <td>82</td> <td>(GMT+12:45) Chatham Islands</td> </tr> <tr> <td>73</td> <td>(GMT+13:00) Nuku'alofa</td> </tr> <tr> <td>86</td> <td>(GMT+13:00) Samoa</td> </tr> <tr> <td>76</td> <td>(GMT+14:00) Kiritimati</td> </tr> </tbody> </table>	Option	Description	58	(GMT+8:00) Perth	59	(GMT+8:00) Taipei	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul	62	(GMT+9:30) Adelaide	63	(GMT+9:30) Darwin	61	(GMT+9:00) Yakutsk	64	(GMT+10:00) Brisbane	65	(GMT+10:00) Canberra, Melbourne, Sydney	66	(GMT+10:00) Guam, Port Moresby	67	(GMT+10:00) Hobart	68	(GMT+10:00) Vladivostok	69	(GMT+10:00) Magadan	70	(GMT+11:00) Solomon Is., New Caledonia	71	(GMT+12:00) Auckland, Wellington	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.	00	(GMT+12:00) Eniwetok, Kwajalein	82	(GMT+12:45) Chatham Islands	73	(GMT+13:00) Nuku'alofa	86	(GMT+13:00) Samoa	76	(GMT+14:00) Kiritimati			
Option	Description																																													
58	(GMT+8:00) Perth																																													
59	(GMT+8:00) Taipei																																													
60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul																																													
62	(GMT+9:30) Adelaide																																													
63	(GMT+9:30) Darwin																																													
61	(GMT+9:00) Yakutsk																																													
64	(GMT+10:00) Brisbane																																													
65	(GMT+10:00) Canberra, Melbourne, Sydney																																													
66	(GMT+10:00) Guam, Port Moresby																																													
67	(GMT+10:00) Hobart																																													
68	(GMT+10:00) Vladivostok																																													
69	(GMT+10:00) Magadan																																													
70	(GMT+11:00) Solomon Is., New Caledonia																																													
71	(GMT+12:00) Auckland, Wellington																																													
72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.																																													
00	(GMT+12:00) Eniwetok, Kwajalein																																													
82	(GMT+12:45) Chatham Islands																																													
73	(GMT+13:00) Nuku'alofa																																													
86	(GMT+13:00) Samoa																																													
76	(GMT+14:00) Kiritimati																																													
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos																																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tos</i></td> <td>IP TOS.</td> </tr> <tr> <td><i>dscp</i></td> <td>DSCP (DiffServ) DS.</td> </tr> </tbody> </table>	Option	Description	<i>tos</i>	IP TOS.	<i>dscp</i>	DSCP (DiffServ) DS.																																							
Option	Description																																													
<i>tos</i>	IP TOS.																																													
<i>dscp</i>	DSCP (DiffServ) DS.																																													
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-	medium																																										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Low priority.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium priority.</td> </tr> <tr> <td><i>high</i></td> <td>High priority.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Low priority.	<i>medium</i>	Medium priority.	<i>high</i>	High priority.			
Option	Description											
<i>low</i>	Low priority.											
<i>medium</i>	Medium priority.											
<i>high</i>	High priority.											
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-	strict								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable anti-replay check.</td> </tr> <tr> <td><i>loose</i></td> <td>Loose anti-replay check.</td> </tr> <tr> <td><i>strict</i></td> <td>Strict anti-replay check.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable anti-replay check.	<i>loose</i>	Loose anti-replay check.	<i>strict</i>	Strict anti-replay check.			
Option	Description											
<i>disable</i>	Disable anti-replay check.											
<i>loose</i>	Loose anti-replay check.											
<i>strict</i>	Strict anti-replay check.											
send-pmtu-icmp	Enable/disable sending of path maximum transmission unit (PMTU) - ICMP destination unreachable packet and to support PMTUD protocol on your network to reduce fragmentation of packets.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of PMTU ICMP destination unreachable packet.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of PMTU ICMP destination unreachable packet.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.	<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.					
Option	Description											
<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.											
<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.											
honor-df	Enable/disable honoring of Don't-Fragment (DF) flag.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable honoring of Don't-Fragment flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable honoring of Don't-Fragment flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable honoring of Don't-Fragment flag.	<i>disable</i>	Disable honoring of Don't-Fragment flag.					
Option	Description											
<i>enable</i>	Enable honoring of Don't-Fragment flag.											
<i>disable</i>	Disable honoring of Don't-Fragment flag.											
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable path MTU discovery.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable path MTU discovery.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable path MTU discovery.	<i>disable</i>	Disable path MTU discovery.					
Option	Description											
<i>enable</i>	Enable path MTU discovery.											
<i>disable</i>	Disable path MTU discovery.											
revision-image-auto-backup	Enable/disable back-up of the latest configuration revision after the firmware is upgraded.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable revision image backup automatically when upgrading image.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable revision image backup automatically when upgrading image.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable revision image backup automatically when upgrading image.	<i>disable</i>	Disable revision image backup automatically when upgrading image.			
Option	Description									
<i>enable</i>	Enable revision image backup automatically when upgrading image.									
<i>disable</i>	Disable revision image backup automatically when upgrading image.									
revision-backup-on-logout	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable revision config backup automatically when logout.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable revision config backup automatically when logout.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable revision config backup automatically when logout.	<i>disable</i>	Disable revision config backup automatically when logout.			
Option	Description									
<i>enable</i>	Enable revision config backup automatically when logout.									
<i>disable</i>	Disable revision config backup automatically when logout.									
management-vdom	Management virtual domain name.	string	Maximum length: 31	root						
hostname	FortiGate unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35							
alias	Alias for your FortiGate unit.	string	Maximum length: 35							
strong-crypto	Enable to use strong encryption and only allow strong ciphers (AES) and digest (SHA1) for HTTPS/SSH/TLS/SSL functions.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strong crypto for HTTPS/SSH/TLS/SSL.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strong crypto for HTTPS/SSH/TLS/SSL.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.	<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.			
Option	Description									
<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.									
<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.									
ssh-cbc-cipher	Enable/disable CBC cipher for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable CBC cipher for SSH access.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable CBC cipher for SSH access.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable CBC cipher for SSH access.	<i>disable</i>	Disable CBC cipher for SSH access.			
Option	Description									
<i>enable</i>	Enable CBC cipher for SSH access.									
<i>disable</i>	Disable CBC cipher for SSH access.									
ssh-hmac-md5	Enable/disable HMAC-MD5 for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HMAC-MD5 for SSH access.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HMAC-MD5 for SSH access.					
Option	Description									
<i>enable</i>	Enable HMAC-MD5 for SSH access.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable HMAC-MD5 for SSH access.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable HMAC-MD5 for SSH access.					
Option	Description									
<i>disable</i>	Disable HMAC-MD5 for SSH access.									
ssh-kex-sha1	Enable/disable SHA1 key exchange for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SHA1 for SSH key exchanges.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SHA1 for SSH key exchanges.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SHA1 for SSH key exchanges.	<i>disable</i>	Disable SHA1 for SSH key exchanges.			
Option	Description									
<i>enable</i>	Enable SHA1 for SSH key exchanges.									
<i>disable</i>	Disable SHA1 for SSH key exchanges.									
ssh-mac-weak	Enable/disable HMAC-SHA1 and UMAC-64-ETM for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.	<i>disable</i>	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.			
Option	Description									
<i>enable</i>	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.									
<i>disable</i>	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.									
ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable static key ciphers in SSL/TLS connections.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable static key ciphers in SSL/TLS connections.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable static key ciphers in SSL/TLS connections.	<i>disable</i>	Disable static key ciphers in SSL/TLS connections.			
Option	Description									
<i>enable</i>	Enable static key ciphers in SSL/TLS connections.									
<i>disable</i>	Disable static key ciphers in SSL/TLS connections.									
snat-route-change	Enable/disable the ability to change the static NAT route.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SNAT route change.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SNAT route change.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SNAT route change.	<i>disable</i>	Disable SNAT route change.			
Option	Description									
<i>enable</i>	Enable SNAT route change.									
<i>disable</i>	Disable SNAT route change.									
cli-audit-log	Enable/disable CLI audit log.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable CLI audit log.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable CLI audit log.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable CLI audit log.	<i>disable</i>	Disable CLI audit log.			
Option	Description									
<i>enable</i>	Enable CLI audit log.									
<i>disable</i>	Disable CLI audit log.									
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048						

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1024</td> <td>1024 bits.</td> </tr> <tr> <td>1536</td> <td>1536 bits.</td> </tr> <tr> <td>2048</td> <td>2048 bits.</td> </tr> <tr> <td>3072</td> <td>3072 bits.</td> </tr> <tr> <td>4096</td> <td>4096 bits.</td> </tr> <tr> <td>6144</td> <td>6144 bits.</td> </tr> <tr> <td>8192</td> <td>8192 bits.</td> </tr> </tbody> </table>	Option	Description	1024	1024 bits.	1536	1536 bits.	2048	2048 bits.	3072	3072 bits.	4096	4096 bits.	6144	6144 bits.	8192	8192 bits.			
Option	Description																			
1024	1024 bits.																			
1536	1536 bits.																			
2048	2048 bits.																			
3072	3072 bits.																			
4096	4096 bits.																			
6144	6144 bits.																			
8192	8192 bits.																			
fds-statistics	Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. This data is used to improve FortiGuard services and is not shared with external parties and is protected by Fortinet's privacy policy.	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard statistics.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard statistics.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard statistics.	<i>disable</i>	Disable FortiGuard statistics.													
Option	Description																			
<i>enable</i>	Enable FortiGuard statistics.																			
<i>disable</i>	Disable FortiGuard statistics.																			
fds-statistics-period	FortiGuard statistics collection period in minutes. .	integer	Minimum value: 1 Maximum value: 1440	60																
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TCP option.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TCP option.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TCP option.	<i>disable</i>	Disable TCP option.													
Option	Description																			
<i>enable</i>	Enable TCP option.																			
<i>disable</i>	Disable TCP option.																			
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable transmission of Link Layer Discovery Protocol (LLDP).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable transmission of Link Layer Discovery Protocol (LLDP).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).													
Option	Description																			
<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).																			
<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).																			



Parameter	Description	Type	Size	Default	
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable	
	<b>Option</b>	<b>Description</b>			
	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).			
	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).			
proxy-auth-timeout	Authentication timeout in minutes for authenticated users .	integer	Minimum value: 1 Maximum value: 300	10	
proxy-re-authentication-mode	Control if users must re-authenticate after a session is closed, traffic has been idle, or from the point at which the user was first created.	option	-	session	
		<b>Option</b>	<b>Description</b>		
		<i>session</i>	Proxy re-authentication timeout begins at the closure of the session.		
		<i>traffic</i>	Proxy re-authentication timeout begins after traffic has not been received.		
	<i>absolute</i>	Proxy re-authentication timeout begins when the user was first created.			
proxy-auth-lifetime	Enable/disable authenticated users lifetime control. This is a cap on the total time a proxy user can be authenticated for after which re-authentication will take place.	option	-	disable	
		<b>Option</b>	<b>Description</b>		
		<i>enable</i>	Enable authenticated users lifetime control.		
	<i>disable</i>	Disable authenticated users lifetime control.			
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users .	integer	Minimum value: 5 Maximum value: 65535	480	
sys-perf-log-interval	Time in minutes between updates of performance statistics logging. .	integer	Minimum value: 0 Maximum value: 15	5	

Parameter	Description	Type	Size	Default						
check-protocol-header	Level of checking performed on protocol headers. Strict checking is more thorough but may affect performance. Loose checking is ok in most cases.	option	-	loose						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>loose</i></td> <td>Check protocol header loosely.</td> </tr> <tr> <td><i>strict</i></td> <td>Check protocol header strictly.</td> </tr> </tbody> </table>	Option	Description	<i>loose</i>	Check protocol header loosely.	<i>strict</i>	Check protocol header strictly.			
Option	Description									
<i>loose</i>	Check protocol header loosely.									
<i>strict</i>	Check protocol header strictly.									
vip-arp-range	Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.	option	-	restricted						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>unlimited</i></td> <td>Send ARPs for all addresses in VIP range.</td> </tr> <tr> <td><i>restricted</i></td> <td>Send ARPs for the first 8192 addresses in VIP range.</td> </tr> </tbody> </table>	Option	Description	<i>unlimited</i>	Send ARPs for all addresses in VIP range.	<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.			
Option	Description									
<i>unlimited</i>	Send ARPs for all addresses in VIP range.									
<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.									
reset-sessionless-tcp	Action to perform if the FortiGate receives a TCP packet but cannot find a corresponding session in its session table. NAT/Route mode only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reset session-less TCP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reset session-less TCP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reset session-less TCP.	<i>disable</i>	Disable reset session-less TCP.			
Option	Description									
<i>enable</i>	Enable reset session-less TCP.									
<i>disable</i>	Disable reset session-less TCP.									
allow-traffic-redirect	Disable to allow traffic to be routed back on a different interface.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable allow traffic redirect.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable allow traffic redirect.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable allow traffic redirect.	<i>disable</i>	Disable allow traffic redirect.			
Option	Description									
<i>enable</i>	Enable allow traffic redirect.									
<i>disable</i>	Disable allow traffic redirect.									
strict-dirty-session-check	Enable to check the session against the original policy when revalidating. This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together. If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strict dirty-session check.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strict dirty-session check.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strict dirty-session check.	<i>disable</i>	Disable strict dirty-session check.			
Option	Description									
<i>enable</i>	Enable strict dirty-session check.									
<i>disable</i>	Disable strict dirty-session check.									
tcp-halfclose-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded .	integer	Minimum value: 1 Maximum value: 86400	120						
tcp-halfopen-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded .	integer	Minimum value: 1 Maximum value: 86400	10						
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	1						
udp-idle-timer	UDP connection session timeout. This command can be useful in managing CPU and memory resources .	integer	Minimum value: 1 Maximum value: 86400	180						
block-session-timer	Duration in seconds for blocked sessions .	integer	Minimum value: 1 Maximum value: 300	30						
ip-src-port-range	IP source port range used for traffic originating from the FortiGate unit.	user	Not Specified	1024-25000						
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable pre-login banner.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable pre-login banner.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable pre-login banner.	<i>disable</i>	Disable pre-login banner.			
Option	Description									
<i>enable</i>	Enable pre-login banner.									
<i>disable</i>	Disable pre-login banner.									
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable post-login banner.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable post-login banner.					
Option	Description									
<i>disable</i>	Disable post-login banner.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable post-login banner.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable post-login banner.							
Option	Description											
<i>enable</i>	Enable post-login banner.											
tftp	Enable/disable TFTP.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TFTP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TFTP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TFTP.	<i>disable</i>	Disable TFTP.					
Option	Description											
<i>enable</i>	Enable TFTP.											
<i>disable</i>	Disable TFTP.											
av-failopen	Set the action to take if the FortiGate is running low on memory or the proxy connection limit has been reached.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.</td> </tr> <tr> <td><i>off</i></td> <td>Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.</td> </tr> <tr> <td><i>one-shot</i></td> <td>Bypass the antivirus system when memory is low.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.	<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.	<i>one-shot</i>	Bypass the antivirus system when memory is low.			
Option	Description											
<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.											
<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.											
<i>one-shot</i>	Bypass the antivirus system when memory is low.											
av-failopen-session	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AV fail open session option.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AV fail open session option.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AV fail open session option.	<i>disable</i>	Disable AV fail open session option.					
Option	Description											
<i>enable</i>	Enable AV fail open session option.											
<i>disable</i>	Disable AV fail open session option.											
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme .	integer	Minimum value: 70 Maximum value: 97	95								
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode .	integer	Minimum value: 70 Maximum value: 97	88								
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode .	integer	Minimum value: 70 Maximum value: 97	82								

Parameter	Description	Type	Size	Default								
cpu-use-threshold	Threshold at which CPU usage is reported.	integer	Minimum value: 50 Maximum value: 99	90								
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>strict</i></td> <td>Check RST range strictly.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable RST range check.</td> </tr> </tbody> </table>	Option	Description	<i>strict</i>	Check RST range strictly.	<i>disable</i>	Disable RST range check.					
Option	Description											
<i>strict</i>	Check RST range strictly.											
<i>disable</i>	Disable RST range check.											
vdom-mode *	Enable/disable support for split/multiple virtual domains (VDMs).	option	-	no-vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-vdom</i></td> <td>Disable split/multiple VDMs mode.</td> </tr> <tr> <td><i>split-vdom</i></td> <td>Enable split VDMs mode.</td> </tr> <tr> <td><i>multi-vdom</i></td> <td>Enable multiple VDMs mode.</td> </tr> </tbody> </table>	Option	Description	<i>no-vdom</i>	Disable split/multiple VDMs mode.	<i>split-vdom</i>	Enable split VDMs mode.	<i>multi-vdom</i>	Enable multiple VDMs mode.			
Option	Description											
<i>no-vdom</i>	Disable split/multiple VDMs mode.											
<i>split-vdom</i>	Enable split VDMs mode.											
<i>multi-vdom</i>	Enable multiple VDMs mode.											
long-vdom-name *	Enable/disable long VDOM name support.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable long VDOM name support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable long VDOM name support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable long VDOM name support.	<i>disable</i>	Disable long VDOM name support.					
Option	Description											
<i>enable</i>	Enable long VDOM name support.											
<i>disable</i>	Disable long VDOM name support.											
edit-vdom-prompt *	Enable/disable edit new VDOM prompt.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable edit new VDOM prompt.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable edit new VDOM prompt.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable edit new VDOM prompt.	<i>disable</i>	Disable edit new VDOM prompt.					
Option	Description											
<i>enable</i>	Enable edit new VDOM prompt.											
<i>disable</i>	Disable edit new VDOM prompt.											
admin-port	Administrative access port for HTTP. .	integer	Minimum value: 1 Maximum value: 65535	80								
admin-sport	Administrative access port for HTTPS. .	integer	Minimum value: 1 Maximum value: 65535	443								

Parameter	Description	Type	Size	Default						
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable redirecting HTTP administration access to HTTPS.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable redirecting HTTP administration access to HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.	<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.			
Option	Description									
<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.									
<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.									
admin-hsts-max-age	HTTPS Strict-Transport-Security header max-age in seconds. A value of 0 will reset any HSTS records in the browser. When admin-https-redirect is disabled the header max-age will be 0.	integer	Minimum value: 0 Maximum value: 2147483647	15552000						
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable password authentication for SSH admin access.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable password authentication for SSH admin access.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable password authentication for SSH admin access.	<i>disable</i>	Disable password authentication for SSH admin access.			
Option	Description									
<i>enable</i>	Enable password authentication for SSH admin access.									
<i>disable</i>	Disable password authentication for SSH admin access.									
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable local admin authentication restriction.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable local admin authentication restriction.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable local admin authentication restriction.	<i>disable</i>	Disable local admin authentication restriction.			
Option	Description									
<i>enable</i>	Enable local admin authentication restriction.									
<i>disable</i>	Disable local admin authentication restriction.									
admin-ssh-port	Administrative access port for SSH. .	integer	Minimum value: 1 Maximum value: 65535	22						
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating .	integer	Minimum value: 10 Maximum value: 3600	120						
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSH v1 compatibility.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSH v1 compatibility.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSH v1 compatibility.	<i>disable</i>	Disable SSH v1 compatibility.			
Option	Description									
<i>enable</i>	Enable SSH v1 compatibility.									
<i>disable</i>	Disable SSH v1 compatibility.									

Parameter	Description	Type	Size	Default						
admin-telnet	Enable/disable TELNET service.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TELNET service.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TELNET service.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TELNET service.	<i>disable</i>	Disable TELNET service.			
Option	Description									
<i>enable</i>	Enable TELNET service.									
<i>disable</i>	Disable TELNET service.									
admin-telnet-port	Administrative access port for TELNET. .	integer	Minimum value: 1 Maximum value: 65535	23						
default-service-source-port	Default service source port range.	user	Not Specified							
admin-maintainer	Enable/disable maintainer administrator login. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password is "bcpb" followed by the FortiGate unit serial number. You have limited time to complete this login.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable login for special user (maintainer).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable login for special user (maintainer).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable login for special user (maintainer).	<i>disable</i>	Disable login for special user (maintainer).			
Option	Description									
<i>enable</i>	Enable login for special user (maintainer).									
<i>disable</i>	Disable login for special user (maintainer).									
admin-reset-button *	press the reset button can reset to factory default	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>press the reset button can reset to factory default</td> </tr> <tr> <td><i>disable</i></td> <td>press the reset button cannot reset to factory default</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	press the reset button can reset to factory default	<i>disable</i>	press the reset button cannot reset to factory default			
Option	Description									
<i>enable</i>	press the reset button can reset to factory default									
<i>disable</i>	press the reset button cannot reset to factory default									
admin-server-cert	Server certificate that the FortiGate uses for HTTPS administrative connections.	string	Maximum length: 35	self-sign						
user-server-cert	Certificate to use for https user authentication.	string	Maximum length: 35	Fortinet_Factory						
admin-https-pki-required	Enable/disable admin login method. Enable to force administrators to provide a valid certificate to log in if PKI is enabled. Disable to allow administrators to log in with a certificate or password.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.</td> </tr> <tr> <td><i>disable</i></td> <td>Admin users can login by providing a valid certificate or password.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.	<i>disable</i>	Admin users can login by providing a valid certificate or password.			
Option	Description									
<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.									
<i>disable</i>	Admin users can login by providing a valid certificate or password.									
wifi-certificate	Certificate to use for WiFi authentication.	string	Maximum length: 35	Fortinet_Wifi						
wifi-ca-certificate	CA certificate that verifies the WiFi certificate.	string	Maximum length: 79	Fortinet_Wifi_CA						
auth-http-port	User authentication HTTP port. .	integer	Minimum value: 1 Maximum value: 65535	1000						
auth-https-port	User authentication HTTPS port. .	integer	Minimum value: 1 Maximum value: 65535	1003						
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of keep alive to extend authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of keep alive to extend authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of keep alive to extend authentication.	<i>disable</i>	Disable use of keep alive to extend authentication.			
Option	Description									
<i>enable</i>	Enable use of keep alive to extend authentication.									
<i>disable</i>	Disable use of keep alive to extend authentication.									
policy-auth-concurrent	Number of concurrent firewall use logins from the same user .	integer	Minimum value: 0 Maximum value: 100	0						
auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-	block-new						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block-new</i></td> <td>Block new user authentication attempts.</td> </tr> <tr> <td><i>logout-inactive</i></td> <td>Logout the most inactive user authenticated sessions.</td> </tr> </tbody> </table>	Option	Description	<i>block-new</i>	Block new user authentication attempts.	<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.			
Option	Description									
<i>block-new</i>	Block new user authentication attempts.									
<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.									
auth-cert	Server certificate that the FortiGate uses for HTTPS firewall authentication connections.	string	Maximum length: 35	Fortinet_Factory						
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-	disable						



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable require client certificate for GUI login.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable require client certificate for GUI login.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable require client certificate for GUI login.	<i>disable</i>	Disable require client certificate for GUI login.					
Option	Description											
<i>enable</i>	Enable require client certificate for GUI login.											
<i>disable</i>	Disable require client certificate for GUI login.											
fortiservice-port	FortiService port . Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535	8013								
cfg-save	Configuration file save mode for CLI changes.	option	-	automatic								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>automatic</i></td> <td>Automatically save config.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually save config.</td> </tr> <tr> <td><i>revert</i></td> <td>Manually save config and revert the config when timeout.</td> </tr> </tbody> </table>	Option	Description	<i>automatic</i>	Automatically save config.	<i>manual</i>	Manually save config.	<i>revert</i>	Manually save config and revert the config when timeout.			
Option	Description											
<i>automatic</i>	Automatically save config.											
<i>manual</i>	Manually save config.											
<i>revert</i>	Manually save config and revert the config when timeout.											
cfg-revert-timeout	Time-out for reverting to the last saved configuration. .	integer	Minimum value: 10 Maximum value: 4294967295	600								
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reboot of system upon restoring configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reboot of system upon restoring configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reboot of system upon restoring configuration.	<i>disable</i>	Disable reboot of system upon restoring configuration.					
Option	Description											
<i>enable</i>	Enable reboot of system upon restoring configuration.											
<i>disable</i>	Disable reboot of system upon restoring configuration.											
admin-scp	Enable/disable using SCP to download the system configuration. You can use SCP as an alternative method for backing up the configuration.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable allow system configuration download by SCP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable allow system configuration download by SCP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable allow system configuration download by SCP.	<i>disable</i>	Disable allow system configuration download by SCP.					
Option	Description											
<i>enable</i>	Enable allow system configuration download by SCP.											
<i>disable</i>	Disable allow system configuration download by SCP.											
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable submission of Security Rating results to FortiGuard.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable submission of Security Rating results to FortiGuard.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable submission of Security Rating results to FortiGuard.	<i>disable</i>	Disable submission of Security Rating results to FortiGuard.			
Option	Description									
<i>enable</i>	Enable submission of Security Rating results to FortiGuard.									
<i>disable</i>	Disable submission of Security Rating results to FortiGuard.									
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable scheduled runs of Security Rating.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable scheduled runs of Security Rating.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable scheduled runs of Security Rating.	<i>disable</i>	Disable scheduled runs of Security Rating.			
Option	Description									
<i>enable</i>	Enable scheduled runs of Security Rating.									
<i>disable</i>	Disable scheduled runs of Security Rating.									
wireless-controller	Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable wireless controller.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable wireless controller.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable wireless controller.	<i>disable</i>	Disable wireless controller.			
Option	Description									
<i>enable</i>	Enable wireless controller.									
<i>disable</i>	Disable wireless controller.									
wireless-controller-port	Port used for the control channel in wireless controller mode .	integer	Minimum value: 1024 Maximum value: 49150	5246						
fortiextender-data-port	FortiExtender data port .	integer	Minimum value: 1024 Maximum value: 49150	25246						
fortiextender	Enable/disable FortiExtender.	option	-	enable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable FortiExtender controller.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable FortiExtender controller.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable FortiExtender controller.	<i>enable</i>	Enable FortiExtender controller.			
Option	Description									
<i>disable</i>	Disable FortiExtender controller.									
<i>enable</i>	Enable FortiExtender controller.									
fortiextender-vlan-mode	Enable/disable FortiExtender VLAN mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiExtender VLAN mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiExtender VLAN mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiExtender VLAN mode.	<i>disable</i>	Disable FortiExtender VLAN mode.			
Option	Description									
<i>enable</i>	Enable FortiExtender VLAN mode.									
<i>disable</i>	Disable FortiExtender VLAN mode.									

Parameter	Description	Type	Size	Default						
switch-controller	Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable switch controller feature.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable switch controller feature.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable switch controller feature.	<i>enable</i>	Enable switch controller feature.			
Option	Description									
<i>disable</i>	Disable switch controller feature.									
<i>enable</i>	Enable switch controller feature.									
switch-controller-reserved-network	Enable reserved network subnet for controlled switches. This is available when the switch controller is enabled.	ipv4-classnet	Not Specified	169.254.0.0 255.255.0.0						
dnsproxy-worker-count	DNS proxy worker count. For a FortiGate unit with multiple logical CPUs, the number of DNS processes may be set to 1 to the number of logical CPUs.	integer	Minimum value: 1 Maximum value: The number of logical CPUs.	1						
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1 **	1						
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 4 **	0						
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs.	integer	Minimum value: 2 Maximum value: 4 **	0						
proxy-hardware-acceleration *	Enable/disable email proxy hardware acceleration.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable email proxy hardware acceleration.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable email proxy hardware acceleration.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable email proxy hardware acceleration.	<i>enable</i>	Enable email proxy hardware acceleration.			
Option	Description									
<i>disable</i>	Disable email proxy hardware acceleration.									
<i>enable</i>	Enable email proxy hardware acceleration.									
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>advisory</i></td> <td>Retrieve FortiGuard advisories, report and news alerts.</td> </tr> </tbody> </table>	Option	Description	<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.					
Option	Description									
<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>latest-threat</i></td> <td>Retrieve latest FortiGuard threats alerts.</td> </tr> <tr> <td><i>latest-virus</i></td> <td>Retrieve latest FortiGuard virus alerts.</td> </tr> <tr> <td><i>latest-attack</i></td> <td>Retrieve latest FortiGuard attack alerts.</td> </tr> <tr> <td><i>new-antivirus-db</i></td> <td>Retrieve FortiGuard AV database release alerts.</td> </tr> <tr> <td><i>new-attack-db</i></td> <td>Retrieve FortiGuard IPS database release alerts.</td> </tr> </tbody> </table>	Option	Description	<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.	<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.	<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.	<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.	<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.			
Option	Description															
<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.															
<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.															
<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.															
<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.															
<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.															
ipsec-hmac-offload *	Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable offload IPsec HMAC processing to hardware if possible.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable offload IPsec HMAC processing to hardware.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.	<i>disable</i>	Disable offload IPsec HMAC processing to hardware.									
Option	Description															
<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.															
<i>disable</i>	Disable offload IPsec HMAC processing to hardware.															
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2	1												
ipv6-allow-anycast-probe	Enable/disable IPv6 address probe through Anycast.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable probing of IPv6 address space through Anycast</td> </tr> <tr> <td><i>disable</i></td> <td>Disable probing of IPv6 address space through Anycast</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable probing of IPv6 address space through Anycast	<i>disable</i>	Disable probing of IPv6 address space through Anycast									
Option	Description															
<i>enable</i>	Enable probing of IPv6 address space through Anycast															
<i>disable</i>	Disable probing of IPv6 address space through Anycast															
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable CA attribute in CSR.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable CA attribute in CSR.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable CA attribute in CSR.	<i>disable</i>	Disable CA attribute in CSR.									
Option	Description															
<i>enable</i>	Enable CA attribute in CSR.															
<i>disable</i>	Disable CA attribute in CSR.															
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WiMax 4G.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WiMax 4G.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WiMax 4G.	<i>disable</i>	Disable WiMax 4G.			
Option	Description									
<i>enable</i>	Enable WiMax 4G.									
<i>disable</i>	Disable WiMax 4G.									
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8						
sslvpn-max-worker-count	Maximum number of SSL-VPN processes. Upper limit for this value is the number of CPUs and depends on the model. Default value of zero means the SSLVPN daemon decides the number of worker processes.	integer	Minimum value: 0 Maximum value: 4 **	0						
sslvpn-kxp-hardware-acceleration *	Enable/disable SSL-VPN KXP hardware acceleration.	option	-	enable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable KXP SSL-VPN hardware acceleration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable KXP SSL-VPN hardware acceleration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable KXP SSL-VPN hardware acceleration.	<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.			
Option	Description									
<i>enable</i>	Enable KXP SSL-VPN hardware acceleration.									
<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.									
sslvpn-cipher-hardware-acceleration *	Enable/disable SSL-VPN hardware acceleration.	option	-	enable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSL-VPN cipher hardware acceleration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL-VPN cipher hardware acceleration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.	<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.			
Option	Description									
<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.									
<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.									
sslvpn-ems-sn-check	Enable/disable verification of EMS serial number in SSL-VPN connection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of EMS serial number in SSL-VPN connection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of EMS serial number in SSL-VPN connection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of EMS serial number in SSL-VPN connection.	<i>disable</i>	Disable verification of EMS serial number in SSL-VPN connection.			
Option	Description									
<i>enable</i>	Enable verification of EMS serial number in SSL-VPN connection.									
<i>disable</i>	Disable verification of EMS serial number in SSL-VPN connection.									
sslvpn-plugin-version-check	Enable/disable checking browser's plugin version by SSL-VPN.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSL-VPN automatic checking of browser plug-in version.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL-VPN automatic checking of browser plug-in version.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.	<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.			
Option	Description									
<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.									
<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.									
two-factor-ftk-expiry	FortiToken authentication session timeout .	integer	Minimum value: 60 Maximum value: 600	60						
two-factor-email-expiry	Email-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300	60						
two-factor-sms-expiry	SMS-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300	60						
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout .	integer	Minimum value: 10 Maximum value: 3600	60						
two-factor-ftm-expiry	FortiToken Mobile session timeout .	integer	Minimum value: 1 Maximum value: 168	72						
wad-worker-count	Number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy, and web caching is handled by all of the CPU cores in a FortiGate unit.	integer	Minimum value: 0 Maximum value: 4 **	0						
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1	1						
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 4 **	0						
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-	enable						


Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dispatching traffic to WAD workers based on source affinity.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dispatching traffic to WAD workers based on source affinity.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.	<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.			
Option	Description									
<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.									
<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.									
wad-memory-change-granularity	Minimum percentage change in system memory usage detected by the wad daemon prior to adjusting TCP window size for any active connection.	integer	Minimum value: 5 Maximum value: 25	10						
login-timestamp	Enable/disable login time recording.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable login time recording.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable login time recording.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable login time recording.	<i>disable</i>	Disable login time recording.			
Option	Description									
<i>enable</i>	Enable login time recording.									
<i>disable</i>	Disable login time recording.									
miglogd-children	Number of logging (miglogd) processes to be allowed to run. Higher number can reduce performance; lower number can slow log processing time. No logs will be dropped or lost if the number is changed.	integer	Minimum value: 0 Maximum value: 15	0						
special-file-23-support	Enable/disable detection of those special format files when using Data Leak Protection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable detection of those special format files when using Data Leak Protection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable detection of those special format files when using Data Leak Protection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable detection of those special format files when using Data Leak Protection.	<i>enable</i>	Enable detection of those special format files when using Data Leak Protection.			
Option	Description									
<i>disable</i>	Disable detection of those special format files when using Data Leak Protection.									
<i>enable</i>	Enable detection of those special format files when using Data Leak Protection.									
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable insertion of address UUID to traffic logs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable insertion of address UUID to traffic logs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable insertion of address UUID to traffic logs.	<i>disable</i>	Disable insertion of address UUID to traffic logs.			
Option	Description									
<i>enable</i>	Enable insertion of address UUID to traffic logs.									
<i>disable</i>	Disable insertion of address UUID to traffic logs.									
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging of SSL connection events.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging of SSL connection events.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging of SSL connection events.	<i>disable</i>	Disable logging of SSL connection events.			
Option	Description									
<i>enable</i>	Enable logging of SSL connection events.									
<i>disable</i>	Disable logging of SSL connection events.									
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table .	integer	Minimum value: 131072 Maximum value: 2147483647	131072						
ndp-max-entry	Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries).	integer	Minimum value: 65536 Maximum value: 2147483647	0						
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647	8192						
max-route-cache-size	Maximum number of IP route cache entries .	integer	Minimum value: 0 Maximum value: 2147483647	0						
ipsec-asic-offload *	Enable/disable ASIC offloading (hardware acceleration) for IPsec VPN traffic. Hardware acceleration can offload IPsec VPN sessions and accelerate encryption and decryption.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ASIC offload for IPsec VPN.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ASIC offload for IPsec VPN.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ASIC offload for IPsec VPN.	<i>disable</i>	Disable ASIC offload for IPsec VPN.			
Option	Description									
<i>enable</i>	Enable ASIC offload for IPsec VPN.									
<i>disable</i>	Disable ASIC offload for IPsec VPN.									
ipsec-soft-dec-async	Enable/disable software decryption asynchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable software decryption asynchronization for IPsec VPN.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable software decryption asynchronization for IPsec VPN.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable software decryption asynchronization for IPsec VPN.	<i>disable</i>	Disable software decryption asynchronization for IPsec VPN.			
Option	Description									
<i>enable</i>	Enable software decryption asynchronization for IPsec VPN.									
<i>disable</i>	Disable software decryption asynchronization for IPsec VPN.									



Parameter	Description	Type	Size	Default								
device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out. .	integer	Minimum value: 30 Maximum value: 31536000	300								
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 1000 Maximum value: 5000	5000								
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 1000 Maximum value: 1000	5000								
gui-device-latitude	Add the latitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19									
gui-device-longitude	Add the longitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19									
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable private data encryption using an AES 128-bit key.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable private data encryption using an AES 128-bit key.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable private data encryption using an AES 128-bit key.	<i>enable</i>	Enable private data encryption using an AES 128-bit key.					
Option	Description											
<i>disable</i>	Disable private data encryption using an AES 128-bit key.											
<i>enable</i>	Enable private data encryption using an AES 128-bit key.											
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic authorization of dedicated Fortinet extension device globally.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic authorization of dedicated Fortinet extension device globally.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.					
Option	Description											
<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.											
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.											
gui-theme	Color scheme for the administration GUI.	option	-	green								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>green</i></td> <td>Green theme.</td> </tr> <tr> <td><i>neutrino</i></td> <td>Neutrino theme.</td> </tr> <tr> <td><i>blue</i></td> <td>Light blue theme.</td> </tr> </tbody> </table>	Option	Description	<i>green</i>	Green theme.	<i>neutrino</i>	Neutrino theme.	<i>blue</i>	Light blue theme.			
Option	Description											
<i>green</i>	Green theme.											
<i>neutrino</i>	Neutrino theme.											
<i>blue</i>	Light blue theme.											

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>melongene</i></td> <td>Melongene theme (eggplant color).</td> </tr> <tr> <td><i>mariner</i></td> <td>Mariner theme (dark blue color).</td> </tr> </tbody> </table>	Option	Description	<i>melongene</i>	Melongene theme (eggplant color).	<i>mariner</i>	Mariner theme (dark blue color).											
Option	Description																	
<i>melongene</i>	Melongene theme (eggplant color).																	
<i>mariner</i>	Mariner theme (dark blue color).																	
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>yyyy/MM/dd</i></td> <td>Year/Month/Day.</td> </tr> <tr> <td><i>dd/MM/yyyy</i></td> <td>Day/Month/Year.</td> </tr> <tr> <td><i>MM/dd/yyyy</i></td> <td>Month/Day/Year.</td> </tr> <tr> <td><i>yyyy-MM-dd</i></td> <td>Year-Month-Day.</td> </tr> <tr> <td><i>dd-MM-yyyy</i></td> <td>Day-Month-Year.</td> </tr> <tr> <td><i>MM-dd-yyyy</i></td> <td>Month-Day-Year.</td> </tr> </tbody> </table>	Option	Description	<i>yyyy/MM/dd</i>	Year/Month/Day.	<i>dd/MM/yyyy</i>	Day/Month/Year.	<i>MM/dd/yyyy</i>	Month/Day/Year.	<i>yyyy-MM-dd</i>	Year-Month-Day.	<i>dd-MM-yyyy</i>	Day-Month-Year.	<i>MM-dd-yyyy</i>	Month-Day-Year.			
Option	Description																	
<i>yyyy/MM/dd</i>	Year/Month/Day.																	
<i>dd/MM/yyyy</i>	Day/Month/Year.																	
<i>MM/dd/yyyy</i>	Month/Day/Year.																	
<i>yyyy-MM-dd</i>	Year-Month-Day.																	
<i>dd-MM-yyyy</i>	Day-Month-Year.																	
<i>MM-dd-yyyy</i>	Month-Day-Year.																	
gui-date-time-source	Source from which the FortiGate GUI uses to display date and time entries.	option	-	system														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>system</i></td> <td>Use this FortiGate unit's configured timezone.</td> </tr> <tr> <td><i>browser</i></td> <td>Use the web browser's timezone.</td> </tr> </tbody> </table>	Option	Description	<i>system</i>	Use this FortiGate unit's configured timezone.	<i>browser</i>	Use the web browser's timezone.											
Option	Description																	
<i>system</i>	Use this FortiGate unit's configured timezone.																	
<i>browser</i>	Use the web browser's timezone.																	
igmp-state-limit	Maximum number of IGMP memberships .	integer	Minimum value: 96 Maximum value: 128000	3200														
legacy-poe-device-support *	Enable/disable legacy POE device support.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable legacy POE device support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable legacy POE device support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable legacy POE device support.	<i>disable</i>	Disable legacy POE device support.											
Option	Description																	
<i>enable</i>	Enable legacy POE device support.																	
<i>disable</i>	Disable legacy POE device support.																	
cloud-communication	Enable/disable all cloud communication.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow cloud communication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable all cloud-related settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow cloud communication.	<i>disable</i>	Disable all cloud-related settings.											
Option	Description																	
<i>enable</i>	Allow cloud communication.																	
<i>disable</i>	Disable all cloud-related settings.																	

Parameter	Description	Type	Size	Default						
	 <p>When set to <i>disable</i>, cloud-related settings (for example, config system autoupdate tunneling status) will be disabled. When a user issues the command to change one of these settings, it will fail with the message <i>cloud communication is disabled in 'system.global'</i>.</p>									
fec-port	Local UDP port for Forward Error Correction .	integer	Minimum value: 49152 Maximum value: 65535	50000						
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiToken Cloud service.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiToken Cloud service.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiToken Cloud service.	<i>disable</i>	Disable FortiToken Cloud service.			
Option	Description									
<i>enable</i>	Enable FortiToken Cloud service.									
<i>disable</i>	Disable FortiToken Cloud service.									
faz-disk-buffer-size	Maximum disk buffer size to temporarily store logs destined for FortiAnalyzer. To be used in the event that FortiAnalyzer is unavailable.	integer	Minimum value: 0 Maximum value: 161061273	0						
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically switch CPU accounting mode.</td> </tr> <tr> <td><i>force</i></td> <td>Force the use of CPU IRQ time accounting mode.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically switch CPU accounting mode.	<i>force</i>	Force the use of CPU IRQ time accounting mode.			
Option	Description									
<i>auto</i>	Automatically switch CPU accounting mode.									
<i>force</i>	Force the use of CPU IRQ time accounting mode.									
fortipam-integration	Enable/disable integration with the FortiIPAM cloud service.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable integration with FortiIPAM for automatic IP address management.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable integration with FortiIPAM for automatic IP address management.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable integration with FortiIPAM for automatic IP address management.	<i>disable</i>	Disable integration with FortiIPAM for automatic IP address management.			
Option	Description									
<i>enable</i>	Enable integration with FortiIPAM for automatic IP address management.									
<i>disable</i>	Disable integration with FortiIPAM for automatic IP address management.									
early-tcp-npu-session	Enable/disable early TCP NPU session.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.					
Option	Description									
<i>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.									

Parameter	Description	Type	Size	Default				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.			
Option	Description							
<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.							

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config system accprofile

Configure access profiles for system administrators.

```

config system accprofile
  Description: Configure access profiles for system administrators.
  edit <name>
    set scope [vdom|global]
    set comments {var-string}
    set secfabgrp [none|read|...]
    set ftviewgrp [none|read|...]
    set authgrp [none|read|...]
    set sysgrp [none|read|...]
    set netgrp [none|read|...]
    set loggrp [none|read|...]
    set fwgrp [none|read|...]
    set vpngrp [none|read|...]
    set utmgrp [none|read|...]
    set wifi [none|read|...]
    config netgrp-permission
      Description: Custom network permission.
      set cfg [none|read|...]
      set packet-capture [none|read|...]
      set route-cfg [none|read|...]
    end
    config sysgrp-permission
      Description: Custom system permission.
      set admin [none|read|...]
      set upd [none|read|...]
      set cfg [none|read|...]
      set mnt [none|read|...]
    end
    config fwgrp-permission
      Description: Custom firewall permission.
      set policy [none|read|...]
      set address [none|read|...]
      set service [none|read|...]
      set schedule [none|read|...]
      set others [none|read|...]
    end
    config loggrp-permission
      Description: Custom Log & Report permission.
      set config [none|read|...]
      set data-access [none|read|...]
  end

```

```

    set report-access [none|read|...]
    set threat-weight [none|read|...]
end
config utmgrp-permission
  Description: Custom Security Profile permissions.
  set antivirus [none|read|...]
  set ips [none|read|...]
  set webfilter [none|read|...]
  set emailfilter [none|read|...]
  set data-loss-prevention [none|read|...]
  set file-filter [none|read|...]
  set application-control [none|read|...]
  set icap [none|read|...]
  set voip [none|read|...]
  set waf [none|read|...]
  set dnsfilter [none|read|...]
  set endpoint-control [none|read|...]
end
set admintimeout-override [enable|disable]
set admintimeout {integer}
set system-diagnostics [enable|disable]
next
end

```

## config system accprofile

Parameter	Description	Type	Size	Default								
scope	Scope of admin access: global or specific VDOM(s).	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>vdom</i></td> <td>VDOM access.</td> </tr> <tr> <td><i>global</i></td> <td>Global access.</td> </tr> </tbody> </table>	Option	Description	<i>vdom</i>	VDOM access.	<i>global</i>	Global access.					
Option	Description											
<i>vdom</i>	VDOM access.											
<i>global</i>	Global access.											
comments	Comment.	var-string	Maximum length: 255									
secfabgrp	Security Fabric.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
ftviewgrp	FortiView.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.							
Option	Description											
<i>none</i>	No access.											

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.							
Option	Description													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
authgrp	Administrator access to Users and Devices.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
sysgrp	System Configuration.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> <tr> <td><i>custom</i></td> <td>Customized access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
netgrp	Network Configuration.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> <tr> <td><i>custom</i></td> <td>Customized access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> <tr> <td><i>custom</i></td> <td>Customized access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
fwgrp	Administrator access to the Firewall configuration.	option	-	none										

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> <tr> <td><i>custom</i></td> <td>Customized access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
utmgrp	Administrator access to Security Profiles.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> <tr> <td><i>custom</i></td> <td>Customized access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
wifi	Administrator access to the WiFi controller and Switch controller.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable overriding the global administrator idle timeout.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable overriding the global administrator idle timeout.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable overriding the global administrator idle timeout.	<i>disable</i>	Disable overriding the global administrator idle timeout.							
Option	Description													
<i>enable</i>	Enable overriding the global administrator idle timeout.													
<i>disable</i>	Disable overriding the global administrator idle timeout.													

Parameter	Description	Type	Size	Default						
admintimeout	Administrator timeout for this access profile .	integer	Minimum value: 1 Maximum value: 480	10						
system-diagnostics	Enable/disable permission to run system diagnostic commands.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable permission to run system diagnostic commands.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable permission to run system diagnostic commands.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable permission to run system diagnostic commands.	<i>disable</i>	Disable permission to run system diagnostic commands.			
Option	Description									
<i>enable</i>	Enable permission to run system diagnostic commands.									
<i>disable</i>	Disable permission to run system diagnostic commands.									

### config netgrp-permission

Parameter	Description	Type	Size	Default								
cfg	Network Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
packet-capture	Packet Capture Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
route-cfg	Router Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											



## config sysgrp-permission

Parameter	Description	Type	Size	Default								
admin	Administrator Users.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></tbody></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
upd	FortiGuard Updates.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></tbody></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
cfg	System Configuration.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></tbody></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
mnt	Maintenance.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></tbody></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

## config fwgrp-permission

Parameter	Description	Type	Size	Default								
policy	Policy Configuration.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></tbody></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

Parameter	Description	Type	Size	Default								
address	Address Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
service	Service Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
schedule	Schedule Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
others	Other Firewall Configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

### config loggrp-permission

Parameter	Description	Type	Size	Default								
config	Log & Report configuration.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

Parameter	Description	Type	Size	Default								
data-access	Log & Report Data Access.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
report-access	Log & Report Report Access.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
threat-weight	Log & Report Threat Weight.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

### config utmgrp-permission

Parameter	Description	Type	Size	Default								
antivirus	Antivirus profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
ips	IPS profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

Parameter	Description	Type	Size	Default								
webfilter	Web Filter profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
emailfilter	AntiSpam filter and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
data-loss-prevention	DLP profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
file-filter	File-filter profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
application-control	Application Control profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
icap	ICAP profiles and settings.	option	-	none								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
voip	VoIP profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
waf	Web Application Firewall profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
dnsfilter	DNS Filter profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
endpoint-control	FortiClient Profiles.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No access.</td> </tr> <tr> <td><i>read</i></td> <td>Read access.</td> </tr> <tr> <td><i>read-write</i></td> <td>Read/write access.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

## config system vdom-link

Configure VDOM links.

```
config system vdom-link
  Description: Configure VDOM links.
```

```

edit <name>
  set vcluster [vcluster1|vcluster2]
  set type [ppp|ethernet|...]
next
end

```

## config system vdom-link

Parameter	Description	Type	Size	Default								
vcluster	Virtual cluster.	option	-	vcluster1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>vcluster1</i></td> <td>Virtual cluster 1.</td> </tr> <tr> <td><i>vcluster2</i></td> <td>Virtual cluster 2.</td> </tr> </tbody> </table>	Option	Description	<i>vcluster1</i>	Virtual cluster 1.	<i>vcluster2</i>	Virtual cluster 2.					
Option	Description											
<i>vcluster1</i>	Virtual cluster 1.											
<i>vcluster2</i>	Virtual cluster 2.											
type	VDOM link type: PPP or Ethernet.	option	-	ppp								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ppp</i></td> <td>PPP VDOM link.</td> </tr> <tr> <td><i>ethernet</i></td> <td>Ethernet VDOM link.</td> </tr> <tr> <td><i>npupair</i></td> <td>NPU VDOM link.</td> </tr> </tbody> </table>	Option	Description	<i>ppp</i>	PPP VDOM link.	<i>ethernet</i>	Ethernet VDOM link.	<i>npupair</i>	NPU VDOM link.			
Option	Description											
<i>ppp</i>	PPP VDOM link.											
<i>ethernet</i>	Ethernet VDOM link.											
<i>npupair</i>	NPU VDOM link.											

## config system switch-interface

Configure software switch interfaces by grouping physical and WiFi interfaces.

```

config system switch-interface
  Description: Configure software switch interfaces by grouping physical and WiFi
  interfaces.
  edit <name>
    set vdom {string}
    set span-dest-port {string}
    set span-source-port <interface-name1>, <interface-name2>, ...
    set member <interface-name1>, <interface-name2>, ...
    set type [switch|hub]
    set intra-switch-policy [implicit|explicit]
    set mac-ttl {integer}
    set span [disable|enable]
    set span-direction [rx|tx|...]
  next
end

```

## config system switch-interface

Parameter	Description	Type	Size	Default
vdom	VDOM that the software switch belongs to.	string	Maximum length: 31	
span-dest-port	SPAN destination port name. All traffic on the SPAN source ports is echoed to the SPAN destination port.	string	Maximum length: 15	
span-source-port <interface-name>	Physical interface name. Port spanning echoes all traffic on the SPAN source ports to the SPAN destination port. Physical interface name.	string	Maximum length: 79	
member <interface-name>	Names of the interfaces that belong to the virtual switch. Physical interface name.	string	Maximum length: 79	
type	Type of switch based on functionality: switch for normal functionality, or hub to duplicate packets to all port members.	option	-	switch
		<b>Option</b>	<b>Description</b>	
		<i>switch</i>	Switch for normal switch functionality (available in NAT mode only).	
		<i>hub</i>	Hub to duplicate packets to all member ports.	
intra-switch-policy	Allow any traffic between switch interfaces or require firewall policies to allow traffic between switch interfaces.	option	-	implicit
		<b>Option</b>	<b>Description</b>	
		<i>implicit</i>	Traffic between switch members is implicitly allowed.	
		<i>explicit</i>	Traffic between switch members must match firewall policies.	
mac-ttl	Duration for which MAC addresses are held in the ARP table .	integer	Minimum value: 300 Maximum value: 8640000	300
span	Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span destination port.	option	-	disable
		<b>Option</b>	<b>Description</b>	
		<i>disable</i>	Disable port spanning.	
		<i>enable</i>	Enable port spanning.	

Parameter	Description	Type	Size	Default								
span-direction	The direction in which the SPAN port operates, either: rx, tx, or both.	option	-	both								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rx</i></td> <td>Copies only received packets from source SPAN ports to the destination SPAN port.</td> </tr> <tr> <td><i>tx</i></td> <td>Copies only transmitted packets from source SPAN ports to the destination SPAN port.</td> </tr> <tr> <td><i>both</i></td> <td>Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.</td> </tr> </tbody> </table>	Option	Description	<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.	<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.	<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.			
Option	Description											
<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.											
<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.											
<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.											

## config system object-tagging

Configure object tagging.

```

config system object-tagging
  Description: Configure object tagging.
  edit <category>
    set address [disable|mandatory|...]
    set device [disable|mandatory|...]
    set interface [disable|mandatory|...]
    set multiple [enable|disable]
    set color {integer}
    set tags <name1>, <name2>, ...
  next
end

```

## config system object-tagging

Parameter	Description	Type	Size	Default								
address	Address.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>mandatory</i></td> <td>Mandatory.</td> </tr> <tr> <td><i>optional</i></td> <td>Optional.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>mandatory</i>	Mandatory.	<i>optional</i>	Optional.			
Option	Description											
<i>disable</i>	Disable.											
<i>mandatory</i>	Mandatory.											
<i>optional</i>	Optional.											
device	Device.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.							
Option	Description											
<i>disable</i>	Disable.											



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mandatory</i></td> <td>Mandatory.</td> </tr> <tr> <td><i>optional</i></td> <td>Optional.</td> </tr> </tbody> </table>	Option	Description	<i>mandatory</i>	Mandatory.	<i>optional</i>	Optional.					
Option	Description											
<i>mandatory</i>	Mandatory.											
<i>optional</i>	Optional.											
interface	Interface.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>mandatory</i></td> <td>Mandatory.</td> </tr> <tr> <td><i>optional</i></td> <td>Optional.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>mandatory</i>	Mandatory.	<i>optional</i>	Optional.			
Option	Description											
<i>disable</i>	Disable.											
<i>mandatory</i>	Mandatory.											
<i>optional</i>	Optional.											
multiple	Allow multiple tag selection.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multi-tagging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multi-tagging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multi-tagging.	<i>disable</i>	Disable multi-tagging.					
Option	Description											
<i>enable</i>	Enable multi-tagging.											
<i>disable</i>	Disable multi-tagging.											
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0								
tags <name>	Tags. Tag name.	string	Maximum length: 79									

## config system lte-modem



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64.

Configure USB LTE/WIMAX devices.

```
config system lte-modem
  Description: Configure USB LTE/WIMAX devices.
  set status [enable|disable]
  set extra-init {string}
  set authtype [none|pap|...]
  set username {string}
  set passwd {password}
  set apn {string}
  set modem-port {integer}
  set mode [standalone|redundant]
  set holddown-timer {integer}
  set interface {string}
```

end

## config system lte-modem

Parameter	Description	Type	Size	Default								
status	Enable/disable USB LTE/WIMAX device.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable USB LTE/WIMA device.</td></tr><tr><td><i>disable</i></td><td>Disable USB LTE/WIMA device.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable USB LTE/WIMA device.	<i>disable</i>	Disable USB LTE/WIMA device.					
Option	Description											
<i>enable</i>	Enable USB LTE/WIMA device.											
<i>disable</i>	Disable USB LTE/WIMA device.											
extra-init	Extra initialization string for USB LTE/WIMAX devices.	string	Maximum length: 127									
authtype	Authentication type for PDP-IP packet data calls.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>Username and password not required.</td></tr><tr><td><i>pap</i></td><td>Use PAP authentication.</td></tr><tr><td><i>chap</i></td><td>Use CHAP authentication.</td></tr></tbody></table>	Option	Description	<i>none</i>	Username and password not required.	<i>pap</i>	Use PAP authentication.	<i>chap</i>	Use CHAP authentication.			
Option	Description											
<i>none</i>	Username and password not required.											
<i>pap</i>	Use PAP authentication.											
<i>chap</i>	Use CHAP authentication.											
username	Authentication username for PDP-IP packet data calls.	string	Maximum length: 63									
passwd	Authentication password for PDP-IP packet data calls.	password	Not Specified									
apn	Login APN string for PDP-IP packet data calls.	string	Maximum length: 127									
modem-port	Modem port index .	integer	Minimum value: 0 Maximum value: 20	255								
mode	Modem operation mode.	option	-	standalone								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>standalone</i></td><td>Standalone modem operation mode.</td></tr><tr><td><i>redundant</i></td><td>Redundant modem operation mode where the modem is used as a backup interface.</td></tr></tbody></table>	Option	Description	<i>standalone</i>	Standalone modem operation mode.	<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.					
Option	Description											
<i>standalone</i>	Standalone modem operation mode.											
<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.											
holddown-timer	Hold down timer .	integer	Minimum value: 10 Maximum value: 60	30								

Parameter	Description	Type	Size	Default
interface	The interface that the modem is acting as a redundant interface for.	string	Maximum length: 63	

## config system interface

Configure interfaces.

```

config system interface
  Description: Configure interfaces.
  edit <name>
    set vdom {string}
    set vrf {integer}
    set cli-conn-status {integer}
    set fortilink [enable|disable]
    set switch-controller-source-ip [outbound|fixed]
    set mode [static|dhcp|...]
  config client-options
    Description: DHCP client options.
    edit <id>
      set code {integer}
      set type [hex|string|...]
      set value {string}
      set ip {user}
    next
  end
  set distance {integer}
  set priority {integer}
  set dhcp-relay-interface-select-method [auto|sdwan|...]
  set dhcp-relay-interface {string}
  set dhcp-relay-service [disable|enable]
  set dhcp-relay-ip {user}
  set dhcp-relay-request-all-server [disable|enable]
  set dhcp-relay-type [regular|ipsec]
  set dhcp-relay-agent-option [enable|disable]
  set management-ip {ipv4-classnet-host}
  set ip {ipv4-classnet-host}
  set allowaccess {option1}, {option2}, ...
  set gwdetect [enable|disable]
  set ping-serv-status {integer}
  set detectserver {user}
  set detectprotocol {option1}, {option2}, ...
  set ha-priority {integer}
  set fail-detect [enable|disable]
  set fail-detect-option {option1}, {option2}, ...
  set fail-alert-method [link-failed-signal|link-down]
  set fail-action-on-extender [soft-restart|hard-restart|...]
  set fail-alert-interfaces <name1>, <name2>, ...
  set dhcp-client-identifier {string}
  set dhcp-renew-time {integer}
  set ipunnumbered {ipv4-address}
  set username {string}
  set pppoe-unnumbered-negotiate [enable|disable]
  set password {password}

```

---

```
set idle-timeout {integer}
set detected-peer-mtu {integer}
set disc-retry-timeout {integer}
set padt-retry-timeout {integer}
set service-name {string}
set ac-name {string}
set lcp-echo-interval {integer}
set lcp-max-echo-fails {integer}
set defaultgw [enable|disable]
set dns-server-override [enable|disable]
set auth-type [auto|pap|...]
set pptp-client [enable|disable]
set pptp-user {string}
set pptp-password {password}
set pptp-server-ip {ipv4-address}
set pptp-auth-type [auto|pap|...]
set pptp-timeout {integer}
set arpforward [enable|disable]
set ndiscforward [enable|disable]
set broadcast-forward [enable|disable]
set bfd [global|enable|...]
set bfd-desired-min-tx {integer}
set bfd-detect-mult {integer}
set bfd-required-min-rx {integer}
set l2forward [enable|disable]
set icmp-send-redirect [enable|disable]
set icmp-accept-redirect [enable|disable]
set vlanforward [enable|disable]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set ips-sniffer-mode [enable|disable]
set ident-accept [enable|disable]
set ipmac [enable|disable]
set subst [enable|disable]
set macaddr {mac-address}
set substitute-dst-mac {mac-address}
set poe [enable|disable]
set speed [auto|10full|...]
set status [up|down]
set netbios-forward [disable|enable]
set wins-ip {ipv4-address}
set type [physical|vlan|...]
set dedicated-to [none|management]
set trust-ip-1 {ipv4-classnet-any}
set trust-ip-2 {ipv4-classnet-any}
set trust-ip-3 {ipv4-classnet-any}
set trust-ip6-1 {ipv6-prefix}
set trust-ip6-2 {ipv6-prefix}
set trust-ip6-3 {ipv6-prefix}
set mtu-override [enable|disable]
set mtu {integer}
set wccp [enable|disable]
set netflow-sampler [disable|tx|...]
set sflow-sampler [enable|disable]
set drop-overlapped-fragment [enable|disable]
set drop-fragment [enable|disable]
set src-check [enable|disable]
```

```

set sample-rate {integer}
set polling-interval {integer}
set sample-direction [tx|rx|...]
set explicit-web-proxy [enable|disable]
set explicit-ftp-proxy [enable|disable]
set proxy-captive-portal [enable|disable]
set tcp-mss {integer}
set inbandwidth {integer}
set outbandwidth {integer}
set egress-shaping-profile {string}
set ingress-shaping-profile {string}
set disconnect-threshold {integer}
set spillover-threshold {integer}
set ingress-spillover-threshold {integer}
set weight {integer}
set interface {string}
set external [enable|disable]
set vlan-protocol [8021q|8021ad]
set vlanid {integer}
set forward-domain {integer}
set remote-ip {ipv4-classnet-host}
set member <interface-name1>, <interface-name2>, ...
set lacp-mode [static|passive|...]
set lacp-ha-slave [enable|disable]
set system-id-type [auto|user]
set system-id {mac-address}
set lacp-speed [slow|fast]
set min-links {integer}
set min-links-down [operational|administrative]
set algorithm [L2|L3|...]
set link-up-delay {integer}
set priority-override [enable|disable]
set aggregate {string}
set redundant-interface {string}
set devindex {integer}
set vindex {integer}
set switch {string}
set description {var-string}
set alias {string}
set l2tp-client [enable|disable]
config l2tp-client-settings
    Description: L2TP client settings.
    set user {string}
    set password {password}
    set peer-host {string}
    set peer-mask {ipv4-netmask}
    set peer-port {integer}
    set auth-type [auto|pap|...]
    set mtu {integer}
    set distance {integer}
    set priority {integer}
    set defaultgw [enable|disable]
    set ip {ipv4-classnet-host}
end
set security-mode [none|captive-portal|...]
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-8021x-mode [default|dynamic-vlan|...]

```

```

set security-8021x-master {string}
set security-8021x-dynamic-vlan-id {integer}
set security-external-web {string}
set security-external-logout {string}
set replacemsg-override-group {string}
set security-redirect-url {string}
set security-exempt-list {string}
set security-groups <name1>, <name2>, ...
set stp [disable|enable]
set stp-ha-slave [disable|enable|...]
set device-identification [enable|disable]
set device-user-identification [enable|disable]
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set lldp-network-policy {string}
set estimated-upstream-bandwidth {integer}
set estimated-downstream-bandwidth {integer}
set measured-upstream-bandwidth {integer}
set measured-downstream-bandwidth {integer}
set bandwidth-measure-time {integer}
set monitor-bandwidth [enable|disable]
set vrrp-virtual-mac [enable|disable]
config vrrp
  Description: VRRP configuration.
  edit <vrid>
    set version [2|3]
    set vrgrp {integer}
    set vrip {ipv4-address-any}
    set priority {integer}
    set adv-interval {integer}
    set start-time {integer}
    set preempt [enable|disable]
    set accept-mode [enable|disable]
    set vrdst {ipv4-address-any}
    set vrdst-priority {integer}
    set ignore-default-route [enable|disable]
    set status [enable|disable]
  config proxy-arp
    Description: VRRP Proxy ARP configuration.
    edit <id>
      set ip {user}
    next
  end
end
set role [lan|wan|...]
set snmp-index {integer}
set secondary-IP [enable|disable]
config secondaryip
  Description: Second IP address of interface.
  edit <id>
    set ip {ipv4-classnet-host}
    set allowaccess {option1}, {option2}, ...
    set gwdetect [enable|disable]
    set ping-serv-status {integer}
    set detectserver {user}
    set detectprotocol {option1}, {option2}, ...

```

```

    set ha-priority {integer}
  next
end
set preserve-session-route [enable|disable]
set auto-auth-extension-device [enable|disable]
set ap-discover [enable|disable]
set fortilink-stacking [enable|disable]
set fortilink-neighbor-detect [lldp|fortilink]
set ip-managed-by-fortiipam [enable|disable]
set managed-subnetwork-size [256|512|...]
set fortilink-split-interface [enable|disable]
set internal {integer}
set fortilink-backup-link {integer}
set switch-controller-access-vlan [enable|disable]
set switch-controller-traffic-policy {string}
set switch-controller-rspan-mode [disable|enable]
set switch-controller-mgmt-vlan {integer}
set switch-controller-igmp-snooping [enable|disable]
set switch-controller-igmp-snooping-proxy [enable|disable]
set switch-controller-igmp-snooping-fast-leave [enable|disable]
set switch-controller-dhcp-snooping [enable|disable]
set switch-controller-dhcp-snooping-verify-mac [enable|disable]
set switch-controller-dhcp-snooping-option82 [enable|disable]
set switch-controller-arp-inspection [enable|disable]
set switch-controller-learning-limit {integer}
set switch-controller-nac {string}
set switch-controller-feature [none|default-vlan|...]
set switch-controller-iot-scanning [enable|disable]
set swc-vlan {integer}
set swc-first-create {integer}
set color {integer}
config tagging
  Description: Config object tagging.
  edit <name>
    set category {string}
    set tags <name1>, <name2>, ...
  next
end
config ipv6
  Description: IPv6 of interface.
  set ip6-mode [static|dhcp|...]
  set nd-mode [basic|SEND-compatible]
  set nd-cert {string}
  set nd-security-level {integer}
  set nd-timestamp-delta {integer}
  set nd-timestamp-fuzz {integer}
  set nd-cga-modifier {user}
  set ip6-dns-server-override [enable|disable]
  set ip6-address {ipv6-prefix}
  config ip6-extra-addr
    Description: Extra IPv6 address prefixes of interface.
    edit <prefix>
      next
    end
  set ip6-allowaccess {option1}, {option2}, ...
  set ip6-send-adv [enable|disable]
  set icmp6-send-redirect [enable|disable]

```

```

set ip6-manage-flag [enable|disable]
set ip6-other-flag [enable|disable]
set ip6-max-interval {integer}
set ip6-min-interval {integer}
set ip6-link-mtu {integer}
set ra-send-mtu [enable|disable]
set ip6-reachable-time {integer}
set ip6-retrans-time {integer}
set ip6-default-life {integer}
set ip6-hop-limit {integer}
set autoconf [enable|disable]
set unique-autoconf-addr [enable|disable]
set interface-identifier {ipv6-address}
set ip6-upstream-interface {string}
set ip6-subnet {ipv6-prefix}
config ip6-prefix-list
  Description: Advertised prefix list.
  edit <prefix>
    set autonomous-flag [enable|disable]
    set onlink-flag [enable|disable]
    set valid-life-time {integer}
    set preferred-life-time {integer}
    set rdns {user}
    set dnssl <domain1>, <domain2>, ...
  next
end
config ip6-delegated-prefix-list
  Description: Advertised IPv6 delegated prefix list.
  edit <prefix-id>
    set upstream-interface {string}
    set autonomous-flag [enable|disable]
    set onlink-flag [enable|disable]
    set subnet {ipv6-network}
    set rdns-service [delegated|default|...]
    set rdns {user}
  next
end
set dhcp6-relay-service [disable|enable]
set dhcp6-relay-type {option}
set dhcp6-relay-ip {user}
set dhcp6-client-options {option1}, {option2}, ...
set dhcp6-prefix-delegation [enable|disable]
set dhcp6-information-request [enable|disable]
set dhcp6-prefix-hint {ipv6-network}
set dhcp6-prefix-hint-plt {integer}
set dhcp6-prefix-hint-vlt {integer}
set vrrp-virtual-mac6 [enable|disable]
set vrip6_link_local {ipv6-address}
config vrrp6
  Description: IPv6 VRRP configuration.
  edit <vrid>
    set vrgrp {integer}
    set vrip6 {ipv6-address}
    set priority {integer}
    set adv-interval {integer}
    set start-time {integer}
    set preempt [enable|disable]

```



```

        set accept-mode [enable|disable]
        set vrdst6 {ipv6-address}
        set status [enable|disable]
    next
end
end
next
end

```

## config system interface

Parameter	Description	Type	Size	Default						
vdom	Interface is in this virtual domain (VDM).	string	Maximum length: 31							
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0						
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0						
fortilink	Enable FortiLink to dedicate this interface to manage other Fortinet devices.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiLink to dedicated interface for managing FortiSwitch devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiLink to dedicated interface for managing FortiSwitch devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.	<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.									
<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.									
switch-controller-source-ip	Source IP address used in FortiLink over L3 connections.	option	-	outbound						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>outbound</i></td> <td>Source IP address is that of the outbound interface.</td> </tr> <tr> <td><i>fixed</i></td> <td>Source IP address is that of the FortiLink interface.</td> </tr> </tbody> </table>	Option	Description	<i>outbound</i>	Source IP address is that of the outbound interface.	<i>fixed</i>	Source IP address is that of the FortiLink interface.			
Option	Description									
<i>outbound</i>	Source IP address is that of the outbound interface.									
<i>fixed</i>	Source IP address is that of the FortiLink interface.									
mode	Addressing mode (static, DHCP, PPPoE).	option	-	static						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Static setting.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Static setting.					
Option	Description									
<i>static</i>	Static setting.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dhcp</i></td> <td>External DHCP client mode.</td> </tr> <tr> <td><i>pppoe</i></td> <td>External PPPoE mode.</td> </tr> </tbody> </table>	Option	Description	<i>dhcp</i>	External DHCP client mode.	<i>pppoe</i>	External PPPoE mode.					
Option	Description											
<i>dhcp</i>	External DHCP client mode.											
<i>pppoe</i>	External PPPoE mode.											
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255	5								
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295	0								
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
dhcp-relay-service	Enable/disable allowing this interface to act as a DHCP relay.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>None.</td> </tr> <tr> <td><i>enable</i></td> <td>DHCP relay agent.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	None.	<i>enable</i>	DHCP relay agent.					
Option	Description											
<i>disable</i>	None.											
<i>enable</i>	DHCP relay agent.											
dhcp-relay-ip	DHCP relay IP address.	user	Not Specified									
dhcp-relay-request-all-server	Enable/disable sending DHCP request to all servers.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Only send DHCP request to matching server.</td> </tr> <tr> <td><i>enable</i></td> <td>Sending DHCP request to all servers.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Only send DHCP request to matching server.	<i>enable</i>	Sending DHCP request to all servers.					
Option	Description											
<i>disable</i>	Only send DHCP request to matching server.											
<i>enable</i>	Sending DHCP request to all servers.											

Parameter	Description	Type	Size	Default																								
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>Regular DHCP relay.</td> </tr> <tr> <td><i>ipsec</i></td> <td>DHCP relay for IPsec.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	Regular DHCP relay.	<i>ipsec</i>	DHCP relay for IPsec.																					
Option	Description																											
<i>regular</i>	Regular DHCP relay.																											
<i>ipsec</i>	DHCP relay for IPsec.																											
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCP relay agent option.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP relay agent option.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCP relay agent option.	<i>disable</i>	Disable DHCP relay agent option.																					
Option	Description																											
<i>enable</i>	Enable DHCP relay agent option.																											
<i>disable</i>	Disable DHCP relay agent option.																											
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																								
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																								
allowaccess	Permitted types of management access to this interface.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>fgfm</i></td> <td>FortiManager access.</td> </tr> <tr> <td><i>radius-acct</i></td> <td>RADIUS accounting access.</td> </tr> <tr> <td><i>probe-response</i></td> <td>Probe access.</td> </tr> <tr> <td><i>fabric</i></td> <td>Security Fabric access.</td> </tr> <tr> <td><i>ftm</i></td> <td>FTM access.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.			
Option	Description																											
<i>ping</i>	PING access.																											
<i>https</i>	HTTPS access.																											
<i>ssh</i>	SSH access.																											
<i>snmp</i>	SNMP access.																											
<i>http</i>	HTTP access.																											
<i>telnet</i>	TELNET access.																											
<i>fgfm</i>	FortiManager access.																											
<i>radius-acct</i>	RADIUS accounting access.																											
<i>probe-response</i>	Probe access.																											
<i>fabric</i>	Security Fabric access.																											
<i>ftm</i>	FTM access.																											
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable																								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable detect gateway alive for first.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable detect gateway alive for first.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable detect gateway alive for first.	<i>disable</i>	Disable detect gateway alive for first.					
Option	Description											
<i>enable</i>	Enable detect gateway alive for first.											
<i>disable</i>	Disable detect gateway alive for first.											
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0								
detectserver	Gateway's ping server for this IP.	user	Not Specified									
detectprotocol	Protocols used to detect the server.	option	-	ping								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING.</td> </tr> <tr> <td><i>tcp-echo</i></td> <td>TCP echo.</td> </tr> <tr> <td><i>udp-echo</i></td> <td>UDP echo.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING.	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.			
Option	Description											
<i>ping</i>	PING.											
<i>tcp-echo</i>	TCP echo.											
<i>udp-echo</i>	UDP echo.											
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1								
fail-detect	Enable/disable fail detection features for this interface.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable interface failed option status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable interface failed option status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable interface failed option status.	<i>disable</i>	Disable interface failed option status.					
Option	Description											
<i>enable</i>	Enable interface failed option status.											
<i>disable</i>	Disable interface failed option status.											
fail-detect-option	Options for detecting that this interface has failed.	option	-	link-down								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>detectserver</i></td> <td>Use a ping server to determine if the interface has failed.</td> </tr> <tr> <td><i>link-down</i></td> <td>Use port detection to determine if the interface has failed.</td> </tr> </tbody> </table>	Option	Description	<i>detectserver</i>	Use a ping server to determine if the interface has failed.	<i>link-down</i>	Use port detection to determine if the interface has failed.					
Option	Description											
<i>detectserver</i>	Use a ping server to determine if the interface has failed.											
<i>link-down</i>	Use port detection to determine if the interface has failed.											
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-	link-down								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>link-failed-signal</i></td> <td>Link-failed-signal.</td> </tr> <tr> <td><i>link-down</i></td> <td>Link-down.</td> </tr> </tbody> </table>	Option	Description	<i>link-failed-signal</i>	Link-failed-signal.	<i>link-down</i>	Link-down.					
Option	Description											
<i>link-failed-signal</i>	Link-failed-signal.											
<i>link-down</i>	Link-down.											

Parameter	Description	Type	Size	Default								
fail-action-on-extender	Action on extender when interface fail .	option	-	soft-restart								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>soft-restart</i></td> <td>Soft-restart-on-extender.</td> </tr> <tr> <td><i>hard-restart</i></td> <td>Hard-restart-on-extender.</td> </tr> <tr> <td><i>reboot</i></td> <td>Reboot-on-extender.</td> </tr> </tbody> </table>	Option	Description	<i>soft-restart</i>	Soft-restart-on-extender.	<i>hard-restart</i>	Hard-restart-on-extender.	<i>reboot</i>	Reboot-on-extender.			
Option	Description											
<i>soft-restart</i>	Soft-restart-on-extender.											
<i>hard-restart</i>	Hard-restart-on-extender.											
<i>reboot</i>	Reboot-on-extender.											
fail-alert-interfaces <name>	Names of the FortiGate interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 79									
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48									
dhcp-renew-time	DHCP renew time in seconds , 0 means use the renew time provided by the server.	integer	Minimum value: 300 Maximum value: 604800	0								
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified	0.0.0.0								
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64									
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IP address negotiating for unnumbered.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IP address negotiating for unnumbered.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IP address negotiating for unnumbered.	<i>disable</i>	Disable IP address negotiating for unnumbered.					
Option	Description											
<i>enable</i>	Enable IP address negotiating for unnumbered.											
<i>disable</i>	Disable IP address negotiating for unnumbered.											
password	PPPoE account's password.	password	Not Specified									
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 32767	0								
detected-peer-mtu	MTU of detected peer .	integer	Minimum value: 0 Maximum value: 4294967295	0								

Parameter	Description	Type	Size	Default						
disc-retry-timeout	Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 4294967295	1						
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295	1						
service-name	PPPoE service name.	string	Maximum length: 63							
ac-name	PPPoE server name.	string	Maximum length: 63							
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5						
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3						
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable default gateway.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable default gateway.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable default gateway.	<i>disable</i>	Disable default gateway.		
Option	Description									
<i>enable</i>	Enable default gateway.									
<i>disable</i>	Disable default gateway.									
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Use DNS acquired by DHCP or PPPoE.</td> </tr> <tr> <td><i>disable</i></td> <td>No not use DNS acquired by DHCP or PPPoE.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Use DNS acquired by DHCP or PPPoE.	<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.		
Option	Description									
<i>enable</i>	Use DNS acquired by DHCP or PPPoE.									
<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.									
auth-type	PPP authentication type to use.	option	-	auto						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically choose authentication.</td> </tr> </tbody> </table>		Option	Description	<i>auto</i>	Automatically choose authentication.				
Option	Description									
<i>auto</i>	Automatically choose authentication.									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pap</i></td> <td>PAP authentication.</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP authentication.</td> </tr> <tr> <td><i>mschapv1</i></td> <td>MS-CHAPv1 authentication.</td> </tr> <tr> <td><i>mschapv2</i></td> <td>MS-CHAPv2 authentication.</td> </tr> </tbody> </table>	Option	Description	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.					
Option	Description															
<i>pap</i>	PAP authentication.															
<i>chap</i>	CHAP authentication.															
<i>mschapv1</i>	MS-CHAPv1 authentication.															
<i>mschapv2</i>	MS-CHAPv2 authentication.															
pptp-client	Enable/disable PPTP client.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PPTP client.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PPTP client.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PPTP client.	<i>disable</i>	Disable PPTP client.									
Option	Description															
<i>enable</i>	Enable PPTP client.															
<i>disable</i>	Disable PPTP client.															
pptp-user	PPTP user name.	string	Maximum length: 64													
pptp-password	PPTP password.	password	Not Specified													
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0												
pptp-auth-type	PPTP authentication type.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically choose authentication.</td> </tr> <tr> <td><i>pap</i></td> <td>PAP authentication.</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP authentication.</td> </tr> <tr> <td><i>mschapv1</i></td> <td>MS-CHAPv1 authentication.</td> </tr> <tr> <td><i>mschapv2</i></td> <td>MS-CHAPv2 authentication.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.			
Option	Description															
<i>auto</i>	Automatically choose authentication.															
<i>pap</i>	PAP authentication.															
<i>chap</i>	CHAP authentication.															
<i>mschapv1</i>	MS-CHAPv1 authentication.															
<i>mschapv2</i>	MS-CHAPv2 authentication.															
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0												
arpforward	Enable/disable ARP forwarding.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ARP forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ARP forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ARP forwarding.	<i>disable</i>	Disable ARP forwarding.									
Option	Description															
<i>enable</i>	Enable ARP forwarding.															
<i>disable</i>	Disable ARP forwarding.															
ndiscforward	Enable/disable NDISC forwarding.	option	-	enable												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NDISC forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NDISC forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NDISC forwarding.	<i>disable</i>	Disable NDISC forwarding.					
Option	Description											
<i>enable</i>	Enable NDISC forwarding.											
<i>disable</i>	Disable NDISC forwarding.											
broadcast-forward	Enable/disable broadcast forwarding.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable broadcast forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable broadcast forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable broadcast forwarding.	<i>disable</i>	Disable broadcast forwarding.					
Option	Description											
<i>enable</i>	Enable broadcast forwarding.											
<i>disable</i>	Disable broadcast forwarding.											
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-	global								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>BFD behavior of this interface will be based on global configuration.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable BFD on this interface and ignore global configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable BFD on this interface and ignore global configuration.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	BFD behavior of this interface will be based on global configuration.	<i>enable</i>	Enable BFD on this interface and ignore global configuration.	<i>disable</i>	Disable BFD on this interface and ignore global configuration.			
Option	Description											
<i>global</i>	BFD behavior of this interface will be based on global configuration.											
<i>enable</i>	Enable BFD on this interface and ignore global configuration.											
<i>disable</i>	Disable BFD on this interface and ignore global configuration.											
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000	250								
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50	3								
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000	250								
l2forward	Enable/disable l2 forwarding.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable L2 forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable L2 forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable L2 forwarding.	<i>disable</i>	Disable L2 forwarding.					
Option	Description											
<i>enable</i>	Enable L2 forwarding.											
<i>disable</i>	Disable L2 forwarding.											
icmp-send-redirect	Enable/disable sending of ICMP redirects.	option	-	enable								



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of ICMP redirects.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of ICMP redirects.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of ICMP redirects.	<i>disable</i>	Disable sending of ICMP redirects.					
Option	Description											
<i>enable</i>	Enable sending of ICMP redirects.											
<i>disable</i>	Disable sending of ICMP redirects.											
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ICMP accept redirect.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ICMP accept redirect.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ICMP accept redirect.	<i>disable</i>	Disable ICMP accept redirect.					
Option	Description											
<i>enable</i>	Enable ICMP accept redirect.											
<i>disable</i>	Disable ICMP accept redirect.											
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable traffic forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable traffic forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable traffic forwarding.	<i>disable</i>	Disable traffic forwarding.					
Option	Description											
<i>enable</i>	Enable traffic forwarding.											
<i>disable</i>	Disable traffic forwarding.											
stpforward	Enable/disable STP forwarding.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable STP forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable STP forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable STP forwarding.	<i>disable</i>	Disable STP forwarding.					
Option	Description											
<i>enable</i>	Enable STP forwarding.											
<i>disable</i>	Disable STP forwarding.											
stpforward-mode	Configure STP forwarding mode.	option	-	rpl-all-ext-id								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rpl-all-ext-id</i></td> <td>Replace all extension IDs (root, bridge).</td> </tr> <tr> <td><i>rpl-bridge-ext-id</i></td> <td>Replace the bridge extension ID only.</td> </tr> <tr> <td><i>rpl-nothing</i></td> <td>Replace nothing.</td> </tr> </tbody> </table>	Option	Description	<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.	<i>rpl-nothing</i>	Replace nothing.			
Option	Description											
<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).											
<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.											
<i>rpl-nothing</i>	Replace nothing.											
ips-sniffer-mode	Enable/disable the use of this interface as a one-armed sniffer.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS sniffer mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS sniffer mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS sniffer mode.	<i>disable</i>	Disable IPS sniffer mode.					
Option	Description											
<i>enable</i>	Enable IPS sniffer mode.											
<i>disable</i>	Disable IPS sniffer mode.											
ident-accept	Enable/disable authentication for this interface.	option	-	disable								

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable determining a user's identity from packet identification.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable determining a user's identity from packet identification.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable determining a user's identity from packet identification.	<i>disable</i>	Disable determining a user's identity from packet identification.									
Option	Description															
<i>enable</i>	Enable determining a user's identity from packet identification.															
<i>disable</i>	Disable determining a user's identity from packet identification.															
ipmac	Enable/disable IP/MAC binding.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IP/MAC binding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IP/MAC binding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IP/MAC binding.	<i>disable</i>	Disable IP/MAC binding.									
Option	Description															
<i>enable</i>	Enable IP/MAC binding.															
<i>disable</i>	Disable IP/MAC binding.															
subst	Enable to always send packets from this interface to a destination MAC address.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send packets from this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not send packets from this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send packets from this interface.	<i>disable</i>	Do not send packets from this interface.									
Option	Description															
<i>enable</i>	Send packets from this interface.															
<i>disable</i>	Do not send packets from this interface.															
macaddr	Change the interface's MAC address.	mac-address	Not Specified	**												
substitute-dst-mac	Destination MAC address that all packets are sent to from this interface.	mac-address	Not Specified	00:00:00:00:00:00												
poe *	Enable/disable PoE status.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PoE status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PoE status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.									
Option	Description															
<i>enable</i>	Enable PoE status.															
<i>disable</i>	Disable PoE status.															
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically adjust speed.</td> </tr> <tr> <td><i>10full</i></td> <td>10M full-duplex.</td> </tr> <tr> <td><i>10half</i></td> <td>10M half-duplex.</td> </tr> <tr> <td><i>100full</i></td> <td>100M full-duplex.</td> </tr> <tr> <td><i>100half</i></td> <td>100M half-duplex.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically adjust speed.	<i>10full</i>	10M full-duplex.	<i>10half</i>	10M half-duplex.	<i>100full</i>	100M full-duplex.	<i>100half</i>	100M half-duplex.			
Option	Description															
<i>auto</i>	Automatically adjust speed.															
<i>10full</i>	10M full-duplex.															
<i>10half</i>	10M half-duplex.															
<i>100full</i>	100M full-duplex.															
<i>100half</i>	100M half-duplex.															

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1000full</i></td> <td>1000M full-duplex.</td> </tr> <tr> <td><i>1000half</i></td> <td>1000M half-duplex.</td> </tr> <tr> <td><i>1000auto</i></td> <td>1000M auto adjust.</td> </tr> </tbody> </table>	Option	Description	<i>1000full</i>	1000M full-duplex.	<i>1000half</i>	1000M half-duplex.	<i>1000auto</i>	1000M auto adjust.																					
Option	Description																													
<i>1000full</i>	1000M full-duplex.																													
<i>1000half</i>	1000M half-duplex.																													
<i>1000auto</i>	1000M auto adjust.																													
status	Bring the interface up or shut the interface down.	option	-	up																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>up</i></td> <td>Bring the interface up.</td> </tr> <tr> <td><i>down</i></td> <td>Shut the interface down.</td> </tr> </tbody> </table>	Option	Description	<i>up</i>	Bring the interface up.	<i>down</i>	Shut the interface down.																							
Option	Description																													
<i>up</i>	Bring the interface up.																													
<i>down</i>	Shut the interface down.																													
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable NETBIOS forwarding.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable NETBIOS forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable NETBIOS forwarding.	<i>enable</i>	Enable NETBIOS forwarding.																							
Option	Description																													
<i>disable</i>	Disable NETBIOS forwarding.																													
<i>enable</i>	Enable NETBIOS forwarding.																													
wins-ip	WINS server IP.	ipv4-address	Not Specified	0.0.0.0																										
type	Interface type.	option	-	vlan																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>physical</i></td> <td>Physical interface.</td> </tr> <tr> <td><i>vlan</i></td> <td>VLAN interface.</td> </tr> <tr> <td><i>aggregate</i></td> <td>Aggregate interface.</td> </tr> <tr> <td><i>redundant</i></td> <td>Redundant interface.</td> </tr> <tr> <td><i>tunnel</i></td> <td>Tunnel interface.</td> </tr> <tr> <td><i>vdom-link</i></td> <td>VDOM link interface.</td> </tr> <tr> <td><i>loopback</i></td> <td>Loopback interface.</td> </tr> <tr> <td><i>switch</i></td> <td>Software switch interface.</td> </tr> <tr> <td><i>hard-switch</i></td> <td>Hardware switch interface.</td> </tr> <tr> <td><i>vap-switch</i></td> <td>VAP interface.</td> </tr> <tr> <td><i>wl-mesh</i></td> <td>WLAN mesh interface.</td> </tr> <tr> <td><i>fext-wan</i></td> <td>FortiExtender interface.</td> </tr> </tbody> </table>	Option	Description	<i>physical</i>	Physical interface.	<i>vlan</i>	VLAN interface.	<i>aggregate</i>	Aggregate interface.	<i>redundant</i>	Redundant interface.	<i>tunnel</i>	Tunnel interface.	<i>vdom-link</i>	VDOM link interface.	<i>loopback</i>	Loopback interface.	<i>switch</i>	Software switch interface.	<i>hard-switch</i>	Hardware switch interface.	<i>vap-switch</i>	VAP interface.	<i>wl-mesh</i>	WLAN mesh interface.	<i>fext-wan</i>	FortiExtender interface.			
Option	Description																													
<i>physical</i>	Physical interface.																													
<i>vlan</i>	VLAN interface.																													
<i>aggregate</i>	Aggregate interface.																													
<i>redundant</i>	Redundant interface.																													
<i>tunnel</i>	Tunnel interface.																													
<i>vdom-link</i>	VDOM link interface.																													
<i>loopback</i>	Loopback interface.																													
<i>switch</i>	Software switch interface.																													
<i>hard-switch</i>	Hardware switch interface.																													
<i>vap-switch</i>	VAP interface.																													
<i>wl-mesh</i>	WLAN mesh interface.																													
<i>fext-wan</i>	FortiExtender interface.																													

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>vxlan</i></td> <td>VXLAN interface.</td> </tr> <tr> <td><i>geneve</i></td> <td>GENEVE interface.</td> </tr> <tr> <td><i>hdlc</i></td> <td>T1/E1 interface.</td> </tr> <tr> <td><i>switch-vlan</i></td> <td>Switch VLAN interface.</td> </tr> <tr> <td><i>emac-vlan</i></td> <td>EMAC VLAN interface.</td> </tr> </tbody> </table>	Option	Description	<i>vxlan</i>	VXLAN interface.	<i>geneve</i>	GENEVE interface.	<i>hdlc</i>	T1/E1 interface.	<i>switch-vlan</i>	Switch VLAN interface.	<i>emac-vlan</i>	EMAC VLAN interface.			
Option	Description															
<i>vxlan</i>	VXLAN interface.															
<i>geneve</i>	GENEVE interface.															
<i>hdlc</i>	T1/E1 interface.															
<i>switch-vlan</i>	Switch VLAN interface.															
<i>emac-vlan</i>	EMAC VLAN interface.															
<i>dedicated-to</i>	Configure interface for single purpose.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Interface not dedicated for any purpose.</td> </tr> <tr> <td><i>management</i></td> <td>Dedicate this interface for management purposes only.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Interface not dedicated for any purpose.	<i>management</i>	Dedicate this interface for management purposes only.									
Option	Description															
<i>none</i>	Interface not dedicated for any purpose.															
<i>management</i>	Dedicate this interface for management purposes only.															
<i>trust-ip-1</i>	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0												
<i>trust-ip-2</i>	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0												
<i>trust-ip-3</i>	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0												
<i>trust-ip6-1</i>	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0												
<i>trust-ip6-2</i>	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0												
<i>trust-ip6-3</i>	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0												
<i>mtu-override</i>	Enable to set a custom MTU for this interface.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override default MTU.</td> </tr> <tr> <td><i>disable</i></td> <td>Use default MTU (1500).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override default MTU.	<i>disable</i>	Use default MTU (1500).									
Option	Description															
<i>enable</i>	Override default MTU.															
<i>disable</i>	Use default MTU (1500).															

Parameter	Description	Type	Size	Default										
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500										
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WCCP protocol on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WCCP protocol on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WCCP protocol on this interface.	<i>disable</i>	Disable WCCP protocol on this interface.							
Option	Description													
<i>enable</i>	Enable WCCP protocol on this interface.													
<i>disable</i>	Disable WCCP protocol on this interface.													
netflow-sampler	Enable/disable NetFlow on this interface and set the data that NetFlow collects (rx, tx, or both).	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable NetFlow protocol on this interface.</td> </tr> <tr> <td><i>tx</i></td> <td>Monitor transmitted traffic on this interface.</td> </tr> <tr> <td><i>rx</i></td> <td>Monitor received traffic on this interface.</td> </tr> <tr> <td><i>both</i></td> <td>Monitor transmitted/received traffic on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable NetFlow protocol on this interface.	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.			
Option	Description													
<i>disable</i>	Disable NetFlow protocol on this interface.													
<i>tx</i>	Monitor transmitted traffic on this interface.													
<i>rx</i>	Monitor received traffic on this interface.													
<i>both</i>	Monitor transmitted/received traffic on this interface.													
sflow-sampler	Enable/disable sFlow on this interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sFlow protocol on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sFlow protocol on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sFlow protocol on this interface.	<i>disable</i>	Disable sFlow protocol on this interface.							
Option	Description													
<i>enable</i>	Enable sFlow protocol on this interface.													
<i>disable</i>	Disable sFlow protocol on this interface.													
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable drop of overlapped fragment packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable drop of overlapped fragment packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable drop of overlapped fragment packets.	<i>disable</i>	Disable drop of overlapped fragment packets.							
Option	Description													
<i>enable</i>	Enable drop of overlapped fragment packets.													
<i>disable</i>	Disable drop of overlapped fragment packets.													
drop-fragment	Enable/disable drop fragment packets.	option	-	disable										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable/disable drop fragment packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not drop fragment packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable/disable drop fragment packets.	<i>disable</i>	Do not drop fragment packets.					
Option	Description											
<i>enable</i>	Enable/disable drop fragment packets.											
<i>disable</i>	Do not drop fragment packets.											
src-check	Enable/disable source IP check.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source IP check.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source IP check.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source IP check.	<i>disable</i>	Disable source IP check.					
Option	Description											
<i>enable</i>	Enable source IP check.											
<i>disable</i>	Disable source IP check.											
sample-rate	sFlow sample rate .	integer	Minimum value: 10 Maximum value: 99999	2000								
polling-interval	sFlow polling interval .	integer	Minimum value: 1 Maximum value: 255	20								
sample-direction	Data that NetFlow collects (rx, tx, or both).	option	-	both								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tx</i></td> <td>Monitor transmitted traffic on this interface.</td> </tr> <tr> <td><i>rx</i></td> <td>Monitor received traffic on this interface.</td> </tr> <tr> <td><i>both</i></td> <td>Monitor transmitted/received traffic on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.			
Option	Description											
<i>tx</i>	Monitor transmitted traffic on this interface.											
<i>rx</i>	Monitor received traffic on this interface.											
<i>both</i>	Monitor transmitted/received traffic on this interface.											
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable explicit Web proxy on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable explicit Web proxy on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable explicit Web proxy on this interface.	<i>disable</i>	Disable explicit Web proxy on this interface.					
Option	Description											
<i>enable</i>	Enable explicit Web proxy on this interface.											
<i>disable</i>	Disable explicit Web proxy on this interface.											
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable explicit FTP proxy on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable explicit FTP proxy on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable explicit FTP proxy on this interface.	<i>disable</i>	Disable explicit FTP proxy on this interface.					
Option	Description											
<i>enable</i>	Enable explicit FTP proxy on this interface.											
<i>disable</i>	Disable explicit FTP proxy on this interface.											

Parameter	Description	Type	Size	Default						
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable proxy captive portal on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable proxy captive portal on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable proxy captive portal on this interface.	<i>disable</i>	Disable proxy captive portal on this interface.			
Option	Description									
<i>enable</i>	Enable proxy captive portal on this interface.									
<i>disable</i>	Disable proxy captive portal on this interface.									
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 0 Maximum value: 4294967295	0						
inbandwidth	Bandwidth limit for incoming traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						
outbandwidth	Bandwidth limit for outgoing traffic .	integer	Minimum value: 0 Maximum value: 16776000	0						
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35							
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35							
disconnect-threshold	Time in milliseconds to wait before sending a notification that this interface is down or disconnected.	integer	Minimum value: 0 Maximum value: 10000	0						
spillover-threshold	Egress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						
ingress-spillover-threshold	Ingress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						

Parameter	Description	Type	Size	Default						
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255	0						
interface	Interface name.	string	Maximum length: 15							
external	Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable identifying the interface as an external interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable identifying the interface as an external interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable identifying the interface as an external interface.	<i>disable</i>	Disable identifying the interface as an external interface.			
Option	Description									
<i>enable</i>	Enable identifying the interface as an external interface.									
<i>disable</i>	Disable identifying the interface as an external interface.									
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>8021q</i></td> <td>IEEE 802.1Q.</td> </tr> <tr> <td><i>8021ad</i></td> <td>IEEE 802.1AD.</td> </tr> </tbody> </table>	Option	Description	<i>8021q</i>	IEEE 802.1Q.	<i>8021ad</i>	IEEE 802.1AD.			
Option	Description									
<i>8021q</i>	IEEE 802.1Q.									
<i>8021ad</i>	IEEE 802.1AD.									
vlanid	VLAN ID .	integer	Minimum value: 1 Maximum value: 4094	0						
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 Maximum value: 2147483647	0						
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0						
member <interface-name>	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79							
lacp-mode	LACP mode.	option	-	active						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Use static aggregation, do not send and ignore any LACP messages.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.					
Option	Description									
<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.									



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>passive</i></td> <td>Passively use LACP to negotiate 802.3ad aggregation.</td> </tr> <tr> <td><i>active</i></td> <td>Actively use LACP to negotiate 802.3ad aggregation.</td> </tr> </tbody> </table>	Option	Description	<i>passive</i>	Passively use LACP to negotiate 802.3ad aggregation.	<i>active</i>	Actively use LACP to negotiate 802.3ad aggregation.			
Option	Description									
<i>passive</i>	Passively use LACP to negotiate 802.3ad aggregation.									
<i>active</i>	Actively use LACP to negotiate 802.3ad aggregation.									
lACP-ha-slave	LACP HA slave.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow HA slave to send/receive LACP messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Block HA slave from sending/receiving LACP messages.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow HA slave to send/receive LACP messages.	<i>disable</i>	Block HA slave from sending/receiving LACP messages.			
Option	Description									
<i>enable</i>	Allow HA slave to send/receive LACP messages.									
<i>disable</i>	Block HA slave from sending/receiving LACP messages.									
system-id-type	Method in which system ID is generated.	option	-	auto						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Use the MAC address of the first member.</td> </tr> <tr> <td><i>user</i></td> <td>User-defined system ID.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Use the MAC address of the first member.	<i>user</i>	User-defined system ID.			
Option	Description									
<i>auto</i>	Use the MAC address of the first member.									
<i>user</i>	User-defined system ID.									
system-id	Define a system ID for the aggregate interface.	mac-address	Not Specified	00:00:00:00:00:00						
lACP-speed	How often the interface sends LACP messages.	option	-	slow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>slow</i></td> <td>Send LACP message every 30 seconds.</td> </tr> <tr> <td><i>fast</i></td> <td>Send LACP message every second.</td> </tr> </tbody> </table>	Option	Description	<i>slow</i>	Send LACP message every 30 seconds.	<i>fast</i>	Send LACP message every second.			
Option	Description									
<i>slow</i>	Send LACP message every 30 seconds.									
<i>fast</i>	Send LACP message every second.									
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32	1						
min-links-down	Action to take when less than the configured minimum number of links are active.	option	-	operational						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>operational</i></td> <td>Set the aggregate operationally down.</td> </tr> <tr> <td><i>administrative</i></td> <td>Set the aggregate administratively down.</td> </tr> </tbody> </table>	Option	Description	<i>operational</i>	Set the aggregate operationally down.	<i>administrative</i>	Set the aggregate administratively down.			
Option	Description									
<i>operational</i>	Set the aggregate operationally down.									
<i>administrative</i>	Set the aggregate administratively down.									
algorithm	Frame distribution algorithm.	option	-	L4						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>L2</i></td> <td>Use layer 2 address for distribution.</td> </tr> <tr> <td><i>L3</i></td> <td>Use layer 3 address for distribution.</td> </tr> <tr> <td><i>L4</i></td> <td>Use layer 4 information for distribution.</td> </tr> </tbody> </table>	Option	Description	<i>L2</i>	Use layer 2 address for distribution.	<i>L3</i>	Use layer 3 address for distribution.	<i>L4</i>	Use layer 4 information for distribution.			
Option	Description											
<i>L2</i>	Use layer 2 address for distribution.											
<i>L3</i>	Use layer 3 address for distribution.											
<i>L4</i>	Use layer 4 information for distribution.											
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50								
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable fail back to higher priority port once recovered.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable fail back to higher priority port once recovered.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable fail back to higher priority port once recovered.	<i>disable</i>	Disable fail back to higher priority port once recovered.					
Option	Description											
<i>enable</i>	Enable fail back to higher priority port once recovered.											
<i>disable</i>	Disable fail back to higher priority port once recovered.											
aggregate	Aggregate interface.	string	Maximum length: 15									
redundant-interface	Redundant interface.	string	Maximum length: 15									
devindex	Device Index.	integer	Minimum value: 0 Maximum value: 4294967295	0								
vindex	Switch control interface VLAN ID.	integer	Minimum value: 0 Maximum value: 65535	0								
switch	Contained in switch.	string	Maximum length: 15									
description	Description.	var-string	Maximum length: 255									
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25									
l2tp-client *	Enable/disable this interface as a Layer 2 Tunnelling Protocol (L2TP) client.	option	-	disable								

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable L2TP client.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable L2TP client.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable L2TP client.	<i>disable</i>	Disable L2TP client.							
Option	Description													
<i>enable</i>	Enable L2TP client.													
<i>disable</i>	Disable L2TP client.													
security-mode	Turn on captive portal authentication for this interface.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No security option.</td> </tr> <tr> <td><i>captive-portal</i></td> <td>Captive portal authentication.</td> </tr> <tr> <td><i>802.1X</i></td> <td>802.1X port-based authentication.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No security option.	<i>captive-portal</i>	Captive portal authentication.	<i>802.1X</i>	802.1X port-based authentication.					
Option	Description													
<i>none</i>	No security option.													
<i>captive-portal</i>	Captive portal authentication.													
<i>802.1X</i>	802.1X port-based authentication.													
security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mac-auth-only</i></td> <td>Enable MAC authentication bypass without EAP.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable MAC authentication bypass.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MAC authentication bypass.</td> </tr> </tbody> </table>	Option	Description	<i>mac-auth-only</i>	Enable MAC authentication bypass without EAP.	<i>enable</i>	Enable MAC authentication bypass.	<i>disable</i>	Disable MAC authentication bypass.					
Option	Description													
<i>mac-auth-only</i>	Enable MAC authentication bypass without EAP.													
<i>enable</i>	Enable MAC authentication bypass.													
<i>disable</i>	Disable MAC authentication bypass.													
security-8021x-mode *	802.1X mode.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>802.1X default mode.</td> </tr> <tr> <td><i>dynamic-vlan</i></td> <td>802.1X dynamic VLAN (master) mode.</td> </tr> <tr> <td><i>fallback</i></td> <td>802.1X fallback (master) mode.</td> </tr> <tr> <td><i>slave</i></td> <td>802.1X slave mode.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	802.1X default mode.	<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.	<i>fallback</i>	802.1X fallback (master) mode.	<i>slave</i>	802.1X slave mode.			
Option	Description													
<i>default</i>	802.1X default mode.													
<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.													
<i>fallback</i>	802.1X fallback (master) mode.													
<i>slave</i>	802.1X slave mode.													
security-8021x-master *	802.1X master virtual-switch.	string	Maximum length: 15											
security-8021x-dynamic-vlan-id *	VLAN ID for virtual switch.	integer	Minimum value: 0 Maximum value: 4094	0										
security-external-web	URL of external authentication web server.	string	Maximum length: 127											
security-external-logout	URL of external authentication logout server.	string	Maximum length: 127											

Parameter	Description	Type	Size	Default								
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35									
security-redirect-url	URL redirection after disclaimer/authentication.	string	Maximum length: 127									
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35									
security-groups <name>	User groups that can authenticate with the captive portal. Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79									
stp *	Enable/disable STP.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable STP.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable STP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable STP.	<i>enable</i>	Enable STP.					
Option	Description											
<i>disable</i>	Disable STP.											
<i>enable</i>	Enable STP.											
stp-ha-slave *	Control STP behaviour on HA slave.	option	-	priority-adjust								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable STP negotiation on HA slave.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable STP negotiation on HA slave.</td> </tr> <tr> <td><i>priority-adjust</i></td> <td>Enable STP negotiation on HA slave and make priority lower than HA master.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable STP negotiation on HA slave.	<i>enable</i>	Enable STP negotiation on HA slave.	<i>priority-adjust</i>	Enable STP negotiation on HA slave and make priority lower than HA master.			
Option	Description											
<i>disable</i>	Disable STP negotiation on HA slave.											
<i>enable</i>	Enable STP negotiation on HA slave.											
<i>priority-adjust</i>	Enable STP negotiation on HA slave and make priority lower than HA master.											
device-identification	Enable/disable passively gathering of device identity information about the devices on the network connected to this interface.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable passive gathering of identity information about hosts.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable passive gathering of identity information about hosts.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable passive gathering of identity information about hosts.	<i>disable</i>	Disable passive gathering of identity information about hosts.					
Option	Description											
<i>enable</i>	Enable passive gathering of identity information about hosts.											
<i>disable</i>	Disable passive gathering of identity information about hosts.											
device-user-identification	Enable/disable passive gathering of user identity information about users on this interface.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable passive gathering of user identity information about users.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable passive gathering of user identity information about users.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable passive gathering of user identity information about users.	<i>disable</i>	Disable passive gathering of user identity information about users.					
Option	Description											
<i>enable</i>	Enable passive gathering of user identity information about users.											
<i>disable</i>	Disable passive gathering of user identity information about users.											

Parameter	Description	Type	Size	Default								
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable reception of Link Layer Discovery Protocol (LLDP).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable reception of Link Layer Discovery Protocol (LLDP).</td> </tr> <tr> <td><i>vdom</i></td> <td>Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).	<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.			
Option	Description											
<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).											
<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).											
<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.											
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable transmission of Link Layer Discovery Protocol (LLDP).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable transmission of Link Layer Discovery Protocol (LLDP).</td> </tr> <tr> <td><i>vdom</i></td> <td>Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).	<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.			
Option	Description											
<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).											
<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).											
<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.											
lldp-network-policy	LLDP-MED network policy profile.	string	Maximum length: 35									
estimated-upstream-bandwidth	Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295	0								
estimated-downstream-bandwidth	Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295	0								
measured-upstream-bandwidth	Measured upstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0								
measured-downstream-bandwidth	Measured downstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0								

Parameter	Description	Type	Size	Default										
bandwidth-measure-time	Bandwidth measure time	integer	Minimum value: 0 Maximum value: 4294967295	0										
monitor-bandwidth	Enable monitoring bandwidth on this interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable monitoring bandwidth on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable monitoring bandwidth on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable monitoring bandwidth on this interface.	<i>disable</i>	Disable monitoring bandwidth on this interface.							
Option	Description													
<i>enable</i>	Enable monitoring bandwidth on this interface.													
<i>disable</i>	Disable monitoring bandwidth on this interface.													
vrrp-virtual-mac	Enable/disable use of virtual MAC for VRRP.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of virtual MAC for VRRP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of virtual MAC for VRRP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of virtual MAC for VRRP.	<i>disable</i>	Disable use of virtual MAC for VRRP.							
Option	Description													
<i>enable</i>	Enable use of virtual MAC for VRRP.													
<i>disable</i>	Disable use of virtual MAC for VRRP.													
role	Interface role.	option	-	undefined										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>lan</i></td> <td>Connected to local network of endpoints.</td> </tr> <tr> <td><i>wan</i></td> <td>Connected to Internet.</td> </tr> <tr> <td><i>dmz</i></td> <td>Connected to server zone.</td> </tr> <tr> <td><i>undefined</i></td> <td>Interface has no specific role.</td> </tr> </tbody> </table>	Option	Description	<i>lan</i>	Connected to local network of endpoints.	<i>wan</i>	Connected to Internet.	<i>dmz</i>	Connected to server zone.	<i>undefined</i>	Interface has no specific role.			
Option	Description													
<i>lan</i>	Connected to local network of endpoints.													
<i>wan</i>	Connected to Internet.													
<i>dmz</i>	Connected to server zone.													
<i>undefined</i>	Interface has no specific role.													
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 1 Maximum value: 2147483647	0										
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable secondary IP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable secondary IP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable secondary IP.	<i>disable</i>	Disable secondary IP.							
Option	Description													
<i>enable</i>	Enable secondary IP.													
<i>disable</i>	Disable secondary IP.													
preserve-session-route	Enable/disable preservation of session route when dirty.	option	-	disable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable preservation of session route when dirty.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable preservation of session route when dirty.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable preservation of session route when dirty.	<i>disable</i>	Disable preservation of session route when dirty.			
Option	Description									
<i>enable</i>	Enable preservation of session route when dirty.									
<i>disable</i>	Disable preservation of session route when dirty.									
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension device on this interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic authorization of dedicated Fortinet extension device on this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic authorization of dedicated Fortinet extension device on this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.			
Option	Description									
<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.									
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.									
ap-discover	Enable/disable automatic registration of unknown FortiAP devices.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic registration of unknown FortiAP devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic registration of unknown FortiAP devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.	<i>disable</i>	Disable automatic registration of unknown FortiAP devices.			
Option	Description									
<i>enable</i>	Enable automatic registration of unknown FortiAP devices.									
<i>disable</i>	Disable automatic registration of unknown FortiAP devices.									
fortilink-stacking	Enable/disable FortiLink switch-stacking on this interface.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiLink switch stacking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiLink switch stacking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiLink switch stacking.	<i>disable</i>	Disable FortiLink switch stacking.			
Option	Description									
<i>enable</i>	Enable FortiLink switch stacking.									
<i>disable</i>	Disable FortiLink switch stacking.									
fortilink-neighbor-detect	Protocol for FortiGate neighbor discovery.	option	-	fortilink						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>lldp</i></td> <td>Detect FortiLink neighbors using LLDP protocol.</td> </tr> <tr> <td><i>fortilink</i></td> <td>Detect FortiLink neighbors using FortiLink protocol.</td> </tr> </tbody> </table>	Option	Description	<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.	<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.			
Option	Description									
<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.									
<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.									
ip-managed-by-fortiipam	Enable/disable automatic IP address assignment of this interface by FortiIPAM.	option	-	disable						

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic IP address assignment of this interface by FortiPAM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic IP address assignment of this interface by FortiPAM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic IP address assignment of this interface by FortiPAM.	<i>disable</i>	Disable automatic IP address assignment of this interface by FortiPAM.																	
Option	Description																							
<i>enable</i>	Enable automatic IP address assignment of this interface by FortiPAM.																							
<i>disable</i>	Disable automatic IP address assignment of this interface by FortiPAM.																							
managed-subnetwork-size	Number of IP addresses to be allocated by FortiPAM and used by this FortiGate unit's DHCP server settings.	option	-	256																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>256</td> <td>Allocate a subnet with 256 IP addresses.</td> </tr> <tr> <td>512</td> <td>Allocate a subnet with 512 IP addresses.</td> </tr> <tr> <td>1024</td> <td>Allocate a subnet with 1024 IP addresses.</td> </tr> <tr> <td>2048</td> <td>Allocate a subnet with 2048 IP addresses.</td> </tr> <tr> <td>4096</td> <td>Allocate a subnet with 4096 IP addresses.</td> </tr> <tr> <td>8192</td> <td>Allocate a subnet with 8192 IP addresses.</td> </tr> <tr> <td>16384</td> <td>Allocate a subnet with 16384 IP addresses.</td> </tr> <tr> <td>32768</td> <td>Allocate a subnet with 32768 IP addresses.</td> </tr> <tr> <td>65536</td> <td>Allocate a subnet with 65536 IP addresses.</td> </tr> </tbody> </table>	Option	Description	256	Allocate a subnet with 256 IP addresses.	512	Allocate a subnet with 512 IP addresses.	1024	Allocate a subnet with 1024 IP addresses.	2048	Allocate a subnet with 2048 IP addresses.	4096	Allocate a subnet with 4096 IP addresses.	8192	Allocate a subnet with 8192 IP addresses.	16384	Allocate a subnet with 16384 IP addresses.	32768	Allocate a subnet with 32768 IP addresses.	65536	Allocate a subnet with 65536 IP addresses.			
Option	Description																							
256	Allocate a subnet with 256 IP addresses.																							
512	Allocate a subnet with 512 IP addresses.																							
1024	Allocate a subnet with 1024 IP addresses.																							
2048	Allocate a subnet with 2048 IP addresses.																							
4096	Allocate a subnet with 4096 IP addresses.																							
8192	Allocate a subnet with 8192 IP addresses.																							
16384	Allocate a subnet with 16384 IP addresses.																							
32768	Allocate a subnet with 32768 IP addresses.																							
65536	Allocate a subnet with 65536 IP addresses.																							
fortilink-split-interface	Enable/disable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiLink split interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	<i>disable</i>	Disable FortiLink split interface.																	
Option	Description																							
<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.																							
<i>disable</i>	Disable FortiLink split interface.																							
internal	Implicitly created.	integer	Minimum value: 0 Maximum value: 255	0																				
fortilink-backup-link	fortilink split interface backup link.	integer	Minimum value: 0 Maximum value: 255	0																				



Parameter	Description	Type	Size	Default						
switch-controller-access-vlan	Block FortiSwitch port-to-port traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow normal VLAN traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.	<i>disable</i>	Allow normal VLAN traffic.			
Option	Description									
<i>enable</i>	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.									
<i>disable</i>	Allow normal VLAN traffic.									
switch-controller-traffic-policy	Switch controller traffic policy for the VLAN.	string	Maximum length: 63							
switch-controller-rspan-mode	Stop Layer2 MAC learning and interception of BPDUs and other packets on this interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable RSPAN passthrough mode on this VLAN interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable RSPAN passthrough mode on this VLAN interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable RSPAN passthrough mode on this VLAN interface.	<i>enable</i>	Enable RSPAN passthrough mode on this VLAN interface.			
Option	Description									
<i>disable</i>	Disable RSPAN passthrough mode on this VLAN interface.									
<i>enable</i>	Enable RSPAN passthrough mode on this VLAN interface.									
switch-controller-mgmt-vlan	VLAN to use for FortiLink management purposes.	integer	Minimum value: 1 Maximum value: 4094	4094						
switch-controller-igmp-snooping	Switch controller IGMP snooping.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IGMP snooping.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IGMP snooping.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IGMP snooping.	<i>disable</i>	Disable IGMP snooping.			
Option	Description									
<i>enable</i>	Enable IGMP snooping.									
<i>disable</i>	Disable IGMP snooping.									
switch-controller-igmp-snooping-proxy	Switch controller IGMP snooping proxy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IGMP snooping proxy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IGMP snooping proxy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IGMP snooping proxy.	<i>disable</i>	Disable IGMP snooping proxy.			
Option	Description									
<i>enable</i>	Enable IGMP snooping proxy.									
<i>disable</i>	Disable IGMP snooping proxy.									
switch-controller-igmp-snooping-fast-leave	Switch controller IGMP snooping fast-leave.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IGMP snooping fast-leave.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IGMP snooping fast-leave.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IGMP snooping fast-leave.	<i>disable</i>	Disable IGMP snooping fast-leave.			
Option	Description									
<i>enable</i>	Enable IGMP snooping fast-leave.									
<i>disable</i>	Disable IGMP snooping fast-leave.									
switch-controller-dhcp-snooping	Switch controller DHCP snooping.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCP snooping for FortiSwitch devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP snooping for FortiSwitch devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCP snooping for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable DHCP snooping for FortiSwitch devices.									
<i>disable</i>	Disable DHCP snooping for FortiSwitch devices.									
switch-controller-dhcp-snooping-verify-mac	Switch controller DHCP snooping verify MAC.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCP snooping verify source MAC for FortiSwitch devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP snooping verify source MAC for FortiSwitch devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.									
<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.									
switch-controller-dhcp-snooping-option82	Switch controller DHCP snooping option82.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCP snooping insert option82 for FortiSwitch devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP snooping insert option82 for FortiSwitch devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.									
<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.									
switch-controller-arp-inspection	Enable/disable FortiSwitch ARP inspection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ARP inspection for FortiSwitch devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ARP inspection for FortiSwitch devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ARP inspection for FortiSwitch devices.	<i>disable</i>	Disable ARP inspection for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable ARP inspection for FortiSwitch devices.									
<i>disable</i>	Disable ARP inspection for FortiSwitch devices.									
switch-controller-learning-limit	Limit the number of dynamic MAC addresses on this VLAN .	integer	Minimum value: 0 Maximum value: 128	0						
switch-controller-nac	Integrated NAC settings for managed FortiSwitch.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default																
switch-controller-feature	Interface's purpose when assigning traffic (read only).	option	-	none																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>VLAN for generic purpose.</td> </tr> <tr> <td><i>default-vlan</i></td> <td>Default VLAN (native) assigned to all switch ports upon discovery.</td> </tr> <tr> <td><i>quarantine</i></td> <td>VLAN for quarantined traffic.</td> </tr> <tr> <td><i>rspan</i></td> <td>VLAN for RSPAN/ERSPAN mirrored traffic.</td> </tr> <tr> <td><i>voice</i></td> <td>VLAN dedicated for voice devices.</td> </tr> <tr> <td><i>video</i></td> <td>VLAN dedicated for camera devices.</td> </tr> <tr> <td><i>nac</i></td> <td>VLAN dedicated for NAC onboarding devices.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	VLAN for generic purpose.	<i>default-vlan</i>	Default VLAN (native) assigned to all switch ports upon discovery.	<i>quarantine</i>	VLAN for quarantined traffic.	<i>rspan</i>	VLAN for RSPAN/ERSPAN mirrored traffic.	<i>voice</i>	VLAN dedicated for voice devices.	<i>video</i>	VLAN dedicated for camera devices.	<i>nac</i>	VLAN dedicated for NAC onboarding devices.			
Option	Description																			
<i>none</i>	VLAN for generic purpose.																			
<i>default-vlan</i>	Default VLAN (native) assigned to all switch ports upon discovery.																			
<i>quarantine</i>	VLAN for quarantined traffic.																			
<i>rspan</i>	VLAN for RSPAN/ERSPAN mirrored traffic.																			
<i>voice</i>	VLAN dedicated for voice devices.																			
<i>video</i>	VLAN dedicated for camera devices.																			
<i>nac</i>	VLAN dedicated for NAC onboarding devices.																			
switch-controller-iot-scanning	Enable/disable managed FortiSwitch IoT scanning.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IoT scanning for managed FortiSwitch devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IoT scanning for managed FortiSwitch devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IoT scanning for managed FortiSwitch devices.	<i>disable</i>	Disable IoT scanning for managed FortiSwitch devices.													
Option	Description																			
<i>enable</i>	Enable IoT scanning for managed FortiSwitch devices.																			
<i>disable</i>	Disable IoT scanning for managed FortiSwitch devices.																			
swc-vlan	Creation status for switch-controller VLANs.	integer	Minimum value: 0 Maximum value: 4294967295	0																
swc-first-create	Initial create for switch-controller VLANs.	integer	Minimum value: 0 Maximum value: 4294967295	0																
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0																

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config client-options

Parameter	Description	Type	Size	Default										
code	DHCP client option code.	integer	Minimum value: 0 Maximum value: 255	0										
type	DHCP client option type.	option	-	hex										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hex</i></td> <td>DHCP option in hex.</td> </tr> <tr> <td><i>string</i></td> <td>DHCP option in string.</td> </tr> <tr> <td><i>ip</i></td> <td>DHCP option in IP.</td> </tr> <tr> <td><i>fqdn</i></td> <td>DHCP option in domain search option format.</td> </tr> </tbody> </table>	Option	Description	<i>hex</i>	DHCP option in hex.	<i>string</i>	DHCP option in string.	<i>ip</i>	DHCP option in IP.	<i>fqdn</i>	DHCP option in domain search option format.			
Option	Description													
<i>hex</i>	DHCP option in hex.													
<i>string</i>	DHCP option in string.													
<i>ip</i>	DHCP option in IP.													
<i>fqdn</i>	DHCP option in domain search option format.													
value	DHCP client option value.	string	Maximum length: 312											
ip	DHCP option IPs.	user	Not Specified											

## config l2tp-client-settings

Parameter	Description	Type	Size	Default						
user	L2TP user name.	string	Maximum length: 127							
password	L2TP password.	password	Not Specified							
peer-host	L2TP peer host address.	string	Maximum length: 255							
peer-mask	L2TP peer mask.	ipv4-netmask	Not Specified	255.255.255.255						
peer-port	L2TP peer port number.	integer	Minimum value: 1 Maximum value: 65535	1701						
auth-type	L2TP authentication type.	option	-	auto						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically choose authentication.</td> </tr> <tr> <td><i>pap</i></td> <td>PAP authentication.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.			
Option	Description									
<i>auto</i>	Automatically choose authentication.									
<i>pap</i>	PAP authentication.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>chap</i></td> <td>CHAP authentication.</td> </tr> <tr> <td><i>mschapv1</i></td> <td>MS-CHAPv1 authentication.</td> </tr> <tr> <td><i>mschapv2</i></td> <td>MS-CHAPv2 authentication.</td> </tr> </tbody> </table>	Option	Description	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.			
Option	Description											
<i>chap</i>	CHAP authentication.											
<i>mschapv1</i>	MS-CHAPv1 authentication.											
<i>mschapv2</i>	MS-CHAPv2 authentication.											
mtu	L2TP MTU.	integer	Minimum value: 40 Maximum value: 65535	1460								
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255	2								
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295	0								
defaultgw	Enable/disable default gateway.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable default gateway.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable default gateway.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable default gateway.	<i>disable</i>	Disable default gateway.					
Option	Description											
<i>enable</i>	Enable default gateway.											
<i>disable</i>	Disable default gateway.											
ip	IP.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								

### config vrrp

Parameter	Description	Type	Size	Default						
version	VRRP version.	option	-	2						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>VRRP version 2.</td> </tr> <tr> <td>3</td> <td>VRRP version 3.</td> </tr> </tbody> </table>	Option	Description	2	VRRP version 2.	3	VRRP version 3.			
Option	Description									
2	VRRP version 2.									
3	VRRP version 3.									

Parameter	Description	Type	Size	Default						
vrgroup	VRRP group ID .	integer	Minimum value: 1 Maximum value: 65535	0						
vrip	IP address of the virtual router.	ipv4-address-any	Not Specified	0.0.0.0						
priority	Priority of the virtual router .	integer	Minimum value: 1 Maximum value: 255	100						
adv-interval	Advertisement interval .	integer	Minimum value: 1 Maximum value: 255	1						
start-time	Startup time .	integer	Minimum value: 1 Maximum value: 255	3						
preempt	Enable/disable preempt mode.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable preempt mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable preempt mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable preempt mode.	<i>disable</i>	Disable preempt mode.			
Option	Description									
<i>enable</i>	Enable preempt mode.									
<i>disable</i>	Disable preempt mode.									
accept-mode	Enable/disable accept mode.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable accept mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable accept mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable accept mode.	<i>disable</i>	Disable accept mode.			
Option	Description									
<i>enable</i>	Enable accept mode.									
<i>disable</i>	Disable accept mode.									
vrdest	Monitor the route to this destination.	ipv4-address-any	Not Specified							
vrdest-priority	Priority of the virtual router when the virtual router destination becomes unreachable .	integer	Minimum value: 0 Maximum value: 254	0						
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ignoring of default route when checking destination.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ignoring of default route when checking destination.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ignoring of default route when checking destination.	<i>disable</i>	Disable ignoring of default route when checking destination.			
Option	Description									
<i>enable</i>	Enable ignoring of default route when checking destination.									
<i>disable</i>	Disable ignoring of default route when checking destination.									
status	Enable/disable this VRRP configuration.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this VRRP configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this VRRP configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this VRRP configuration.	<i>disable</i>	Disable this VRRP configuration.			
Option	Description									
<i>enable</i>	Enable this VRRP configuration.									
<i>disable</i>	Disable this VRRP configuration.									

### config proxy-arp

Parameter	Description	Type	Size	Default
ip	Set IP addresses of proxy ARP.	user	Not Specified	

### config secondaryip

Parameter	Description	Type	Size	Default																				
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																				
allowaccess	Management access settings for the secondary IP address.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>fgfm</i></td> <td>FortiManager access.</td> </tr> <tr> <td><i>radius-acct</i></td> <td>RADIUS accounting access.</td> </tr> <tr> <td><i>probe-response</i></td> <td>Probe access.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.			
Option	Description																							
<i>ping</i>	PING access.																							
<i>https</i>	HTTPS access.																							
<i>ssh</i>	SSH access.																							
<i>snmp</i>	SNMP access.																							
<i>http</i>	HTTP access.																							
<i>telnet</i>	TELNET access.																							
<i>fgfm</i>	FortiManager access.																							
<i>radius-acct</i>	RADIUS accounting access.																							
<i>probe-response</i>	Probe access.																							

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fabric</i></td> <td>Security Fabric access.</td> </tr> <tr> <td><i>ftm</i></td> <td>FTM access.</td> </tr> </tbody> </table>	Option	Description	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.					
Option	Description											
<i>fabric</i>	Security Fabric access.											
<i>ftm</i>	FTM access.											
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable detect gateway alive for first.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable detect gateway alive for first.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable detect gateway alive for first.	<i>disable</i>	Disable detect gateway alive for first.					
Option	Description											
<i>enable</i>	Enable detect gateway alive for first.											
<i>disable</i>	Disable detect gateway alive for first.											
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0								
detectserver	Gateway's ping server for this IP.	user	Not Specified									
detectprotocol	Protocols used to detect the server.	option	-	ping								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING.</td> </tr> <tr> <td><i>tcp-echo</i></td> <td>TCP echo.</td> </tr> <tr> <td><i>udp-echo</i></td> <td>UDP echo.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING.	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.			
Option	Description											
<i>ping</i>	PING.											
<i>tcp-echo</i>	TCP echo.											
<i>udp-echo</i>	UDP echo.											
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1								

### config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	



## config ipv6

Parameter	Description	Type	Size	Default										
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-	static										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Static setting.</td> </tr> <tr> <td><i>dhcp</i></td> <td>DHCPv6 client mode.</td> </tr> <tr> <td><i>pppoe</i></td> <td>IPv6 over PPPoE mode.</td> </tr> <tr> <td><i>delegated</i></td> <td>IPv6 address with delegated prefix.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	DHCPv6 client mode.	<i>pppoe</i>	IPv6 over PPPoE mode.	<i>delegated</i>	IPv6 address with delegated prefix.			
Option	Description													
<i>static</i>	Static setting.													
<i>dhcp</i>	DHCPv6 client mode.													
<i>pppoe</i>	IPv6 over PPPoE mode.													
<i>delegated</i>	IPv6 address with delegated prefix.													
nd-mode	Neighbor discovery mode.	option	-	basic										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>basic</i></td> <td>Do not support SEND.</td> </tr> <tr> <td><i>SEND-compatible</i></td> <td>Support SEND.</td> </tr> </tbody> </table>	Option	Description	<i>basic</i>	Do not support SEND.	<i>SEND-compatible</i>	Support SEND.							
Option	Description													
<i>basic</i>	Do not support SEND.													
<i>SEND-compatible</i>	Support SEND.													
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35											
nd-security-level	Neighbor discovery security level .	integer	Minimum value: 0 Maximum value: 7	0										
nd-timestamp-delta	Neighbor discovery timestamp delta value .	integer	Minimum value: 1 Maximum value: 3600	300										
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor .	integer	Minimum value: 1 Maximum value: 60	1										
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified											
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable using the DNS server acquired by DHCP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable using the DNS server acquired by DHCP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable using the DNS server acquired by DHCP.	<i>disable</i>	Disable using the DNS server acquired by DHCP.							
Option	Description													
<i>enable</i>	Enable using the DNS server acquired by DHCP.													
<i>disable</i>	Disable using the DNS server acquired by DHCP.													

Parameter	Description	Type	Size	Default																		
ip6-address	Primary IPv6 address prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx	ipv6-prefix	Not Specified	::/0																		
ip6-allowaccess	Allow management access to the interface.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>fgfm</i></td> <td>FortiManager access.</td> </tr> <tr> <td><i>fabric</i></td> <td>Fabric access.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>fabric</i>	Fabric access.			
Option	Description																					
<i>ping</i>	PING access.																					
<i>https</i>	HTTPS access.																					
<i>ssh</i>	SSH access.																					
<i>snmp</i>	SNMP access.																					
<i>http</i>	HTTP access.																					
<i>telnet</i>	TELNET access.																					
<i>fgfm</i>	FortiManager access.																					
<i>fabric</i>	Fabric access.																					
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending advertisements about this interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending advertisements about this interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending advertisements about this interface.	<i>disable</i>	Disable sending advertisements about this interface.															
Option	Description																					
<i>enable</i>	Enable sending advertisements about this interface.																					
<i>disable</i>	Disable sending advertisements about this interface.																					
icmp6-send-redirect	Enable/disable sending of ICMPv6 redirects.	option	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of ICMPv6 redirects.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of ICMPv6 redirects.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of ICMPv6 redirects.	<i>disable</i>	Disable sending of ICMPv6 redirects.															
Option	Description																					
<i>enable</i>	Enable sending of ICMPv6 redirects.																					
<i>disable</i>	Disable sending of ICMPv6 redirects.																					
ip6-manage-flag	Enable/disable the managed flag.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the managed IPv6 flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the managed IPv6 flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the managed IPv6 flag.	<i>disable</i>	Disable the managed IPv6 flag.															
Option	Description																					
<i>enable</i>	Enable the managed IPv6 flag.																					
<i>disable</i>	Disable the managed IPv6 flag.																					
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-	disable																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the other IPv6 flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the other IPv6 flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the other IPv6 flag.	<i>disable</i>	Disable the other IPv6 flag.			
Option	Description									
<i>enable</i>	Enable the other IPv6 flag.									
<i>disable</i>	Disable the other IPv6 flag.									
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800	600						
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350	198						
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000	0						
ra-send-mtu	Enable/disable sending link MTU in RA packet.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending link MTU in RA packet.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending link MTU in RA packet.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending link MTU in RA packet.	<i>disable</i>	Disable sending link MTU in RA packet.			
Option	Description									
<i>enable</i>	Enable sending link MTU in RA packet.									
<i>disable</i>	Disable sending link MTU in RA packet.									
ip6-reachable-time	IPv6 reachable time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 3600000	0						
ip6-retrans-time	IPv6 retransmit time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000	1800						
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default								
autoconf	Enable/disable address auto config.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auto-configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable auto-configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auto-configuration.	<i>disable</i>	Disable auto-configuration.					
Option	Description											
<i>enable</i>	Enable auto-configuration.											
<i>disable</i>	Disable auto-configuration.											
unique-autoconf-addr	Enable/disable unique auto config address.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable unique auto-configuration address.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable unique auto-configuration address.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable unique auto-configuration address.	<i>disable</i>	Disable unique auto-configuration address.					
Option	Description											
<i>enable</i>	Enable unique auto-configuration address.											
<i>disable</i>	Disable unique auto-configuration address.											
interface-identifier	IPv6 interface identifier.	ipv6-address	Not Specified	::								
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15									
ip6-subnet	Subnet to routing prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx	ipv6-prefix	Not Specified	::/0								
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DHCPv6 relay</td> </tr> <tr> <td><i>enable</i></td> <td>Enable DHCPv6 relay.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DHCPv6 relay	<i>enable</i>	Enable DHCPv6 relay.					
Option	Description											
<i>disable</i>	Disable DHCPv6 relay											
<i>enable</i>	Enable DHCPv6 relay.											
dhcp6-relay-type	DHCPv6 relay type.	option	-	regular								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>Regular DHCP relay.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	Regular DHCP relay.							
Option	Description											
<i>regular</i>	Regular DHCP relay.											
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified									
dhcp6-client-options	DHCPv6 client options.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rapid</i></td> <td>Send rapid commit option.</td> </tr> <tr> <td><i>iapd</i></td> <td>Send including IA-PD option.</td> </tr> <tr> <td><i>iana</i></td> <td>Send including IA-NA option.</td> </tr> </tbody> </table>	Option	Description	<i>rapid</i>	Send rapid commit option.	<i>iapd</i>	Send including IA-PD option.	<i>iana</i>	Send including IA-NA option.			
Option	Description											
<i>rapid</i>	Send rapid commit option.											
<i>iapd</i>	Send including IA-PD option.											
<i>iana</i>	Send including IA-NA option.											

Parameter	Description	Type	Size	Default						
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCPv6 prefix delegation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCPv6 prefix delegation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCPv6 prefix delegation.	<i>disable</i>	Disable DHCPv6 prefix delegation.			
Option	Description									
<i>enable</i>	Enable DHCPv6 prefix delegation.									
<i>disable</i>	Disable DHCPv6 prefix delegation.									
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCPv6 information request.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCPv6 information request.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCPv6 information request.	<i>disable</i>	Disable DHCPv6 information request.			
Option	Description									
<i>enable</i>	Enable DHCPv6 information request.									
<i>disable</i>	Disable DHCPv6 information request.									
dhcp6-prefix-hint	DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.	ipv6-network	Not Specified	::/0						
dhcp6-prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 Maximum value: 4294967295	604800						
dhcp6-prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000						
vrrp-virtual-mac6	Enable/disable virtual MAC for VRRP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable virtual MAC for VRRP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable virtual MAC for VRRP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable virtual MAC for VRRP.	<i>disable</i>	Disable virtual MAC for VRRP.			
Option	Description									
<i>enable</i>	Enable virtual MAC for VRRP.									
<i>disable</i>	Disable virtual MAC for VRRP.									
vrip6_link_local	Link-local IPv6 address of virtual router.	ipv6-address	Not Specified	::						

### config ip6-prefix-list

Parameter	Description	Type	Size	Default
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the autonomous flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the autonomous flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the autonomous flag.	<i>disable</i>	Disable the autonomous flag.			
Option	Description									
<i>enable</i>	Enable the autonomous flag.									
<i>disable</i>	Disable the autonomous flag.									
onlink-flag	Enable/disable the onlink flag.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the onlink flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the onlink flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the onlink flag.	<i>disable</i>	Disable the onlink flag.			
Option	Description									
<i>enable</i>	Enable the onlink flag.									
<i>disable</i>	Disable the onlink flag.									
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000						
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	604800						
rdnss	Recursive DNS server option.	user	Not Specified							
dnssl <domain>	DNS search list option. Domain name.	string	Maximum length: 79							

### config ip6-delegated-prefix-list

Parameter	Description	Type	Size	Default						
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15							
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the autonomous flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the autonomous flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the autonomous flag.	<i>disable</i>	Disable the autonomous flag.			
Option	Description									
<i>enable</i>	Enable the autonomous flag.									
<i>disable</i>	Disable the autonomous flag.									
onlink-flag	Enable/disable the onlink flag.	option	-	enable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the onlink flag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the onlink flag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the onlink flag.	<i>disable</i>	Disable the onlink flag.					
Option	Description											
<i>enable</i>	Enable the onlink flag.											
<i>disable</i>	Disable the onlink flag.											
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified	::/0								
rdnss-service	Recursive DNS service option.	option	-	specify								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>delegated</i></td> <td>Delegated RDNSS settings.</td> </tr> <tr> <td><i>default</i></td> <td>System RDNSS settings.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify recursive DNS servers.</td> </tr> </tbody> </table>	Option	Description	<i>delegated</i>	Delegated RDNSS settings.	<i>default</i>	System RDNSS settings.	<i>specify</i>	Specify recursive DNS servers.			
Option	Description											
<i>delegated</i>	Delegated RDNSS settings.											
<i>default</i>	System RDNSS settings.											
<i>specify</i>	Specify recursive DNS servers.											
rdnss	Recursive DNS server option.	user	Not Specified									

### config vrrp6

Parameter	Description	Type	Size	Default
vrgroup	VRRP group ID .	integer	Minimum value: 1 Maximum value: 65535	0
vrip6	IPv6 address of the virtual router.	ipv6-address	Not Specified	::
priority	Priority of the virtual router .	integer	Minimum value: 1 Maximum value: 255	100
adv-interval	Advertisement interval .	integer	Minimum value: 1 Maximum value: 255	1
start-time	Startup time .	integer	Minimum value: 1 Maximum value: 255	3
preempt	Enable/disable preempt mode.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable preempt mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable preempt mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable preempt mode.	<i>disable</i>	Disable preempt mode.			
Option	Description									
<i>enable</i>	Enable preempt mode.									
<i>disable</i>	Disable preempt mode.									
accept-mode	Enable/disable accept mode.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable accept mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable accept mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable accept mode.	<i>disable</i>	Disable accept mode.			
Option	Description									
<i>enable</i>	Enable accept mode.									
<i>disable</i>	Disable accept mode.									
vrdst6	Monitor the route to this destination.	ipv6-address	Not Specified							
status	Enable/disable VRRP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VRRP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VRRP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VRRP.	<i>disable</i>	Disable VRRP.			
Option	Description									
<i>enable</i>	Enable VRRP.									
<i>disable</i>	Disable VRRP.									

## config system physical-switch



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E. It is not available for FortiGate 501E, FortiGate 3000D, FortiGate VM64.

Configure physical switches.

```
config system physical-switch
  Description: Configure physical switches.
  edit <name>
    set age-enable [enable|disable]
    set age-val {integer}
  next
end
```

## config system physical-switch

Parameter	Description	Type	Size	Default
age-enable	Enable/disable layer 2 age timer.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable layer 2 ageing timer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable layer 2 ageing timer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable layer 2 ageing timer.	<i>disable</i>	Disable layer 2 ageing timer.			
Option	Description									
<i>enable</i>	Enable layer 2 ageing timer.									
<i>disable</i>	Disable layer 2 ageing timer.									
age-val	Layer 2 table age timer value.	integer	Minimum value: 0 Maximum value: 4294967295	3158067						

## config system virtual-switch



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E. It is not available for FortiGate 501E, FortiGate 3000D, FortiGate VM64.

Configure virtual hardware switch interfaces.

```
config system virtual-switch
  Description: Configure virtual hardware switch interfaces.
  edit <name>
    set physical-switch {string}
    config port
      Description: Configure member ports.
      edit <name>
        set alias {string}
        set poe [enable|disable]
      next
    end
    set span [disable|enable]
    set span-source-port {string}
    set span-dest-port {string}
    set span-direction [rx|tx|...]
  next
end
```

## config system virtual-switch

Parameter	Description	Type	Size	Default
physical-switch	Physical switch parent.	string	Maximum length: 15	
span	Enable/disable SPAN.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SPAN.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SPAN.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SPAN.	<i>enable</i>	Enable SPAN.					
Option	Description											
<i>disable</i>	Disable SPAN.											
<i>enable</i>	Enable SPAN.											
span-source-port	SPAN source port.	string	Maximum length: 15									
span-dest-port	SPAN destination port.	string	Maximum length: 15									
span-direction	SPAN direction.	option	-	both								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rx</i></td> <td>SPAN receive direction only.</td> </tr> <tr> <td><i>tx</i></td> <td>SPAN transmit direction only.</td> </tr> <tr> <td><i>both</i></td> <td>SPAN both directions.</td> </tr> </tbody> </table>	Option	Description	<i>rx</i>	SPAN receive direction only.	<i>tx</i>	SPAN transmit direction only.	<i>both</i>	SPAN both directions.			
Option	Description											
<i>rx</i>	SPAN receive direction only.											
<i>tx</i>	SPAN transmit direction only.											
<i>both</i>	SPAN both directions.											

## config port

Parameter	Description	Type	Size	Default						
alias	Alias.	string	Maximum length: 25							
poe *	Enable/disable PoE status.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PoE status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PoE status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.			
Option	Description									
<i>enable</i>	Enable PoE status.									
<i>disable</i>	Disable PoE status.									

\* This parameter may not exist in some models.

## config system stp



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E. It is not available for FortiGate 501E, FortiGate 3000D, FortiGate VM64.

Configure Spanning Tree Protocol (STP).

```
config system stp
  Description: Configure Spanning Tree Protocol (STP).
  set switch-priority [0|4096|...]
  set hello-time {integer}
```

```

set forward-delay {integer}
set max-age {integer}
set max-hops {integer}
end

```

## config system stp

Parameter	Description	Type	Size	Default																																
switch-priority	STP switch priority; the lower the number the higher the priority (select from 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, and 57344).	option	-	32768																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td></tr> <tr><td>4096</td><td>4096</td></tr> <tr><td>8192</td><td>8192</td></tr> <tr><td>12288</td><td>12288</td></tr> <tr><td>16384</td><td>16384</td></tr> <tr><td>20480</td><td>20480</td></tr> <tr><td>24576</td><td>24576</td></tr> <tr><td>28672</td><td>28672</td></tr> <tr><td>32768</td><td>32768</td></tr> <tr><td>36864</td><td>36864</td></tr> <tr><td>40960</td><td>40960</td></tr> <tr><td>45056</td><td>45056</td></tr> <tr><td>49152</td><td>49152</td></tr> <tr><td>53248</td><td>53248</td></tr> <tr><td>57344</td><td>57344</td></tr> </tbody> </table>	Option	Description	0	0	4096	4096	8192	8192	12288	12288	16384	16384	20480	20480	24576	24576	28672	28672	32768	32768	36864	36864	40960	40960	45056	45056	49152	49152	53248	53248	57344	57344			
Option	Description																																			
0	0																																			
4096	4096																																			
8192	8192																																			
12288	12288																																			
16384	16384																																			
20480	20480																																			
24576	24576																																			
28672	28672																																			
32768	32768																																			
36864	36864																																			
40960	40960																																			
45056	45056																																			
49152	49152																																			
53248	53248																																			
57344	57344																																			
hello-time	Hello time .	integer	Minimum value: 1 Maximum value: 10	2																																
forward-delay	Forward delay .	integer	Minimum value: 4 Maximum value: 30	15																																

Parameter	Description	Type	Size	Default
max-age	Maximum packet age .	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops .	integer	Minimum value: 1 Maximum value: 40	20

## config system password-policy

Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.

```

config system password-policy
  Description: Configure password policy for locally defined administrator passwords and
              IPsec VPN pre-shared keys.
  set status [enable|disable]
  set apply-to {option1}, {option2}, ...
  set minimum-length {integer}
  set min-lower-case-letter {integer}
  set min-upper-case-letter {integer}
  set min-non-alphanumeric {integer}
  set min-number {integer}
  set change-4-characters [enable|disable]
  set expire-status [enable|disable]
  set expire-day {integer}
  set reuse-password [enable|disable]
end

```

## config system password-policy

Parameter	Description	Type	Size	Default						
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable password policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable password policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.			
Option	Description									
<i>enable</i>	Enable password policy.									
<i>disable</i>	Disable password policy.									
apply-to	Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.	option	-	admin-password						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>admin-password</i></td> <td>Apply to administrator passwords.</td> </tr> <tr> <td><i>ipsec-preshared-key</i></td> <td>Apply to IPsec pre-shared keys.</td> </tr> </tbody> </table>	Option	Description	<i>admin-password</i>	Apply to administrator passwords.	<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.			
Option	Description									
<i>admin-password</i>	Apply to administrator passwords.									
<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.									
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
change-4-characters	Enable/disable changing at least 4 characters for a new password (This attribute overrides reuse-password if both are enabled).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable requiring that at least 4 characters must be changed in a new password.</td> </tr> <tr> <td><i>disable</i></td> <td>No requirements for the number of characters to change in a new password. A new password can be the same as the old password.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.	<i>disable</i>	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.			
Option	Description									
<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.									
<i>disable</i>	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.									
expire-status	Enable/disable password expiration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Passwords expire after expire-day days.</td> </tr> <tr> <td><i>disable</i></td> <td>Passwords do not expire.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.			
Option	Description									
<i>enable</i>	Passwords expire after expire-day days.									
<i>disable</i>	Passwords do not expire.									

Parameter	Description	Type	Size	Default
expire-day	Number of days after which passwords expire .	integer	Minimum value: 1 Maximum value: 999	90
reuse-password	Enable/disable reusing of password (if both reuse-password and change-4-characters are enabled, change-4-characters overrides).	option	-	enable

Option	Description
<i>enable</i>	Administrators are allowed to reuse the same password.
<i>disable</i>	Administrators must create a new password.

## config system password-policy-guest-admin

Configure the password policy for guest administrators.

```

config system password-policy-guest-admin
  Description: Configure the password policy for guest administrators.
  set status [enable|disable]
  set apply-to {option1}, {option2}, ...
  set minimum-length {integer}
  set min-lower-case-letter {integer}
  set min-upper-case-letter {integer}
  set min-non-alphanumeric {integer}
  set min-number {integer}
  set change-4-characters [enable|disable]
  set expire-status [enable|disable]
  set expire-day {integer}
  set reuse-password [enable|disable]
end

```

## config system password-policy-guest-admin

Parameter	Description	Type	Size	Default
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable

Option	Description
<i>enable</i>	Enable password policy.
<i>disable</i>	Disable password policy.

Parameter	Description	Type	Size	Default						
apply-to	Guest administrator to which this password policy applies.	option	-	guest-admin-password						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>guest-admin-password</i></td> <td>Apply to guest administrator password.</td> </tr> </tbody> </table>				Option	Description	<i>guest-admin-password</i>	Apply to guest administrator password.		
Option	Description									
<i>guest-admin-password</i>	Apply to guest administrator password.									
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
change-4-characters	Enable/disable changing at least 4 characters for a new password (This attribute overrides reuse-password if both are enabled).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable requiring that at least 4 characters must be changed in a new password.</td> </tr> <tr> <td><i>disable</i></td> <td>No requirements for the number of characters to change in a new password. A new password can be the same as the old password.</td> </tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.	<i>disable</i>	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.
Option	Description									
<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.									
<i>disable</i>	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.									
expire-status	Enable/disable password expiration.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Passwords expire after expire-day days.</td> </tr> <tr> <td><i>disable</i></td> <td>Passwords do not expire.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.			
Option	Description									
<i>enable</i>	Passwords expire after expire-day days.									
<i>disable</i>	Passwords do not expire.									
expire-day	Number of days after which passwords expire .	integer	Minimum value: 1 Maximum value: 999	90						
reuse-password	Enable/disable reusing of password (if both reuse-password and change-4-characters are enabled, change-4-characters overrides).	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Administrators are allowed to reuse the same password.</td> </tr> <tr> <td><i>disable</i></td> <td>Administrators must create a new password.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.			
Option	Description									
<i>enable</i>	Administrators are allowed to reuse the same password.									
<i>disable</i>	Administrators must create a new password.									

## config system sms-server

Configure SMS server for sending SMS messages to support user authentication.

```
config system sms-server
  Description: Configure SMS server for sending SMS messages to support user
  authentication.
  edit <name>
    set mail-server {string}
  next
end
```

## config system sms-server

Parameter	Description	Type	Size	Default
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	

## config system custom-language

Configure custom languages.

```
config system custom-language
  Description: Configure custom languages.
  edit <name>
    set filename {string}
    set comments {var-string}
  next
```



end

## config system custom-language

Parameter	Description	Type	Size	Default
filename	Custom language file path.	string	Maximum length: 63	
comments	Comment.	var-string	Maximum length: 255	

## config system admin

Configure admin users.

```
config system admin
  Description: Configure admin users.
  edit <name>
    set wildcard [enable|disable]
    set remote-auth [enable|disable]
    set remote-group {string}
    set password {password-2}
    set peer-auth [enable|disable]
    set peer-group {string}
    set trusthost1 {ipv4-classnet}
    set trusthost2 {ipv4-classnet}
    set trusthost3 {ipv4-classnet}
    set trusthost4 {ipv4-classnet}
    set trusthost5 {ipv4-classnet}
    set trusthost6 {ipv4-classnet}
    set trusthost7 {ipv4-classnet}
    set trusthost8 {ipv4-classnet}
    set trusthost9 {ipv4-classnet}
    set trusthost10 {ipv4-classnet}
    set ip6-trusthost1 {ipv6-prefix}
    set ip6-trusthost2 {ipv6-prefix}
    set ip6-trusthost3 {ipv6-prefix}
    set ip6-trusthost4 {ipv6-prefix}
    set ip6-trusthost5 {ipv6-prefix}
    set ip6-trusthost6 {ipv6-prefix}
    set ip6-trusthost7 {ipv6-prefix}
    set ip6-trusthost8 {ipv6-prefix}
    set ip6-trusthost9 {ipv6-prefix}
    set ip6-trusthost10 {ipv6-prefix}
    set accprofile {string}
    set allow-remove-admin-session [enable|disable]
    set comments {var-string}
    set vdom <name1>, <name2>, ...
    set ssh-public-key1 {user}
    set ssh-public-key2 {user}
    set ssh-public-key3 {user}
    set ssh-certificate {string}
    set schedule {string}
```

```

set accprofile-override [enable|disable]
set radius-vdom-override [enable|disable]
set password-expire {user}
set force-password-change [enable|disable]
set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set fortitoken {string}
set email-to {string}
set sms-server [fortiguard|custom]
set sms-custom-server {string}
set sms-phone {string}
set guest-auth [disable|enable]
set guest-usergroups <name1>, <name2>, ...
set guest-lang {string}
next
end

```

## config system admin

Parameter	Description	Type	Size	Default						
wildcard	Enable/disable wildcard RADIUS authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable username wildcard.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable username wildcard.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable username wildcard.	<i>disable</i>	Disable username wildcard.			
Option	Description									
<i>enable</i>	Enable username wildcard.									
<i>disable</i>	Disable username wildcard.									
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable remote authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable remote authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable remote authentication.	<i>disable</i>	Disable remote authentication.			
Option	Description									
<i>enable</i>	Enable remote authentication.									
<i>disable</i>	Disable remote authentication.									
remote-group	User group name used for remote auth.	string	Maximum length: 35							
password	Admin user password.	password-2	Not Specified							
peer-auth	Set to enable peer certificate authentication (for HTTPS admin access).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable peer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable peer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable peer.	<i>disable</i>	Disable peer.			
Option	Description									
<i>enable</i>	Enable peer.									
<i>disable</i>	Disable peer.									

Parameter	Description	Type	Size	Default
peer-group	Name of peer group defined under config user group which has PKI members. Used for peer certificate authentication (for HTTPS admin access).	string	Maximum length: 35	
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost2	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost3	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost4	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost5	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost6	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost7	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost8	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost9	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
trusthost10	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost2	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost3	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost4	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost5	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost6	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost8	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost9	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost10	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiGate features.	string	Maximum length: 35	
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable allow-remove option.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable allow-remove option.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable allow-remove option.	<i>disable</i>	Disable allow-remove option.			
Option	Description									
<i>enable</i>	Enable allow-remove option.									
<i>disable</i>	Disable allow-remove option.									
comments	Comment.	var-string	Maximum length: 255							
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79							
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							
ssh-certificate	Select the certificate to be used by the FortiGate for authentication with an SSH client.	string	Maximum length: 35							
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35							
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiGate features that this administrator can access.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable access profile override.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable access profile override.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable access profile override.	<i>disable</i>	Disable access profile override.			
Option	Description									
<i>enable</i>	Enable access profile override.									
<i>disable</i>	Disable access profile override.									
radius-vdom-override	Enable to use the names of VDOMs provided by the remote authentication server to control the VDOMs that this administrator can access.	option	-	disable						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VDOM override.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VDOM override.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VDOM override.	<i>disable</i>	Disable VDOM override.									
Option	Description															
<i>enable</i>	Enable VDOM override.															
<i>disable</i>	Disable VDOM override.															
password-expire	Password expire time.	user	Not Specified													
force-password-change	Enable/disable force password change on next login.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable force password change on next login.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable force password change on next login.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable force password change on next login.	<i>disable</i>	Disable force password change on next login.									
Option	Description															
<i>enable</i>	Enable force password change on next login.															
<i>disable</i>	Disable force password change on next login.															
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable two-factor authentication.</td> </tr> <tr> <td><i>fortitoken</i></td> <td>Use FortiToken or FortiToken mobile two-factor authentication.</td> </tr> <tr> <td><i>fortitoken-cloud</i></td> <td>FortiToken Cloud Service.</td> </tr> <tr> <td><i>email</i></td> <td>Send a two-factor authentication code to the configured email-to email address.</td> </tr> <tr> <td><i>sms</i></td> <td>Send a two-factor authentication code to the configured sms-server and sms-phone.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable two-factor authentication.	<i>fortitoken</i>	Use FortiToken or FortiToken mobile two-factor authentication.	<i>fortitoken-cloud</i>	FortiToken Cloud Service.	<i>email</i>	Send a two-factor authentication code to the configured email-to email address.	<i>sms</i>	Send a two-factor authentication code to the configured sms-server and sms-phone.			
Option	Description															
<i>disable</i>	Disable two-factor authentication.															
<i>fortitoken</i>	Use FortiToken or FortiToken mobile two-factor authentication.															
<i>fortitoken-cloud</i>	FortiToken Cloud Service.															
<i>email</i>	Send a two-factor authentication code to the configured email-to email address.															
<i>sms</i>	Send a two-factor authentication code to the configured sms-server and sms-phone.															
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortitoken</i></td> <td>FortiToken authentication.</td> </tr> <tr> <td><i>email</i></td> <td>Email one time password.</td> </tr> <tr> <td><i>sms</i></td> <td>SMS one time password.</td> </tr> </tbody> </table>	Option	Description	<i>fortitoken</i>	FortiToken authentication.	<i>email</i>	Email one time password.	<i>sms</i>	SMS one time password.							
Option	Description															
<i>fortitoken</i>	FortiToken authentication.															
<i>email</i>	Email one time password.															
<i>sms</i>	SMS one time password.															
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>email</i></td> <td>Email notification for activation code.</td> </tr> <tr> <td><i>sms</i></td> <td>SMS notification for activation code.</td> </tr> </tbody> </table>	Option	Description	<i>email</i>	Email notification for activation code.	<i>sms</i>	SMS notification for activation code.									
Option	Description															
<i>email</i>	Email notification for activation code.															
<i>sms</i>	SMS notification for activation code.															

Parameter	Description	Type	Size	Default						
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16							
email-to	This administrator's email address.	string	Maximum length: 63							
sms-server	Send SMS messages using the FortiGuard SMS server or a custom server.	option	-	fortiguard						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard</i></td> <td>Send SMS by FortiGuard.</td> </tr> <tr> <td><i>custom</i></td> <td>Send SMS by custom server.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.			
Option	Description									
<i>fortiguard</i>	Send SMS by FortiGuard.									
<i>custom</i>	Send SMS by custom server.									
sms-custom-server	Custom SMS server to send SMS messages to.	string	Maximum length: 35							
sms-phone	Phone number on which the administrator receives SMS messages.	string	Maximum length: 15							
guest-auth	Enable/disable guest authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable guest authentication.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable guest authentication.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable guest authentication.	<i>enable</i>	Enable guest authentication.			
Option	Description									
<i>disable</i>	Disable guest authentication.									
<i>enable</i>	Enable guest authentication.									
guest-usergroups <name>	Select guest user groups. Select guest user groups.	string	Maximum length: 79							
guest-lang	Guest management portal language.	string	Maximum length: 35							

## config system api-user

Configure API users.

```
config system api-user
  Description: Configure API users.
  edit <name>
    set comments {var-string}
    set api-key {password-2}
    set accprofile {string}
    set vdom <name1>, <name2>, ...
    set schedule {string}
    set cors-allow-origin {string}
    set peer-auth [enable|disable]
    set peer-group {string}
  config trusthost
    Description: Trusthost.
    edit <id>
```

```

        set type [ipv4-trusthost|ipv6-trusthost]
        set ipv4-trusthost {ipv4-classnet}
        set ipv6-trusthost {ipv6-prefix}
    next
end
next
end

```

## config system api-user

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 255							
api-key	Admin user password.	password-2	Not Specified							
accprofile	Admin user access profile.	string	Maximum length: 35							
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79							
schedule	Schedule name.	string	Maximum length: 35							
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using "*" if possible.	string	Maximum length: 269							
peer-auth	Enable/disable peer authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable peer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable peer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable peer.	<i>disable</i>	Disable peer.			
Option	Description									
<i>enable</i>	Enable peer.									
<i>disable</i>	Disable peer.									
peer-group	Peer group name.	string	Maximum length: 35							

## config trusthost

Parameter	Description	Type	Size	Default						
type	Trusthost type.	option	-	ipv4-trusthost						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4-trusthost</i></td> <td>IPv4 trusthost.</td> </tr> <tr> <td><i>ipv6-trusthost</i></td> <td>IPv6 trusthost.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4-trusthost</i>	IPv4 trusthost.	<i>ipv6-trusthost</i>	IPv6 trusthost.			
Option	Description									
<i>ipv4-trusthost</i>	IPv4 trusthost.									
<i>ipv6-trusthost</i>	IPv6 trusthost.									



Parameter	Description	Type	Size	Default
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified	::/0

## config system sso-admin

Configure SSO admin users.

```
config system sso-admin
  Description: Configure SSO admin users.
  edit <name>
    set accprofile {string}
    set vdom <name1>, <name2>, ...
  next
end
```

## config system sso-admin

Parameter	Description	Type	Size	Default
accprofile	SSO admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

## config system settings

Configure VDOM settings.

```
config system settings
  Description: Configure VDOM settings.
  set comments {var-string}
  set opmode [nat|transparent]
  set ngfw-mode [profile-based|policy-based]
  set http-external-dest [fortiweb|forticache]
  set firewall-session-dirty [check-all|check-new|...]
  set manageip {user}
  set gateway {ipv4-address}
  set ip {ipv4-classnet-host}
  set manageip6 {ipv6-prefix}
  set gateway6 {ipv6-address}
  set ip6 {ipv6-prefix}
  set device {string}
  set bfd [enable|disable]
  set bfd-desired-min-tx {integer}
  set bfd-required-min-rx {integer}
  set bfd-detect-mult {integer}
```

---

```
set bfd-dont-enforce-src-port [enable|disable]
set utf8-spam-tagging [enable|disable]
set wccp-cache-engine [enable|disable]
set vpn-stats-log {option1}, {option2}, ...
set vpn-stats-period {integer}
set v4-ecmp-mode [source-ip-based|weight-based|...]
set mac-ttl {integer}
set fw-session-hairpin [enable|disable]
set prp-trailer-action [enable|disable]
set snat-hairpin-traffic [enable|disable]
set dhcp-proxy [enable|disable]
set dhcp-proxy-interface-select-method [auto|sdwan|...]
set dhcp-proxy-interface {string}
set dhcp-server-ip {user}
set dhcp6-server-ip {user}
set central-nat [enable|disable]
set gui-default-policy-columns <name1>, <name2>, ...
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set link-down-access [enable|disable]
set auxiliary-session [enable|disable]
set asymroute [enable|disable]
set asymroute-icmp [enable|disable]
set tcp-session-without-syn [enable|disable]
set ses-denied-traffic [enable|disable]
set strict-src-check [enable|disable]
set allow-linkdown-path [enable|disable]
set asymroute6 [enable|disable]
set asymroute6-icmp [enable|disable]
set sctp-session-without-init [enable|disable]
set sip-expectation [enable|disable]
set sip-nat-trace [enable|disable]
set status [enable|disable]
set sip-tcp-port {integer}
set sip-udp-port {integer}
set sip-ssl-port {integer}
set sccp-port {integer}
set multicast-forward [enable|disable]
set multicast-ttl-notchange [enable|disable]
set multicast-skip-policy [enable|disable]
set allow-subnet-overlap [enable|disable]
set deny-tcp-with-icmp [enable|disable]
set ecmp-max-paths {integer}
set discovered-device-timeout {integer}
set email-portal-check-dns [disable|enable]
set default-voip-alg-mode [proxy-based|kernel-helper-based]
set gui-icap [enable|disable]
set gui-nat46-64 [enable|disable]
set gui-implicit-policy [enable|disable]
set gui-dns-database [enable|disable]
set gui-load-balance [enable|disable]
set gui-multicast-policy [enable|disable]
set gui-dos-policy [enable|disable]
set gui-object-colors [enable|disable]
set gui-replacement-message-groups [enable|disable]
set gui-voip-profile [enable|disable]
set gui-ap-profile [enable|disable]
```

```

set gui-security-profile-group [enable|disable]
set gui-local-in-policy [enable|disable]
set gui-explicit-proxy [enable|disable]
set gui-dynamic-routing [enable|disable]
set gui-sslvpn-personal-bookmarks [enable|disable]
set gui-sslvpn-realms [enable|disable]
set gui-policy-based-ipsec [enable|disable]
set gui-threat-weight [enable|disable]
set gui-spamfilter [enable|disable]
set gui-file-filter [enable|disable]
set gui-application-control [enable|disable]
set gui-ips [enable|disable]
set gui-endpoint-control [enable|disable]
set gui-endpoint-control-advanced [enable|disable]
set gui-dhcp-advanced [enable|disable]
set gui-vpn [enable|disable]
set gui-wireless-controller [enable|disable]
set gui-switch-controller [enable|disable]
set gui-fortiap-split-tunneling [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-wan-load-balancing [enable|disable]
set gui-antivirus [enable|disable]
set gui-webfilter [enable|disable]
set gui-dnsfilter [enable|disable]
set gui-waf-profile [enable|disable]
set gui-fortiextender-controller [enable|disable]
set gui-advanced-policy [enable|disable]
set gui-allow-unnamed-policy [enable|disable]
set gui-email-collection [enable|disable]
set gui-multiple-interface-policy [enable|disable]
set gui-policy-disclaimer [enable|disable]
set ike-session-resume [enable|disable]
set ike-quick-crash-detect [enable|disable]
set ike-dn-format [with-space|no-space]
set ike-policy-route [enable|disable]
set block-land-attack [disable|enable]
end

```

## config system settings

Parameter	Description	Type	Size	Default
comments	VDOM comments.	var-string	Maximum length: 255	
opmode	Firewall operation mode (NAT or Transparent).	option	-	nat
	<b>Option</b>	<b>Description</b>		
	<i>nat</i>	Change to NAT mode.		
	<i>transparent</i>	Change to transparent mode.		

Parameter	Description	Type	Size	Default								
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-	profile-based								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>profile-based</i></td> <td>Application and web-filtering are configured using profiles applied to policy entries.</td> </tr> <tr> <td><i>policy-based</i></td> <td>Application and web-filtering are configured as policy match conditions.</td> </tr> </tbody> </table>	Option	Description	<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.	<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.					
Option	Description											
<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.											
<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.											
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-	fortiweb								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiweb</i></td> <td>Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.</td> </tr> <tr> <td><i>forticache</i></td> <td>Offload HTTP traffic to FortiCache for external web caching and WAN optimization.</td> </tr> </tbody> </table>	Option	Description	<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.	<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.					
Option	Description											
<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.											
<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.											
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-	check-all								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>check-all</i></td> <td>All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.</td> </tr> <tr> <td><i>check-new</i></td> <td>Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.</td> </tr> <tr> <td><i>check-policy-option</i></td> <td>Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.</td> </tr> </tbody> </table>	Option	Description	<i>check-all</i>	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.	<i>check-new</i>	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.	<i>check-policy-option</i>	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.			
Option	Description											
<i>check-all</i>	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.											
<i>check-new</i>	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.											
<i>check-policy-option</i>	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.											
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified									
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0								
ip	IP address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified	::/0								
gateway6	Transparent mode IPv4 default gateway IP address.	ipv6-address	Not Specified	::								
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified	::/0								

Parameter	Description	Type	Size	Default						
device	Interface to use for management access for NAT mode.	string	Maximum length: 35							
bfd	Enable/disable Bi-directional Forwarding Detection (BFD) on all interfaces.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Bi-directional Forwarding Detection (BFD) on all interfaces.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Bi-directional Forwarding Detection (BFD) on all interfaces.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.	<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.			
Option	Description									
<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.									
<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.									
bfd-desired-min-tx	BFD desired minimal transmit interval .	integer	Minimum value: 1 Maximum value: 100000	250						
bfd-required-min-rx	BFD required minimal receive interval .	integer	Minimum value: 1 Maximum value: 100000	250						
bfd-detect-mult	BFD detection multiplier .	integer	Minimum value: 1 Maximum value: 50	3						
bfd-dont-enforce-src-port	Enable to not enforce verifying the source port of BFD Packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verifying the source port of BFD Packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verifying the source port of BFD Packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verifying the source port of BFD Packets.	<i>disable</i>	Disable verifying the source port of BFD Packets.			
Option	Description									
<i>enable</i>	Enable verifying the source port of BFD Packets.									
<i>disable</i>	Disable verifying the source port of BFD Packets.									
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Convert antispam tags to UTF-8.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not convert antispam tags.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Convert antispam tags to UTF-8.	<i>disable</i>	Do not convert antispam tags.			
Option	Description									
<i>enable</i>	Convert antispam tags to UTF-8.									
<i>disable</i>	Do not convert antispam tags.									
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-	disable						

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WCCP cache engine.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WCCP cache engine.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WCCP cache engine.	<i>disable</i>	Disable WCCP cache engine.							
Option	Description													
<i>enable</i>	Enable WCCP cache engine.													
<i>disable</i>	Disable WCCP cache engine.													
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-	ipsec pptp l2tp ssl										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipsec</i></td> <td>IPsec.</td> </tr> <tr> <td><i>pptp</i></td> <td>PPTP.</td> </tr> <tr> <td><i>l2tp</i></td> <td>L2TP.</td> </tr> <tr> <td><i>ssl</i></td> <td>SSL.</td> </tr> </tbody> </table>	Option	Description	<i>ipsec</i>	IPsec.	<i>pptp</i>	PPTP.	<i>l2tp</i>	L2TP.	<i>ssl</i>	SSL.			
Option	Description													
<i>ipsec</i>	IPsec.													
<i>pptp</i>	PPTP.													
<i>l2tp</i>	L2TP.													
<i>ssl</i>	SSL.													
vpn-stats-period	Period to send VPN log statistics .	integer	Minimum value: 0 Maximum value: 4294967295	600										
v4-ecmp-mode	IPv4 Equal-cost multi-path (ECMP) routing and load balancing mode.	option	-	source-ip-based										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>source-ip-based</i></td> <td>Select next hop based on source IP.</td> </tr> <tr> <td><i>weight-based</i></td> <td>Select next hop based on weight.</td> </tr> <tr> <td><i>usage-based</i></td> <td>Select next hop based on usage.</td> </tr> <tr> <td><i>source-dest-ip-based</i></td> <td>Select next hop based on both source and destination IPs.</td> </tr> </tbody> </table>	Option	Description	<i>source-ip-based</i>	Select next hop based on source IP.	<i>weight-based</i>	Select next hop based on weight.	<i>usage-based</i>	Select next hop based on usage.	<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.			
Option	Description													
<i>source-ip-based</i>	Select next hop based on source IP.													
<i>weight-based</i>	Select next hop based on weight.													
<i>usage-based</i>	Select next hop based on usage.													
<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.													
mac-ttl	Duration of MAC addresses in Transparent mode .	integer	Minimum value: 300 Maximum value: 8640000	300										
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiGate.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Perform a policy check every time.</td> </tr> <tr> <td><i>disable</i></td> <td>Perform a policy check only the first time the session is received.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Perform a policy check every time.	<i>disable</i>	Perform a policy check only the first time the session is received.							
Option	Description													
<i>enable</i>	Perform a policy check every time.													
<i>disable</i>	Perform a policy check only the first time the session is received.													

Parameter	Description	Type	Size	Default								
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Try to keep PRP trailer.</td> </tr> <tr> <td><i>disable</i></td> <td>Trim PRP trailer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Try to keep PRP trailer.	<i>disable</i>	Trim PRP trailer.					
Option	Description											
<i>enable</i>	Try to keep PRP trailer.											
<i>disable</i>	Trim PRP trailer.											
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SNAT for hairpin traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SNAT for hairpin traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SNAT for hairpin traffic.	<i>disable</i>	Disable SNAT for hairpin traffic.					
Option	Description											
<i>enable</i>	Enable SNAT for hairpin traffic.											
<i>disable</i>	Disable SNAT for hairpin traffic.											
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the DHCP proxy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the DHCP proxy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the DHCP proxy.	<i>disable</i>	Disable the DHCP proxy.					
Option	Description											
<i>enable</i>	Enable the DHCP proxy.											
<i>disable</i>	Disable the DHCP proxy.											
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified									
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified									
central-nat	Enable/disable central NAT.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable central NAT.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable central NAT.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable central NAT.	<i>disable</i>	Disable central NAT.					
Option	Description											
<i>enable</i>	Enable central NAT.											
<i>disable</i>	Disable central NAT.											

Parameter	Description	Type	Size	Default								
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79									
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception for this VDOM or apply global settings to this VDOM.	option	-	global								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable LLDP reception for this VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable LLDP reception for this VDOM.</td> </tr> <tr> <td><i>global</i></td> <td>Use the global LLDP reception configuration for this VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable LLDP reception for this VDOM.	<i>disable</i>	Disable LLDP reception for this VDOM.	<i>global</i>	Use the global LLDP reception configuration for this VDOM.			
Option	Description											
<i>enable</i>	Enable LLDP reception for this VDOM.											
<i>disable</i>	Disable LLDP reception for this VDOM.											
<i>global</i>	Use the global LLDP reception configuration for this VDOM.											
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission for this VDOM or apply global settings to this VDOM.	option	-	global								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable LLDP transmission for this VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable LLDP transmission for this VDOM.</td> </tr> <tr> <td><i>global</i></td> <td>Use the global LLDP transmission configuration for this VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable LLDP transmission for this VDOM.	<i>disable</i>	Disable LLDP transmission for this VDOM.	<i>global</i>	Use the global LLDP transmission configuration for this VDOM.			
Option	Description											
<i>enable</i>	Enable LLDP transmission for this VDOM.											
<i>disable</i>	Disable LLDP transmission for this VDOM.											
<i>global</i>	Use the global LLDP transmission configuration for this VDOM.											
link-down-access	Enable/disable link down access traffic.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow link down access traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Block link down access traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow link down access traffic.	<i>disable</i>	Block link down access traffic.					
Option	Description											
<i>enable</i>	Allow link down access traffic.											
<i>disable</i>	Block link down access traffic.											
auxiliary-session	Enable/disable auxiliary session.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auxiliary session for this VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable auxiliary session for this VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auxiliary session for this VDOM.	<i>disable</i>	Disable auxiliary session for this VDOM.					
Option	Description											
<i>enable</i>	Enable auxiliary session for this VDOM.											
<i>disable</i>	Disable auxiliary session for this VDOM.											
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPv4 asymmetric routing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPv4 asymmetric routing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPv4 asymmetric routing.	<i>disable</i>	Disable IPv4 asymmetric routing.					
Option	Description											
<i>enable</i>	Enable IPv4 asymmetric routing.											
<i>disable</i>	Disable IPv4 asymmetric routing.											



Parameter	Description	Type	Size	Default						
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ICMP asymmetric routing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ICMP asymmetric routing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ICMP asymmetric routing.	<i>disable</i>	Disable ICMP asymmetric routing.			
Option	Description									
<i>enable</i>	Enable ICMP asymmetric routing.									
<i>disable</i>	Disable ICMP asymmetric routing.									
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow TCP session without SYN flags.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow TCP session without SYN flags.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow TCP session without SYN flags.	<i>disable</i>	Do not allow TCP session without SYN flags.			
Option	Description									
<i>enable</i>	Allow TCP session without SYN flags.									
<i>disable</i>	Do not allow TCP session without SYN flags.									
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Include denied sessions in the session table.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not add denied sessions to the session table.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Include denied sessions in the session table.	<i>disable</i>	Do not add denied sessions to the session table.			
Option	Description									
<i>enable</i>	Include denied sessions in the session table.									
<i>disable</i>	Do not add denied sessions to the session table.									
strict-src-check	Enable/disable strict source verification.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strict source verification.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strict source verification.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strict source verification.	<i>disable</i>	Disable strict source verification.			
Option	Description									
<i>enable</i>	Enable strict source verification.									
<i>disable</i>	Disable strict source verification.									
allow-linkdown-path	Enable/disable link down path.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow link down path.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow link down path.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow link down path.	<i>disable</i>	Do not allow link down path.			
Option	Description									
<i>enable</i>	Allow link down path.									
<i>disable</i>	Do not allow link down path.									
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable asymmetric IPv6 routing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable asymmetric IPv6 routing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable asymmetric IPv6 routing.	<i>disable</i>	Disable asymmetric IPv6 routing.			
Option	Description									
<i>enable</i>	Enable asymmetric IPv6 routing.									
<i>disable</i>	Disable asymmetric IPv6 routing.									

Parameter	Description	Type	Size	Default						
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable asymmetric ICMPv6 routing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable asymmetric ICMPv6 routing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable asymmetric ICMPv6 routing.	<i>disable</i>	Disable asymmetric ICMPv6 routing.			
Option	Description									
<i>enable</i>	Enable asymmetric ICMPv6 routing.									
<i>disable</i>	Disable asymmetric ICMPv6 routing.									
sctp-session-without-init	Enable/disable Sctp session creation without Sctp INIT.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Sctp session creation without Sctp INIT.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Sctp session creation without Sctp INIT.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Sctp session creation without Sctp INIT.	<i>disable</i>	Disable Sctp session creation without Sctp INIT.			
Option	Description									
<i>enable</i>	Enable Sctp session creation without Sctp INIT.									
<i>disable</i>	Disable Sctp session creation without Sctp INIT.									
sip-expectation	Enable/disable the SIP kernel session helper to create an expectation for port 5060.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow SIP session helper to create an expectation for port 5060.</td> </tr> <tr> <td><i>disable</i></td> <td>Prevent SIP session helper from creating an expectation for port 5060.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow SIP session helper to create an expectation for port 5060.	<i>disable</i>	Prevent SIP session helper from creating an expectation for port 5060.			
Option	Description									
<i>enable</i>	Allow SIP session helper to create an expectation for port 5060.									
<i>disable</i>	Prevent SIP session helper from creating an expectation for port 5060.									
sip-nat-trace	Enable/disable recording the original SIP source IP address when NAT is used.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Record the original SIP source IP address when NAT is used.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not record the original SIP source IP address when NAT is used.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Record the original SIP source IP address when NAT is used.	<i>disable</i>	Do not record the original SIP source IP address when NAT is used.			
Option	Description									
<i>enable</i>	Record the original SIP source IP address when NAT is used.									
<i>disable</i>	Do not record the original SIP source IP address when NAT is used.									
status	Enable/disable this VDOM.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this VDOM.	<i>disable</i>	Disable this VDOM.			
Option	Description									
<i>enable</i>	Enable this VDOM.									
<i>disable</i>	Disable this VDOM.									
sip-tcp-port	TCP port the SIP proxy monitors for SIP traffic .	integer	Minimum value: 1 Maximum value: 65535	5060						
sip-udp-port	UDP port the SIP proxy monitors for SIP traffic .	integer	Minimum value: 1 Maximum value: 65535	5060						

Parameter	Description	Type	Size	Default						
sip-ssl-port	TCP port the SIP proxy monitors for SIP SSL/TLS traffic .	integer	Minimum value: 0 Maximum value: 65535	5061						
sccp-port	TCP port the SCCP proxy monitors for SCCP traffic .	integer	Minimum value: 0 Maximum value: 65535	2000						
multicast-forward	Enable/disable multicast forwarding.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast forwarding.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast forwarding.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast forwarding.	<i>disable</i>	Disable multicast forwarding.			
Option	Description									
<i>enable</i>	Enable multicast forwarding.									
<i>disable</i>	Disable multicast forwarding.									
multicast-ttl-notchange	Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>The multicast TTL is not changed.</td> </tr> <tr> <td><i>disable</i></td> <td>The multicast TTL may be changed.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	The multicast TTL is not changed.	<i>disable</i>	The multicast TTL may be changed.			
Option	Description									
<i>enable</i>	The multicast TTL is not changed.									
<i>disable</i>	The multicast TTL may be changed.									
multicast-skip-policy	Enable/disable allowing multicast traffic through the FortiGate without a policy check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Require a multicast policy to allow multicast traffic to pass through the FortiGate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.	<i>disable</i>	Require a multicast policy to allow multicast traffic to pass through the FortiGate.			
Option	Description									
<i>enable</i>	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.									
<i>disable</i>	Require a multicast policy to allow multicast traffic to pass through the FortiGate.									
allow-subnet-overlap	Enable/disable allowing interface subnets to use overlapping IP addresses.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable overlapping subnets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable overlapping subnets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable overlapping subnets.	<i>disable</i>	Disable overlapping subnets.			
Option	Description									
<i>enable</i>	Enable overlapping subnets.									
<i>disable</i>	Disable overlapping subnets.									
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Deny TCP with ICMP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable denying TCP with ICMP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Deny TCP with ICMP.	<i>disable</i>	Disable denying TCP with ICMP.			
Option	Description									
<i>enable</i>	Deny TCP with ICMP.									
<i>disable</i>	Disable denying TCP with ICMP.									
ecmp-max-paths	Maximum number of Equal Cost Multi-Path .	integer	Minimum value: 1 Maximum value: 255	255						
discovered-device-timeout	Timeout for discovered devices .	integer	Minimum value: 1 Maximum value: 365	28						
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable email address checking with DNS.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable email address checking with DNS.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable email address checking with DNS.	<i>enable</i>	Enable email address checking with DNS.			
Option	Description									
<i>disable</i>	Disable email address checking with DNS.									
<i>enable</i>	Enable email address checking with DNS.									
default-voip-alg-mode	Configure how the FortiGate handles VoIP traffic when a policy that accepts the traffic doesn't include a VoIP profile.	option	-	proxy-based						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>proxy-based</i></td> <td>Use a default proxy-based VoIP ALG.</td> </tr> <tr> <td><i>kernel-helper-based</i></td> <td>Use the SIP session helper.</td> </tr> </tbody> </table>	Option	Description	<i>proxy-based</i>	Use a default proxy-based VoIP ALG.	<i>kernel-helper-based</i>	Use the SIP session helper.			
Option	Description									
<i>proxy-based</i>	Use a default proxy-based VoIP ALG.									
<i>kernel-helper-based</i>	Use the SIP session helper.									
gui-icap	Enable/disable ICAP on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable ICAP on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ICAP on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ICAP on the GUI.	<i>disable</i>	Disable ICAP on the GUI.			
Option	Description									
<i>enable</i>	Enable ICAP on the GUI.									
<i>disable</i>	Disable ICAP on the GUI.									
gui-nat46-64	Enable/disable NAT46 and NAT64 settings on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NAT46 and NAT64 settings on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NAT46 and NAT64 settings on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NAT46 and NAT64 settings on the GUI.	<i>disable</i>	Disable NAT46 and NAT64 settings on the GUI.			
Option	Description									
<i>enable</i>	Enable NAT46 and NAT64 settings on the GUI.									
<i>disable</i>	Disable NAT46 and NAT64 settings on the GUI.									

Parameter	Description	Type	Size	Default						
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable implicit firewall policies on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable implicit firewall policies on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable implicit firewall policies on the GUI.	<i>disable</i>	Disable implicit firewall policies on the GUI.			
Option	Description									
<i>enable</i>	Enable implicit firewall policies on the GUI.									
<i>disable</i>	Disable implicit firewall policies on the GUI.									
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DNS database settings on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DNS database settings on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DNS database settings on the GUI.	<i>disable</i>	Disable DNS database settings on the GUI.			
Option	Description									
<i>enable</i>	Enable DNS database settings on the GUI.									
<i>disable</i>	Disable DNS database settings on the GUI.									
gui-load-balance	Enable/disable server load balancing on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable server load balancing on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable server load balancing on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable server load balancing on the GUI.	<i>disable</i>	Disable server load balancing on the GUI.			
Option	Description									
<i>enable</i>	Enable server load balancing on the GUI.									
<i>disable</i>	Disable server load balancing on the GUI.									
gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast firewall policies on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast firewall policies on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast firewall policies on the GUI.	<i>disable</i>	Disable multicast firewall policies on the GUI.			
Option	Description									
<i>enable</i>	Enable multicast firewall policies on the GUI.									
<i>disable</i>	Disable multicast firewall policies on the GUI.									
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-	disable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DoS policies on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DoS policies on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DoS policies on the GUI.	<i>disable</i>	Disable DoS policies on the GUI.			
Option	Description									
<i>enable</i>	Enable DoS policies on the GUI.									
<i>disable</i>	Disable DoS policies on the GUI.									
gui-object-colors	Enable/disable object colors on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable object colors on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable object colors on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable object colors on the GUI.	<i>disable</i>	Disable object colors on the GUI.			
Option	Description									
<i>enable</i>	Enable object colors on the GUI.									
<i>disable</i>	Disable object colors on the GUI.									

Parameter	Description	Type	Size	Default						
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable replacement message groups on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable replacement message groups on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable replacement message groups on the GUI.	<i>disable</i>	Disable replacement message groups on the GUI.			
Option	Description									
<i>enable</i>	Enable replacement message groups on the GUI.									
<i>disable</i>	Disable replacement message groups on the GUI.									
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VoIP profiles on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VoIP profiles on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VoIP profiles on the GUI.	<i>disable</i>	Disable VoIP profiles on the GUI.			
Option	Description									
<i>enable</i>	Enable VoIP profiles on the GUI.									
<i>disable</i>	Disable VoIP profiles on the GUI.									
gui-ap-profile	Enable/disable FortiAP profiles on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAP profiles on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAP profiles on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAP profiles on the GUI.	<i>disable</i>	Disable FortiAP profiles on the GUI.			
Option	Description									
<i>enable</i>	Enable FortiAP profiles on the GUI.									
<i>disable</i>	Disable FortiAP profiles on the GUI.									
gui-security-profile-group	Enable/disable Security Profile Groups on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Security Profile Groups on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Security Profile Groups on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Security Profile Groups on the GUI.	<i>disable</i>	Disable Security Profile Groups on the GUI.			
Option	Description									
<i>enable</i>	Enable Security Profile Groups on the GUI.									
<i>disable</i>	Disable Security Profile Groups on the GUI.									
gui-local-in-policy	Enable/disable Local-In policies on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Local-In policies on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Local-In policies on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Local-In policies on the GUI.	<i>disable</i>	Disable Local-In policies on the GUI.			
Option	Description									
<i>enable</i>	Enable Local-In policies on the GUI.									
<i>disable</i>	Disable Local-In policies on the GUI.									
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the explicit proxy on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the explicit proxy on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the explicit proxy on the GUI.	<i>disable</i>	Disable the explicit proxy on the GUI.			
Option	Description									
<i>enable</i>	Enable the explicit proxy on the GUI.									
<i>disable</i>	Disable the explicit proxy on the GUI.									

Parameter	Description	Type	Size	Default						
gui-dynamic-routing	Enable/disable dynamic routing on the GUI.	option	-	disable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dynamic routing on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dynamic routing on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dynamic routing on the GUI.	<i>disable</i>	Disable dynamic routing on the GUI.			
Option	Description									
<i>enable</i>	Enable dynamic routing on the GUI.									
<i>disable</i>	Disable dynamic routing on the GUI.									
gui-sslvpn-personal-bookmarks	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSL-VPN personal bookmark management on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL-VPN personal bookmark management on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSL-VPN personal bookmark management on the GUI.	<i>disable</i>	Disable SSL-VPN personal bookmark management on the GUI.			
Option	Description									
<i>enable</i>	Enable SSL-VPN personal bookmark management on the GUI.									
<i>disable</i>	Disable SSL-VPN personal bookmark management on the GUI.									
gui-sslvpn-realms	Enable/disable SSL-VPN realms on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSL-VPN realms on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL-VPN realms on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSL-VPN realms on the GUI.	<i>disable</i>	Disable SSL-VPN realms on the GUI.			
Option	Description									
<i>enable</i>	Enable SSL-VPN realms on the GUI.									
<i>disable</i>	Disable SSL-VPN realms on the GUI.									
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable policy-based IPsec VPN on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable policy-based IPsec VPN on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable policy-based IPsec VPN on the GUI.	<i>disable</i>	Disable policy-based IPsec VPN on the GUI.			
Option	Description									
<i>enable</i>	Enable policy-based IPsec VPN on the GUI.									
<i>disable</i>	Disable policy-based IPsec VPN on the GUI.									
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable threat weight on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable threat weight on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable threat weight on the GUI.	<i>disable</i>	Disable threat weight on the GUI.			
Option	Description									
<i>enable</i>	Enable threat weight on the GUI.									
<i>disable</i>	Disable threat weight on the GUI.									
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Antispam on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Antispam on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Antispam on the GUI.	<i>disable</i>	Disable Antispam on the GUI.			
Option	Description									
<i>enable</i>	Enable Antispam on the GUI.									
<i>disable</i>	Disable Antispam on the GUI.									

Parameter	Description	Type	Size	Default						
gui-file-filter	Enable/disable File-filter on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable File-filter on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable File-filter on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable File-filter on the GUI.	<i>disable</i>	Disable File-filter on the GUI.			
Option	Description									
<i>enable</i>	Enable File-filter on the GUI.									
<i>disable</i>	Disable File-filter on the GUI.									
gui-application-control	Enable/disable application control on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable application control on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable application control on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable application control on the GUI.	<i>disable</i>	Disable application control on the GUI.			
Option	Description									
<i>enable</i>	Enable application control on the GUI.									
<i>disable</i>	Disable application control on the GUI.									
gui-ips	Enable/disable IPS on the GUI.	option	-	disable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPS on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPS on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPS on the GUI.	<i>disable</i>	Disable IPS on the GUI.			
Option	Description									
<i>enable</i>	Enable IPS on the GUI.									
<i>disable</i>	Disable IPS on the GUI.									
gui-endpoint-control	Enable/disable endpoint control on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable endpoint control on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable endpoint control on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable endpoint control on the GUI.	<i>disable</i>	Disable endpoint control on the GUI.			
Option	Description									
<i>enable</i>	Enable endpoint control on the GUI.									
<i>disable</i>	Disable endpoint control on the GUI.									
gui-endpoint-control-advanced	Enable/disable advanced endpoint control options on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable advanced endpoint control options on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable advanced endpoint control options on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable advanced endpoint control options on the GUI.	<i>disable</i>	Disable advanced endpoint control options on the GUI.			
Option	Description									
<i>enable</i>	Enable advanced endpoint control options on the GUI.									
<i>disable</i>	Disable advanced endpoint control options on the GUI.									
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable advanced DHCP options on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable advanced DHCP options on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable advanced DHCP options on the GUI.	<i>disable</i>	Disable advanced DHCP options on the GUI.			
Option	Description									
<i>enable</i>	Enable advanced DHCP options on the GUI.									
<i>disable</i>	Disable advanced DHCP options on the GUI.									



Parameter	Description	Type	Size	Default						
gui-vpn	Enable/disable VPN tunnels on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable VPN tunnels on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VPN tunnels on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VPN tunnels on the GUI.	<i>disable</i>	Disable VPN tunnels on the GUI.			
Option	Description									
<i>enable</i>	Enable VPN tunnels on the GUI.									
<i>disable</i>	Disable VPN tunnels on the GUI.									
gui-wireless-controller	Enable/disable the wireless controller on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the wireless controller on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the wireless controller on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the wireless controller on the GUI.	<i>disable</i>	Disable the wireless controller on the GUI.			
Option	Description									
<i>enable</i>	Enable the wireless controller on the GUI.									
<i>disable</i>	Disable the wireless controller on the GUI.									
gui-switch-controller	Enable/disable the switch controller on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the switch controller on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the switch controller on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the switch controller on the GUI.	<i>disable</i>	Disable the switch controller on the GUI.			
Option	Description									
<i>enable</i>	Enable the switch controller on the GUI.									
<i>disable</i>	Disable the switch controller on the GUI.									
gui-fortiap-split-tunneling	Enable/disable FortiAP split tunneling on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiAP split tunneling on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiAP split tunneling on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiAP split tunneling on the GUI.	<i>disable</i>	Disable FortiAP split tunneling on the GUI.			
Option	Description									
<i>enable</i>	Enable FortiAP split tunneling on the GUI.									
<i>disable</i>	Disable FortiAP split tunneling on the GUI.									
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable advanced web filtering on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable advanced web filtering on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable advanced web filtering on the GUI.	<i>disable</i>	Disable advanced web filtering on the GUI.			
Option	Description									
<i>enable</i>	Enable advanced web filtering on the GUI.									
<i>disable</i>	Disable advanced web filtering on the GUI.									
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable traffic shaping on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable traffic shaping on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable traffic shaping on the GUI.	<i>disable</i>	Disable traffic shaping on the GUI.			
Option	Description									
<i>enable</i>	Enable traffic shaping on the GUI.									
<i>disable</i>	Disable traffic shaping on the GUI.									

Parameter	Description	Type	Size	Default						
gui-wan-load-balancing	Enable/disable SD-WAN on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SD-WAN on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SD-WAN on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SD-WAN on the GUI.	<i>disable</i>	Disable SD-WAN on the GUI.			
Option	Description									
<i>enable</i>	Enable SD-WAN on the GUI.									
<i>disable</i>	Disable SD-WAN on the GUI.									
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AntiVirus on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AntiVirus on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AntiVirus on the GUI.	<i>disable</i>	Disable AntiVirus on the GUI.			
Option	Description									
<i>enable</i>	Enable AntiVirus on the GUI.									
<i>disable</i>	Disable AntiVirus on the GUI.									
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Web filtering on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Web filtering on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Web filtering on the GUI.	<i>disable</i>	Disable Web filtering on the GUI.			
Option	Description									
<i>enable</i>	Enable Web filtering on the GUI.									
<i>disable</i>	Disable Web filtering on the GUI.									
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DNS Filtering on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DNS Filtering on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DNS Filtering on the GUI.	<i>disable</i>	Disable DNS Filtering on the GUI.			
Option	Description									
<i>enable</i>	Enable DNS Filtering on the GUI.									
<i>disable</i>	Disable DNS Filtering on the GUI.									
gui-waf-profile	Enable/disable Web Application Firewall on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Web Application Firewall on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Web Application Firewall on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Web Application Firewall on the GUI.	<i>disable</i>	Disable Web Application Firewall on the GUI.			
Option	Description									
<i>enable</i>	Enable Web Application Firewall on the GUI.									
<i>disable</i>	Disable Web Application Firewall on the GUI.									
gui-fortixtender-controller	Enable/disable FortiExtender on the GUI.	option	-	enable **						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiExtender on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiExtender on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiExtender on the GUI.	<i>disable</i>	Disable FortiExtender on the GUI.			
Option	Description									
<i>enable</i>	Enable FortiExtender on the GUI.									
<i>disable</i>	Disable FortiExtender on the GUI.									

Parameter	Description	Type	Size	Default						
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable advanced policy configuration on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable advanced policy configuration on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable advanced policy configuration on the GUI.	<i>disable</i>	Disable advanced policy configuration on the GUI.			
Option	Description									
<i>enable</i>	Enable advanced policy configuration on the GUI.									
<i>disable</i>	Disable advanced policy configuration on the GUI.									
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the requirement for policy naming on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the requirement for policy naming on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the requirement for policy naming on the GUI.	<i>disable</i>	Disable the requirement for policy naming on the GUI.			
Option	Description									
<i>enable</i>	Enable the requirement for policy naming on the GUI.									
<i>disable</i>	Disable the requirement for policy naming on the GUI.									
gui-email-collection	Enable/disable email collection on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable email collection on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable email collection on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable email collection on the GUI.	<i>disable</i>	Disable email collection on the GUI.			
Option	Description									
<i>enable</i>	Enable email collection on the GUI.									
<i>disable</i>	Disable email collection on the GUI.									
gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding multiple interfaces to a policy on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding multiple interfaces to a policy on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.	<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.			
Option	Description									
<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.									
<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.									
gui-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable policy disclaimer on the GUI.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable policy disclaimer on the GUI.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable policy disclaimer on the GUI.	<i>disable</i>	Disable policy disclaimer on the GUI.			
Option	Description									
<i>enable</i>	Enable policy disclaimer on the GUI.									
<i>disable</i>	Disable policy disclaimer on the GUI.									
ike-session-resume	Enable/disable IKEv2 session resumption (RFC 5723).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 session resumption (RFC 5723).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).					
Option	Description									
<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IKEv2 session resumption (RFC 5723).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).					
Option	Description									
<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).									
ike-quick-crash-detect	Enable/disable IKE quick crash detection (RFC 6290).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKE quick crash detection (RFC 6290).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKE quick crash detection (RFC 6290).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKE quick crash detection (RFC 6290).	<i>disable</i>	Disable IKE quick crash detection (RFC 6290).			
Option	Description									
<i>enable</i>	Enable IKE quick crash detection (RFC 6290).									
<i>disable</i>	Disable IKE quick crash detection (RFC 6290).									
ike-dn-format	Configure IKE ASN.1 Distinguished Name format conventions.	option	-	with-space						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>with-space</i></td> <td>Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.</td> </tr> <tr> <td><i>no-space</i></td> <td>Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.</td> </tr> </tbody> </table>	Option	Description	<i>with-space</i>	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.	<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.			
Option	Description									
<i>with-space</i>	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.									
<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.									
ike-policy-route	Enable/disable IKE Policy Based Routing (PBR).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKE Policy Based Routing (PBR).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKE Policy Based Routing (PBR).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKE Policy Based Routing (PBR).	<i>disable</i>	Disable IKE Policy Based Routing (PBR).			
Option	Description									
<i>enable</i>	Enable IKE Policy Based Routing (PBR).									
<i>disable</i>	Disable IKE Policy Based Routing (PBR).									
block-land-attack	Enable/disable blocking of land attacks.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not block land attack.</td> </tr> <tr> <td><i>enable</i></td> <td>Block land attack.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not block land attack.	<i>enable</i>	Block land attack.			
Option	Description									
<i>disable</i>	Do not block land attack.									
<i>enable</i>	Block land attack.									

\*\* Values may differ between models.

## config system sit-tunnel

Configure IPv6 tunnel over IPv4.

```
config system sit-tunnel
  Description: Configure IPv6 tunnel over IPv4.
  edit <name>
    set source {ipv4-address}
    set destination {ipv4-address}
    set ip6 {ipv6-prefix}
```

```

    set interface {string}
    set auto-asic-offload [enable|disable]
  next
end

```

## config system sit-tunnel

Parameter	Description	Type	Size	Default
source	Source IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0
destination	Destination IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0
ip6	IPv6 address of the tunnel.	ipv6-prefix	Not Specified	::/0
interface	Interface name.	string	Maximum length: 15	
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable

Option	Description
<i>enable</i>	Enable auto ASIC offloading.
<i>disable</i>	Disable ASIC offloading.

\* This parameter may not exist in some models.

## config system npu



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64.

Configure NPU attributes.

```

config system npu
  Description: Configure NPU attributes.
  set iph-rsvd-re-cksum [enable|disable]
  set per-session-accounting [disable|traffic-log-only|...]
  config fp-anomaly
    Description: NP6Lite anomaly protection (packet drop or send trap to host).
    set ipv4-ver-err [drop|trap-to-host]
    set ipv4-ihl-err [drop|trap-to-host]
    set ipv4-len-err [drop|trap-to-host]
    set ipv4-ttlzero-err [drop|trap-to-host]
    set ipv4-csum-err [drop|trap-to-host]
    set ipv4-opt-err [drop|trap-to-host]
    set tcp-hlen-err [drop|trap-to-host]
  end
end

```

```

set tcp-plen-err [drop|trap-to-host]
set tcp-csum-err [drop|trap-to-host]
set udp-plen-err [drop|trap-to-host]
set udp-hlen-err [drop|trap-to-host]
set udp-csum-err [drop|trap-to-host]
set udp-len-err [drop|trap-to-host]
set udplite-cover-err [drop|trap-to-host]
set udplite-csum-err [drop|trap-to-host]
set icmp-minlen-err [drop|trap-to-host]
set icmp-csum-err [drop|trap-to-host]
set esp-minlen-err [drop|trap-to-host]
set unknproto-minlen-err [drop|trap-to-host]
set ipv6-ver-err [drop|trap-to-host]
set ipv6-ihl-err [drop|trap-to-host]
set ipv6-plen-zero [drop|trap-to-host]
set ipv6-exthdr-order-err [drop|trap-to-host]
set ipv6-exthdr-len-err [drop|trap-to-host]
end
end

```

## config system npu

Parameter	Description	Type	Size	Default
iph-rsvd-recksum *	Enable/disable IP checksum re-calculation for packets with iph.reserved bit set.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IP checksum re-calculation for packets with iph.reserved bit set.		
	<i>disable</i>	Disable IP checksum re-calculation for packets with iph.reserved bit set.		
per-session-accounting *	Enable/disable per-session accounting.	option	-	traffic-log-only
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable per-session accounting.		
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.		
	<i>enable</i>	Per-session accounting for all sessions.		

\* This parameter may not exist in some models.

## config fp-anomaly

Parameter	Description	Type	Size	Default
ipv4-ver-err	Invalid IPv4 header version anomalies.	option	-	drop

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid header version.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid header version to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid header version.	<i>trap-to-host</i>	Forward IPv4 invalid header version to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid header version.									
<i>trap-to-host</i>	Forward IPv4 invalid header version to main CPU for processing.									
ipv4-ihl-err	Invalid IPv4 header length anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid header length.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid header length to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid header length.	<i>trap-to-host</i>	Forward IPv4 invalid header length to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid header length.									
<i>trap-to-host</i>	Forward IPv4 invalid header length to main CPU for processing.									
ipv4-len-err	Invalid IPv4 packet length anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid packet length.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid packet length to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid packet length.	<i>trap-to-host</i>	Forward IPv4 invalid packet length to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid packet length.									
<i>trap-to-host</i>	Forward IPv4 invalid packet length to main CPU for processing.									
ipv4-ttlzero-err	Invalid IPv4 TTL field zero anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid TTL field zero.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid TTL field zero to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid TTL field zero.	<i>trap-to-host</i>	Forward IPv4 invalid TTL field zero to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid TTL field zero.									
<i>trap-to-host</i>	Forward IPv4 invalid TTL field zero to main CPU for processing.									
ipv4-csum-err	Invalid IPv4 packet checksum anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid L3 checksum.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid L3 checksum to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid L3 checksum.	<i>trap-to-host</i>	Forward IPv4 invalid L3 checksum to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid L3 checksum.									
<i>trap-to-host</i>	Forward IPv4 invalid L3 checksum to main CPU for processing.									
ipv4-opt-err	Invalid IPv4 option parsing anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid option parsing.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid option parsing to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid option parsing.	<i>trap-to-host</i>	Forward IPv4 invalid option parsing to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid option parsing.									
<i>trap-to-host</i>	Forward IPv4 invalid option parsing to main CPU for processing.									
tcp-hlen-err	Invalid IPv4 TCP header length anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid TCP packet header length.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid TCP packet header length to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid TCP packet header length.	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet header length to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid TCP packet header length.									
<i>trap-to-host</i>	Forward IPv4 invalid TCP packet header length to main CPU for processing.									

Parameter	Description	Type	Size	Default
tcp-plen-err	Invalid IPv4 TCP packet length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet length to main CPU for processing.		
tcp-csum-err	Invalid IPv4 TCP packet checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet checksum to main CPU for processing.		
udp-plen-err	Invalid IPv4 UDP packet minimum length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP packet minimum length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet minimum length to main CPU for processing.		
udp-hlen-err	Invalid IPv4 UDP packet header length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP header length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP header length to main CPU for processing.		
udp-csum-err	Invalid IPv4 UDP packet checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet checksum to main CPU for processing.		
udp-len-err	Invalid IPv4 UDP packet length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet length to main CPU for processing.		
udplite-cover-err	Invalid IPv4 UDP-Lite packet coverage anomalies.	option	-	drop



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid UDP-Lite packet coverage.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid UDP-Lite packet coverage.	<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid UDP-Lite packet coverage.									
<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.									
udplite-csum-err	Invalid IPv4 UDP-Lite packet checksum anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid UDP-Lite packet checksum.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid UDP-Lite packet checksum.	<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid UDP-Lite packet checksum.									
<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.									
icmp-minlen-err	Invalid IPv4 ICMP short packet anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid ICMP short packet.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid ICMP short packet to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid ICMP short packet.	<i>trap-to-host</i>	Forward IPv4 invalid ICMP short packet to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid ICMP short packet.									
<i>trap-to-host</i>	Forward IPv4 invalid ICMP short packet to main CPU for processing.									
icmp-csum-err	Invalid IPv4 ICMP packet checksum anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid ICMP checksum.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid ICMP checksum to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid ICMP checksum.	<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid ICMP checksum.									
<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.									
esp-minlen-err	Invalid IPv4 ESP short packet anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid ESP short packet.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid ESP short packet to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid ESP short packet.	<i>trap-to-host</i>	Forward IPv4 invalid ESP short packet to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid ESP short packet.									
<i>trap-to-host</i>	Forward IPv4 invalid ESP short packet to main CPU for processing.									
unknproto-minlen-err	Invalid IPv4 L4 unknown protocol short packet anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv4 invalid L4 unknown protocol short packet.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv4 invalid L4 unknown protocol short packet.	<i>trap-to-host</i>	Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid L4 unknown protocol short packet.									
<i>trap-to-host</i>	Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.									
ipv6-ver-err	Invalid IPv6 packet version anomalies.	option	-	drop						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv6 with invalid packet version.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv6 with invalid packet version to FortiOS.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv6 with invalid packet version.	<i>trap-to-host</i>	Forward IPv6 with invalid packet version to FortiOS.			
Option	Description									
<i>drop</i>	Drop IPv6 with invalid packet version.									
<i>trap-to-host</i>	Forward IPv6 with invalid packet version to FortiOS.									
ipv6-ihl-err	Invalid IPv6 packet length anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv6 with invalid packet length.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv6 with invalid packet length to FortiOS.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv6 with invalid packet length.	<i>trap-to-host</i>	Forward IPv6 with invalid packet length to FortiOS.			
Option	Description									
<i>drop</i>	Drop IPv6 with invalid packet length.									
<i>trap-to-host</i>	Forward IPv6 with invalid packet length to FortiOS.									
ipv6-plen-zero	Invalid IPv6 packet payload length zero anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv6 with invalid packet payload length zero.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv6 with invalid packet payload length zero to FortiOS.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv6 with invalid packet payload length zero.	<i>trap-to-host</i>	Forward IPv6 with invalid packet payload length zero to FortiOS.			
Option	Description									
<i>drop</i>	Drop IPv6 with invalid packet payload length zero.									
<i>trap-to-host</i>	Forward IPv6 with invalid packet payload length zero to FortiOS.									
ipv6-exthdr-order-err	Invalid IPv6 packet extension header ordering anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv6 with invalid packet extension header ordering.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv6 with invalid packet extension header ordering to FortiOS.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv6 with invalid packet extension header ordering.	<i>trap-to-host</i>	Forward IPv6 with invalid packet extension header ordering to FortiOS.			
Option	Description									
<i>drop</i>	Drop IPv6 with invalid packet extension header ordering.									
<i>trap-to-host</i>	Forward IPv6 with invalid packet extension header ordering to FortiOS.									
ipv6-exthdr-len-err	Invalid IPv6 packet chain extension header total length anomalies.	option	-	drop						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop</i></td> <td>Drop IPv6 with invalid packet chain extension header total length.</td> </tr> <tr> <td><i>trap-to-host</i></td> <td>Forward IPv6 with invalid packet chain extension header total length to FortiOS.</td> </tr> </tbody> </table>	Option	Description	<i>drop</i>	Drop IPv6 with invalid packet chain extension header total length.	<i>trap-to-host</i>	Forward IPv6 with invalid packet chain extension header total length to FortiOS.			
Option	Description									
<i>drop</i>	Drop IPv6 with invalid packet chain extension header total length.									
<i>trap-to-host</i>	Forward IPv6 with invalid packet chain extension header total length to FortiOS.									

## config system fssso-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fssso-polling
  Description: Configure Fortinet Single Sign On (FSSO) server.
  set status [enable|disable]
  set listening-port {integer}
  set authentication [enable|disable]
  set auth-password {password}
end
```

## config system fssso-polling

Parameter	Description	Type	Size	Default						
status	Enable/disable FSSO Polling Mode.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable FSSO Polling Mode.</td></tr><tr><td><i>disable</i></td><td>Disable FSSO Polling Mode.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable FSSO Polling Mode.	<i>disable</i>	Disable FSSO Polling Mode.			
Option	Description									
<i>enable</i>	Enable FSSO Polling Mode.									
<i>disable</i>	Disable FSSO Polling Mode.									
listening-port	Listening port to accept clients .	integer	Minimum value: 1 Maximum value: 65535	8000						
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable FSSO Agent Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable FSSO Agent Authentication.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable FSSO Agent Authentication.	<i>disable</i>	Disable FSSO Agent Authentication.			
Option	Description									
<i>enable</i>	Enable FSSO Agent Authentication.									
<i>disable</i>	Disable FSSO Agent Authentication.									
auth-password	Password to connect to FSSO Agent.	password	Not Specified							

## config system ha

Configure HA.

```
config system ha
  Description: Configure HA.
  set group-id {integer}
  set group-name {string}
  set mode [standalone|a-a|...]
  set sync-packet-balance [enable|disable]
  set password {password}
  set key {password}
  set hbdev {user}
  set session-sync-dev {user}
  set route-ttl {integer}
  set route-wait {integer}
  set route-hold {integer}
  set multicast-ttl {integer}
  set load-balance-all [enable|disable]
  set sync-config [enable|disable]
  set encryption [enable|disable]
  set authentication [enable|disable]
  set hb-interval {integer}
  set hb-lost-threshold {integer}
  set hello-holddown {integer}
  set gratuitous-arps [enable|disable]
```

```

set arps {integer}
set arps-interval {integer}
set session-pickup [enable|disable]
set session-pickup-connectionless [enable|disable]
set session-pickup-expectation [enable|disable]
set session-pickup-nat [enable|disable]
set session-pickup-delay [enable|disable]
set link-failed-signal [enable|disable]
set uninterruptible-upgrade [enable|disable]
set uninterruptible-primary-wait {integer}
set standalone-mgmt-vdom [enable|disable]
set ha-mgmt-status [enable|disable]
config ha-mgmt-interfaces
  Description: Reserve interfaces to manage individual cluster units.
  edit <id>
    set interface {string}
    set dst {ipv4-classnet}
    set gateway {ipv4-address}
    set gateway6 {ipv6-address}
  next
end
set ha-eth-type {string}
set hc-eth-type {string}
set l2ep-eth-type {string}
set ha-uptime-diff-margin {integer}
set standalone-config-sync [enable|disable]
set logical-sn [enable|disable]
set vcluster-id {integer}
set override [enable|disable]
set priority {integer}
set override-wait-time {integer}
set schedule [none|hub|...]
set weight {user}
set cpu-threshold {user}
set memory-threshold {user}
set http-proxy-threshold {user}
set ftp-proxy-threshold {user}
set imap-proxy-threshold {user}
set nntp-proxy-threshold {user}
set pop3-proxy-threshold {user}
set smtp-proxy-threshold {user}
set monitor {user}
set pingserver-monitor-interface {user}
set pingserver-failover-threshold {integer}
set pingserver-secondary-force-reset [enable|disable]
set pingserver-flip-timeout {integer}
set vdom {user}
set vcluster2 [enable|disable]
config secondary-vcluster
  Description: Configure virtual cluster 2.
  set vcluster-id {integer}
  set override [enable|disable]
  set priority {integer}
  set override-wait-time {integer}
  set monitor {user}
  set pingserver-monitor-interface {user}
  set pingserver-failover-threshold {integer}

```

```

    set pingserver-secondary-force-reset [enable|disable]
    set vdom {user}
end
set ha-direct [enable|disable]
set memory-compatible-mode [enable|disable]
end

```

## config system ha

Parameter	Description	Type	Size	Default								
group-id	HA group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255	0								
group-name	Cluster group name. Must be the same for all members.	string	Maximum length: 32									
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standalone</i></td> <td>Standalone mode.</td> </tr> <tr> <td><i>a-a</i></td> <td>Active-active mode.</td> </tr> <tr> <td><i>a-p</i></td> <td>Active-passive mode.</td> </tr> </tbody> </table>	Option	Description	<i>standalone</i>	Standalone mode.	<i>a-a</i>	Active-active mode.	<i>a-p</i>	Active-passive mode.			
Option	Description											
<i>standalone</i>	Standalone mode.											
<i>a-a</i>	Active-active mode.											
<i>a-p</i>	Active-passive mode.											
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HA packet distribution to multiple CPUs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HA packet distribution to multiple CPUs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HA packet distribution to multiple CPUs.	<i>disable</i>	Disable HA packet distribution to multiple CPUs.					
Option	Description											
<i>enable</i>	Enable HA packet distribution to multiple CPUs.											
<i>disable</i>	Disable HA packet distribution to multiple CPUs.											
password	Cluster password. Must be the same for all members.	password	Not Specified									
key	key	password	Not Specified									
hbdev	Heartbeat interfaces. Must be the same for all members. Enter <interface> <priority> pairs to specify the priority of each heartbeat interface. Higher priority takes precedence.	user	Not Specified									
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified									

Parameter	Description	Type	Size	Default
route-ttl	TTL for primary unit routes . Increase to maintain active routes during failover.	integer	Minimum value: 5 Maximum value: 3600	10
route-wait	Time to wait before sending new routes to the cluster .	integer	Minimum value: 0 Maximum value: 3600	0
route-hold	Time to wait between routing table updates to the cluster .	integer	Minimum value: 0 Maximum value: 3600	10
multicast-ttl	HA multicast TTL on primary .	integer	Minimum value: 5 Maximum value: 3600	600
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable load balance.		
	<i>disable</i>	Disable load balance.		
sync-config	Enable/disable configuration synchronization.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable configuration synchronization.		
	<i>disable</i>	Disable configuration synchronization.		
encryption	Enable/disable heartbeat message encryption.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable heartbeat message encryption.		
	<i>disable</i>	Disable heartbeat message encryption.		
authentication	Enable/disable heartbeat message authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable heartbeat message authentication.		
	<i>disable</i>	Disable heartbeat message authentication.		

Parameter	Description	Type	Size	Default						
hb-interval	Time between sending heartbeat packets . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2						
hb-lost-threshold	Number of lost heartbeats to signal a failure . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	6 **						
hello-holddown	Time to wait before changing from hello to work state .	integer	Minimum value: 5 Maximum value: 300	20						
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable gratuitous ARPs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable gratuitous ARPs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable gratuitous ARPs.	<i>disable</i>	Disable gratuitous ARPs.			
Option	Description									
<i>enable</i>	Enable gratuitous ARPs.									
<i>disable</i>	Disable gratuitous ARPs.									
arps	Number of gratuitous ARPs . Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60	5						
arps-interval	Time between gratuitous ARPs . Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20	8						
session-pickup	Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable session pickup.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable session pickup.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable session pickup.	<i>disable</i>	Disable session pickup.			
Option	Description									
<i>enable</i>	Enable session pickup.									
<i>disable</i>	Disable session pickup.									
session-pickup-connectionless	Enable/disable UDP and ICMP session sync.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
session-pickup-expectation	Enable/disable session helper expectation session sync for FGSP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
session-pickup-nat	Enable/disable NAT session sync for FGSP.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
session-pickup-delay	Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
link-failed-signal	Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uninterruptible-primary-wait	Number of minutes the primary HA unit waits before the secondary HA unit is considered upgraded and the system is started before starting its own upgrade .	integer	Minimum value: 1 Maximum value: 300	30						
standalone-mgmt-vdom	Enable/disable standalone management VDOM.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ha-eth-type	HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8890						
hc-eth-type	Transparent mode HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8891						
l2ep-eth-type	Telnet session HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8893						
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535	300						
standalone-config-sync	Enable/disable FGSP configuration synchronization.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
logical-sn	Enable/disable usage of the logical serial number.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable usage of the logical serial number.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable usage of the logical serial number.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable usage of the logical serial number.	<i>disable</i>	Disable usage of the logical serial number.			
Option	Description									
<i>enable</i>	Enable usage of the logical serial number.									
<i>disable</i>	Disable usage of the logical serial number.									
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default																		
override	Enable and increase the priority of the unit that should always be primary.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
Option	Description																					
<i>enable</i>	Enable setting.																					
<i>disable</i>	Disable setting.																					
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255	128																		
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0																		
schedule	Type of A-A load balancing. Use none if you have external load balancers.	option	-	round-robin																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>hub</i></td> <td>Hub.</td> </tr> <tr> <td><i>leastconnection</i></td> <td>Least connection.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Round robin.</td> </tr> <tr> <td><i>weight-round-robin</i></td> <td>Weight round robin.</td> </tr> <tr> <td><i>random</i></td> <td>Random.</td> </tr> <tr> <td><i>ip</i></td> <td>IP.</td> </tr> <tr> <td><i>ipport</i></td> <td>IP port.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>hub</i>	Hub.	<i>leastconnection</i>	Least connection.	<i>round-robin</i>	Round robin.	<i>weight-round-robin</i>	Weight round robin.	<i>random</i>	Random.	<i>ip</i>	IP.	<i>ipport</i>	IP port.			
Option	Description																					
<i>none</i>	None.																					
<i>hub</i>	Hub.																					
<i>leastconnection</i>	Least connection.																					
<i>round-robin</i>	Round robin.																					
<i>weight-round-robin</i>	Weight round robin.																					
<i>random</i>	Random.																					
<i>ip</i>	IP.																					
<i>ipport</i>	IP port.																					
weight	Weight-round-robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified	0 40																		
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified																			
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified																			
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified																			
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified																			

Parameter	Description	Type	Size	Default						
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified							
nntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified							
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified							
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified							
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified							
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified							
pingserver-failover-threshold	Remote IP monitoring failover threshold .	integer	Minimum value: 0 Maximum value: 50	0						
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable force reset of secondary after PING server failure.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable force reset of secondary after PING server failure.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable force reset of secondary after PING server failure.	<i>disable</i>	Disable force reset of secondary after PING server failure.			
Option	Description									
<i>enable</i>	Enable force reset of secondary after PING server failure.									
<i>disable</i>	Disable force reset of secondary after PING server failure.									
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60						
vdom	VDOMs in virtual cluster 1.	user	Not Specified							
vcluster2	Enable/disable virtual cluster 2 for virtual clustering.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
ha-direct	Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager, FortiSandbox, sFlow, and Netflow.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager, FortiSandbox, sFlow, and Netflow.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager, FortiSandbox, sFlow, and Netflow.	<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager, FortiSandbox, sFlow, and Netflow.			
Option	Description									
<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager, FortiSandbox, sFlow, and Netflow.									
<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager, FortiSandbox, sFlow, and Netflow.									
memory-compatible-mode	Enable/disable memory compatible mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

### config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
interface	Interface to reserve for HA management.	string	Maximum length: 15	
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Default route gateway for reserved HA management interface.	ipv4-address	Not Specified	0.0.0.0
gateway6	Default IPv6 gateway for reserved HA management interface.	ipv6-address	Not Specified	::

### config secondary-vcluster

Parameter	Description	Type	Size	Default
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	1
override	Enable and increase the priority of the unit that should always be primary.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255	128						
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0						
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified							
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified							
pingserver-failover-threshold	Remote IP monitoring failover threshold .	integer	Minimum value: 0 Maximum value: 50	0						
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable force reset of secondary after PING server failure.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable force reset of secondary after PING server failure.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable force reset of secondary after PING server failure.	<i>disable</i>	Disable force reset of secondary after PING server failure.			
Option	Description									
<i>enable</i>	Enable force reset of secondary after PING server failure.									
<i>disable</i>	Disable force reset of secondary after PING server failure.									
vdom	VDOMs in virtual cluster 2.	user	Not Specified							

## config system ha-monitor

Configure HA monitor.

```

config system ha-monitor
  Description: Configure HA monitor.
  set monitor-vlan [enable|disable]
  set vlan-hb-interval {integer}
  set vlan-hb-lost-threshold {integer}
end

```

## config system ha-monitor

Parameter	Description	Type	Size	Default						
monitor-vlan	Enable/disable monitor VLAN interfaces.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable monitor VLAN interfaces.</td></tr><tr><td><i>disable</i></td><td>Disable monitor VLAN interfaces.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable monitor VLAN interfaces.	<i>disable</i>	Disable monitor VLAN interfaces.			
Option	Description									
<i>enable</i>	Enable monitor VLAN interfaces.									
<i>disable</i>	Disable monitor VLAN interfaces.									
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30	5						
vlan-hb-lost-threshold	VLAN lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 60	3						

## config system storage

Configure logical storage.

```
config system storage
  Description: Configure logical storage.
  edit <name>
    set status [enable|disable]
    set media-status [enable|disable|...]
    set order {integer}
    set partition {string}
    set device {string}
    set size {integer}
    set usage {option}
  next
end
```

## config system storage

Parameter	Description	Type	Size	Default						
status	Enable/disable storage.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default								
media-status	The physical status of current media.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Storage is enabled.</td> </tr> <tr> <td><i>disable</i></td> <td>Storage is disabled.</td> </tr> <tr> <td><i>fail</i></td> <td>Storage have some fail sector.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Storage is enabled.	<i>disable</i>	Storage is disabled.	<i>fail</i>	Storage have some fail sector.			
Option	Description											
<i>enable</i>	Storage is enabled.											
<i>disable</i>	Storage is disabled.											
<i>fail</i>	Storage have some fail sector.											
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255	0								
partition	Label of underlying partition.	string	Maximum length: 16	<unknown>								
device	Partition device.	string	Maximum length: 19	?								
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295	0								
usage	Use hard disk for logging and WAN Optimization.	option	-	log								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>log</i></td> <td>Use hard disk for logging.</td> </tr> </tbody> </table>	Option	Description	<i>log</i>	Use hard disk for logging.							
Option	Description											
<i>log</i>	Use hard disk for logging.											

## config system dedicated-mgmt

Configure dedicated management.

```

config system dedicated-mgmt
  Description: Configure dedicated management.
  set status [enable|disable]
  set interface {string}
  set default-gateway {ipv4-address}
  set dhcp-server [enable|disable]
  set dhcp-netmask {ipv4-netmask}
  set dhcp-start-ip {ipv4-address}
  set dhcp-end-ip {ipv4-address}
end

```

## config system dedicated-mgmt

Parameter	Description	Type	Size	Default						
status	Enable/disable dedicated management.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
interface	Dedicated management interface.	string	Maximum length: 15							
default-gateway	Default gateway for dedicated management interface.	ipv4-address	Not Specified	0.0.0.0						
dhcp-server	Enable/disable DHCP server on management interface.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable DHCP server on management port.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP server on management port.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable DHCP server on management port.	<i>disable</i>	Disable DHCP server on management port.			
Option	Description									
<i>enable</i>	Enable DHCP server on management port.									
<i>disable</i>	Disable DHCP server on management port.									
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified	0.0.0.0						
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0						
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0						

## config system arp-table

Configure ARP table.

```
config system arp-table
  Description: Configure ARP table.
  edit <id>
    set interface {string}
    set ip {ipv4-address}
    set mac {mac-address}
  next
end
```



## config system arp-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

## config system ipv6-neighbor-cache

Configure IPv6 neighbor cache table.

```
config system ipv6-neighbor-cache
  Description: Configure IPv6 neighbor cache table.
  edit <id>
    set interface {string}
    set ipv6 {ipv6-address}
    set mac {mac-address}
  next
end
```

## config system ipv6-neighbor-cache

Parameter	Description	Type	Size	Default
interface	Select the associated interface name from available options.	string	Maximum length: 15	
ipv6	IPv6 address (format: xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx).	ipv6-address	Not Specified	::
mac	MAC address (format: xx:xx:xx:xx:xx:xx).	mac-address	Not Specified	00:00:00:00:00:00

## config system dns

Configure DNS.

```
config system dns
  Description: Configure DNS.
  set primary {ipv4-address}
  set secondary {ipv4-address}
  set dns-over-tls [disable|enable|...]
  set ssl-certificate {string}
  set server-hostname <hostname1>, <hostname2>, ...
  set domain <domain1>, <domain2>, ...
  set ip6-primary {ipv6-address}
```

```

set ip6-secondary {ipv6-address}
set timeout {integer}
set retry {integer}
set dns-cache-limit {integer}
set dns-cache-ttl {integer}
set cache-notfound-responses [disable|enable]
set source-ip {ipv4-address}
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config system dns

Parameter	Description	Type	Size	Default
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
dns-over-tls	Enable/disable/enforce DNS over TLS.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DNS over TLS.		
	<i>enable</i>	Use TLS for DNS queries if TLS is available.		
	<i>enforce</i>	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.		
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127	
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127	
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified	::
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified	::
timeout	DNS query timeout interval in seconds .	integer	Minimum value: 1 Maximum value: 10	5

Parameter	Description	Type	Size	Default								
retry	Number of times to retry .	integer	Minimum value: 0 Maximum value: 5	2								
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295	5000								
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400	1800								
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-	disable								
		<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable cache NOTFOUND responses from DNS server.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable cache NOTFOUND responses from DNS server.</td> </tr> </tbody> </table>			Option	Description	<i>disable</i>	Disable cache NOTFOUND responses from DNS server.	<i>enable</i>	Enable cache NOTFOUND responses from DNS server.		
Option	Description											
<i>disable</i>	Disable cache NOTFOUND responses from DNS server.											
<i>enable</i>	Enable cache NOTFOUND responses from DNS server.											
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified	0.0.0.0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
		<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>			Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system ddns

Configure DDNS.

```
config system ddns
  Description: Configure DDNS.
  edit <ddnsid>
    set dns-server [dyndns.org|dysns.net|...]
    set server-type [ipv4|ipv6]
    set dns-server-addr <addr1>, <addr2>, ...
```

```

set ddns-zone {string}
set ddns-ttl {integer}
set ddns-auth [disable|tsig]
set ddns-keyname {string}
set ddns-key {user}
set ddns-domain {string}
set ddns-username {string}
set ddns-sn {string}
set ddns-password {password}
set use-public-ip [disable|enable]
set addr-type [ipv4|ipv6]
set update-interval {integer}
set clear-text [disable|enable]
set ssl-certificate {string}
set bound-ip {ipv4-address}
set monitor-interface <interface-name1>, <interface-name2>, ...
next
end

```

## config system ddns

Parameter	Description	Type	Size	Default																								
ddns-server	Select a DDNS service provider.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dyndns.org</i></td> <td>members.dyndns.org and dnsalias.com</td> </tr> <tr> <td><i>dyns.net</i></td> <td>www.dyns.net</td> </tr> <tr> <td><i>tzo.com</i></td> <td>rh.tzo.com</td> </tr> <tr> <td><i>vavic.com</i></td> <td>Peanut Hull</td> </tr> <tr> <td><i>dipdns.net</i></td> <td>dipdnserver.dipdns.com</td> </tr> <tr> <td><i>now.net.cn</i></td> <td>ip.todayisp.com</td> </tr> <tr> <td><i>dhs.org</i></td> <td>members.dhs.org</td> </tr> <tr> <td><i>easydns.com</i></td> <td>members.easydns.com</td> </tr> <tr> <td><i>genericDDNS</i></td> <td>Generic DDNS based on RFC2136.</td> </tr> <tr> <td><i>FortiGuardDDNS</i></td> <td>FortiGuard DDNS service.</td> </tr> <tr> <td><i>noip.com</i></td> <td>dynupdate.no-ip.com</td> </tr> </tbody> </table>	Option	Description	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com	<i>dyns.net</i>	www.dyns.net	<i>tzo.com</i>	rh.tzo.com	<i>vavic.com</i>	Peanut Hull	<i>dipdns.net</i>	dipdnserver.dipdns.com	<i>now.net.cn</i>	ip.todayisp.com	<i>dhs.org</i>	members.dhs.org	<i>easydns.com</i>	members.easydns.com	<i>genericDDNS</i>	Generic DDNS based on RFC2136.	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.	<i>noip.com</i>	dynupdate.no-ip.com			
Option	Description																											
<i>dyndns.org</i>	members.dyndns.org and dnsalias.com																											
<i>dyns.net</i>	www.dyns.net																											
<i>tzo.com</i>	rh.tzo.com																											
<i>vavic.com</i>	Peanut Hull																											
<i>dipdns.net</i>	dipdnserver.dipdns.com																											
<i>now.net.cn</i>	ip.todayisp.com																											
<i>dhs.org</i>	members.dhs.org																											
<i>easydns.com</i>	members.easydns.com																											
<i>genericDDNS</i>	Generic DDNS based on RFC2136.																											
<i>FortiGuardDDNS</i>	FortiGuard DDNS service.																											
<i>noip.com</i>	dynupdate.no-ip.com																											
server-type	Address type of the DDNS server.	option	-	ipv4																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Use IPv4 addressing.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Use IPv6 addressing.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	Use IPv4 addressing.	<i>ipv6</i>	Use IPv6 addressing.																					
Option	Description																											
<i>ipv4</i>	Use IPv4 addressing.																											
<i>ipv6</i>	Use IPv6 addressing.																											

Parameter	Description	Type	Size	Default						
ddns-server-addr <addr>	Generic DDNS server IP/FQDN list. IP address or FQDN of the server.	string	Maximum length: 256							
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64							
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 60 Maximum value: 86400	300						
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DDNS authentication.</td> </tr> <tr> <td><i>tsig</i></td> <td>Enable TSIG authentication based on RFC2845.</td> </tr> </tbody> </table>				Option	Description	<i>disable</i>	Disable DDNS authentication.	<i>tsig</i>	Enable TSIG authentication based on RFC2845.
Option	Description									
<i>disable</i>	Disable DDNS authentication.									
<i>tsig</i>	Enable TSIG authentication based on RFC2845.									
ddns-keyname	DDNS update key name.	string	Maximum length: 64							
ddns-key	DDNS update key (base 64 encoding).	user	Not Specified							
ddns-domain	Your fully qualified domain name (for example, yourname.DDNS.com).	string	Maximum length: 64							
ddns-username	DDNS user name.	string	Maximum length: 64							
ddns-sn	DDNS Serial Number.	string	Maximum length: 64							
ddns-password	DDNS password.	password	Not Specified							
use-public-ip	Enable/disable use of public IP address.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of public IP address.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of public IP address.</td> </tr> </tbody> </table>				Option	Description	<i>disable</i>	Disable use of public IP address.	<i>enable</i>	Enable use of public IP address.
Option	Description									
<i>disable</i>	Disable use of public IP address.									
<i>enable</i>	Enable use of public IP address.									
addr-type	Address type of interface address in DDNS update.	option	-	ipv4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Use IPv4 address of the interface.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Use IPv6 address of the interface.</td> </tr> </tbody> </table>				Option	Description	<i>ipv4</i>	Use IPv4 address of the interface.	<i>ipv6</i>	Use IPv6 address of the interface.
Option	Description									
<i>ipv4</i>	Use IPv4 address of the interface.									
<i>ipv6</i>	Use IPv6 address of the interface.									

Parameter	Description	Type	Size	Default						
update-interval	DDNS update interval .	integer	Minimum value: 60 Maximum value: 2592000	300						
clear-text	Enable/disable use of clear text connections.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of clear text connections.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of clear text connections.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of clear text connections.	<i>enable</i>	Enable use of clear text connections.			
Option	Description									
<i>disable</i>	Disable use of clear text connections.									
<i>enable</i>	Enable use of clear text connections.									
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
bound-ip	Bound IP address.	ipv4-address	Not Specified	0.0.0.0						
monitor-interface <interface-name>	Monitored interface. Interface name.	string	Maximum length: 79							

## config system sflow

Configure sFlow.

```
config system sflow
  Description: Configure sFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config system sflow

Parameter	Description	Type	Size	Default
collector-ip	IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to .	ipv4-address	Not Specified	0.0.0.0
collector-port	UDP port number used for sending sFlow datagrams .	integer	Minimum value: 0 Maximum value: 65535	6343

Parameter	Description	Type	Size	Default								
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system vdom-sflow

Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.

```
config system vdom-sflow
  Description: Configure sFlow per VDOM to add or change the IP address and UDP port that
  FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow
  collector.
  set vdom-sflow [enable|disable]
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

## config system vdom-sflow

Parameter	Description	Type	Size	Default						
vdom-sflow	Enable/disable the sFlow configuration for the current VDOM.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sFlow for this VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sFlow for this VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sFlow for this VDOM.	<i>disable</i>	Disable sFlow for this VDOM.			
Option	Description									
<i>enable</i>	Enable sFlow for this VDOM.									
<i>disable</i>	Disable sFlow for this VDOM.									
collector-ip	IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to .	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default								
collector-port	UDP port number used for sending sFlow datagrams .	integer	Minimum value: 0 Maximum value: 65535	6343								
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system netflow

Configure NetFlow.

```

config system netflow
  Description: Configure NetFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set active-flow-timeout {integer}
  set inactive-flow-timeout {integer}
  set template-tx-timeout {integer}
  set template-tx-counter {integer}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end

```

## config system netflow

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0



Parameter	Description	Type	Size	Default								
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055								
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified	0.0.0.0								
active-flow-timeout	Timeout to report active flows .	integer	Minimum value: 1 Maximum value: 60	30								
inactive-flow-timeout	Timeout for periodic report of finished flows .	integer	Minimum value: 10 Maximum value: 600	15								
template-tx-timeout	Timeout for periodic template flowset transmission .	integer	Minimum value: 1 Maximum value: 1440	30								
template-tx-counter	Counter of flowset records before resending a template flowset record.	integer	Minimum value: 10 Maximum value: 6000	20								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system vdom-netflow

Configure NetFlow per VDOM.

```
config system vdom-netflow
  Description: Configure NetFlow per VDOM.
  set vdom-netflow [enable|disable]
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
```

```

set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config system vdom-netflow

Parameter	Description	Type	Size	Default								
vdom-netflow	Enable/disable NetFlow per VDOM.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NetFlow per VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NetFlow per VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NetFlow per VDOM.	<i>disable</i>	Disable NetFlow per VDOM.					
Option	Description											
<i>enable</i>	Enable NetFlow per VDOM.											
<i>disable</i>	Disable NetFlow per VDOM.											
collector-ip	NetFlow collector IP address.	ipv4-address	Not Specified	0.0.0.0								
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055								
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified	0.0.0.0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system vdom-dns

Configure DNS servers for a non-management VDOM.

```

config system vdom-dns
  Description: Configure DNS servers for a non-management VDOM.
  set vdom-dns [enable|disable]
  set primary {ipv4-address}
  set secondary {ipv4-address}
  set dns-over-tls [disable|enable|...]
  set ssl-certificate {string}
  set server-hostname <hostname1>, <hostname2>, ...
  set ip6-primary {ipv6-address}

```

```

set ip6-secondary {ipv6-address}
set source-ip {ipv4-address}
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config system vdom-dns

Parameter	Description	Type	Size	Default								
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable configuring DNS servers for the current VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable configuring DNS servers for the current VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable configuring DNS servers for the current VDOM.	<i>disable</i>	Disable configuring DNS servers for the current VDOM.					
Option	Description											
<i>enable</i>	Enable configuring DNS servers for the current VDOM.											
<i>disable</i>	Disable configuring DNS servers for the current VDOM.											
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								
dns-over-tls	Enable/disable/enforce DNS over TLS.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DNS over TLS.</td> </tr> <tr> <td><i>enable</i></td> <td>Use TLS for DNS queries if TLS is available.</td> </tr> <tr> <td><i>enforce</i></td> <td>Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DNS over TLS.	<i>enable</i>	Use TLS for DNS queries if TLS is available.	<i>enforce</i>	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.			
Option	Description											
<i>disable</i>	Disable DNS over TLS.											
<i>enable</i>	Use TLS for DNS queries if TLS is available.											
<i>enforce</i>	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.											
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory								
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127									
ip6-primary	Primary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified	0.0.0.0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system replacemsg-image

Configure replacement message images.

```
config system replacemsg-image
  Description: Configure replacement message images.
  edit <name>
    set image-type [gif|jpg|...]
    set image-base64 {var-string}
  next
end
```

## config system replacemsg-image

Parameter	Description	Type	Size	Default										
image-type	Image type.	option	-	png										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>gif</i></td> <td>GIF image.</td> </tr> <tr> <td><i>jpg</i></td> <td>JPEG image.</td> </tr> <tr> <td><i>tiff</i></td> <td>TIFF image.</td> </tr> <tr> <td><i>png</i></td> <td>PNG image.</td> </tr> </tbody> </table>	Option	Description	<i>gif</i>	GIF image.	<i>jpg</i>	JPEG image.	<i>tiff</i>	TIFF image.	<i>png</i>	PNG image.			
Option	Description													
<i>gif</i>	GIF image.													
<i>jpg</i>	JPEG image.													
<i>tiff</i>	TIFF image.													
<i>png</i>	PNG image.													
image-base64	Image data.	var-string	Maximum length: 32768											

## config system replacemsg mail

Replacement messages.

```
config system replacemsg mail
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
```

```

    set header [none|http|...]
    set format [none|text|...]
  next
end

```

## config system replacemsg mail

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg http

Replacement messages.

```

config system replacemsg http
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end

```

## config system replacemsg http

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg webproxy

Replacement messages.

```
config system replacemsg webproxy
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg webproxy

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg ftp

Replacement messages.

```

config system replacemsg ftp
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end

```

## config system replacemsg ftp

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg fortiguard-wf

Replacement messages.

```
config system replacemsg fortiguard-wf
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											



## config system replacemsg spam

Replacement messages.

```
config system replacemsg spam
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg spam

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg alertmail

Replacement messages.

```
config system replacemsg alertmail
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg alertmail

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg admin

Replacement messages.

```
config system replacemsg admin
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg admin

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg auth

Replacement messages.

```

config system replacemsg auth
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end

```

## config system replacemsg auth

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg sslvpn

Replacement messages.

```
config system replacemsg sslvpn
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg sslvpn

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg nac-quar

Replacement messages.

```
config system replacemsg nac-quar
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg nac-quar

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg traffic-quota

Replacement messages.

```
config system replacemsg traffic-quota
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg traffic-quota

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg utm

Replacement messages.

```
config system replacemsg utm
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg icap

Replacement messages.

```
config system replacemsg icap
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

## config system replacemsg icap

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system replacemsg-group

Configure replacement message groups.

```

config system replacemsg-group
  Description: Configure replacement message groups.
  edit <name>
    set comment {var-string}
    set group-type [default|utm|...]
  config mail
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
    next
  end
  config http
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
    next
  end
  config webproxy
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
    next
  end
  config ftp
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
    next
  end
  config fortiguard-wf
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}

```



```

        set header [none|http|...]
        set format [none|text|...]
    next
end
config spam
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config alertmail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config admin
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config auth
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config sslvpn
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config nac-quar
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config traffic-quota
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]

```

```

        set format [none|text|...]
    next
end
config utm
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config custom-message
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config icap
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
next
end

```

## config system replacemsg-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Per-vdom replacement messages.		
	<i>utm</i>	For use with UTM settings in firewall policies.		
	<i>auth</i>	For use with authentication pages in firewall policies.		

## config mail

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config http

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No header type.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP</td> </tr> <tr> <td><i>8bit</i></td> <td>8 bit.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No format type.</td> </tr> <tr> <td><i>text</i></td> <td>Text format.</td> </tr> <tr> <td><i>html</i></td> <td>HTML format.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config webproxy

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config ftp

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config fortiguard-wf

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config spam

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config alertmail

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config admin

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config auth

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config sslvpn

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config nac-quar

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config traffic-quota

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											



## config utm

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config custom-message

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config icap

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></tbody></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
Option	Description											
<i>none</i>	No header type.											
<i>http</i>	HTTP											
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></tbody></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
Option	Description											
<i>none</i>	No format type.											
<i>text</i>	Text format.											
<i>html</i>	HTML format.											

## config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
  Description: SNMP system info configuration.
  set status [enable|disable]
  set engine-id {string}
  set description {var-string}
  set contact-info {var-string}
  set location {var-string}
  set trap-high-cpu-threshold {integer}
  set trap-low-memory-threshold {integer}
  set trap-log-full-threshold {integer}
end
```

## config system snmp sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
engine-id	Local SNMP engineID string (maximum 24 characters).	string	Maximum length: 24							
description	System description.	var-string	Maximum length: 255							
contact-info	Contact information.	var-string	Maximum length: 255							
location	System location.	var-string	Maximum length: 255							
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80						
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80						
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	90						

## config system snmp community

SNMP community configuration.

```

config system snmp community
  Description: SNMP community configuration.
  edit <id>
    set name {string}
    set status [enable|disable]
  config hosts
    Description: Configure IPv4 SNMP managers (hosts).
    edit <id>
      set source-ip {ipv4-address}
      set ip {user}
      set ha-direct [enable|disable]
      set host-type [any|query|...]
    next
  end
  config hosts6
    Description: Configure IPv6 SNMP managers.

```

```

edit <id>
    set source-ipv6 {ipv6-address}
    set ipv6 {ipv6-prefix}
    set ha-direct [enable|disable]
    set host-type [any|query|...]
next
end
set query-v1-status [enable|disable]
set query-v1-port {integer}
set query-v2c-status [enable|disable]
set query-v2c-port {integer}
set trap-v1-status [enable|disable]
set trap-v1-lport {integer}
set trap-v1-rport {integer}
set trap-v2c-status [enable|disable]
set trap-v2c-lport {integer}
set trap-v2c-rport {integer}
set events {option1}, {option2}, ...
next
end

```

## config system snmp community

Parameter	Description	Type	Size	Default						
name	Community name.	string	Maximum length: 35							
status	Enable/disable this SNMP community.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v1-port	SNMP v1 query port .	integer	Minimum value: 1 Maximum value: 65535	161						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535	161						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v1-lport	SNMP v1 trap local port .	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v1-rport	SNMP v1 trap remote port .	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 1 Maximum value: 65535	162						

---

Parameter	Description	Type	Size	Default
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 1 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
events	SNMP trap events.	option	-	cpu-high mem-low log- full intf-ip vpn- tun-up vpn- tun-down ha- switch ha-hb- failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm-if-change bgp- established bgp- backward- transition ha- member-up ha-member- down ent- conf-change av-conserve av-bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open faz- disconnect wc-ap-up wc- ap-down fswctl- session-up fswctl- session-down load-balance- real-server- down per- cpu-high dhcp pool- usage **

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>cpu-high</i>	Send a trap when CPU usage is high.		
	<i>mem-low</i>	Send a trap when available memory is low.		
	<i>log-full</i>	Send a trap when log disk space becomes low.		
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.		
	<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.		
	<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.		
	<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.		
	<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.		
	<i>ips-signature</i>	Send a trap when IPS detects an attack.		
	<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.		
	<i>av-virus</i>	Send a trap when AntiVirus finds a virus.		
	<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.		
	<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.		
	<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.		
	<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.		
	<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.		
	<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.		
	<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.		
	<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.		
	<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.		
	<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		



Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ips-pkg-update</i></td> <td>Send a trap when the IPS signature database or engine is updated.</td> </tr> <tr> <td><i>ips-fail-open</i></td> <td>Send a trap when the IPS network buffer is full.</td> </tr> <tr> <td><i>faz-disconnect</i></td> <td>Send a trap when a FortiAnalyzer disconnects from the FortiGate.</td> </tr> <tr> <td><i>wc-ap-up</i></td> <td>Send a trap when a managed FortiAP comes up.</td> </tr> <tr> <td><i>wc-ap-down</i></td> <td>Send a trap when a managed FortiAP goes down.</td> </tr> <tr> <td><i>fswctl-session-up</i></td> <td>Send a trap when a FortiSwitch controller session comes up.</td> </tr> <tr> <td><i>fswctl-session-down</i></td> <td>Send a trap when a FortiSwitch controller session goes down.</td> </tr> <tr> <td><i>load-balance-real-server-down</i></td> <td>Send a trap when a server load balance real server goes down.</td> </tr> <tr> <td><i>device-new</i></td> <td>Send a trap when a new device is found.</td> </tr> <tr> <td><i>per-cpu-high</i></td> <td>Send a trap when per-CPU usage is high.</td> </tr> <tr> <td><i>dhcp</i></td> <td>Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.</td> </tr> <tr> <td><i>pool-usage</i></td> <td>Send a trap about ippool usage.</td> </tr> </tbody> </table>	Option	Description	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.	<i>device-new</i>	Send a trap when a new device is found.	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.	<i>pool-usage</i>	Send a trap about ippool usage.			
Option	Description																													
<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.																													
<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.																													
<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.																													
<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.																													
<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.																													
<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.																													
<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.																													
<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.																													
<i>device-new</i>	Send a trap when a new device is found.																													
<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.																													
<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.																													
<i>pool-usage</i>	Send a trap about ippool usage.																													

\*\* Values may differ between models.

## config hosts

Parameter	Description	Type	Size	Default						
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified	0.0.0.0						
ip	IPv4 address of the SNMP manager (host).	user	Not Specified							
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both. No traps will be sent when IP type is subnet.	option	-	any						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Accept queries from and send traps to this SNMP manager.</td> </tr> <tr> <td><i>query</i></td> <td>Accept queries from this SNMP manager but do not send traps.</td> </tr> <tr> <td><i>trap</i></td> <td>Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.	<i>query</i>	Accept queries from this SNMP manager but do not send traps.	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.			
Option	Description											
<i>any</i>	Accept queries from and send traps to this SNMP manager.											
<i>query</i>	Accept queries from this SNMP manager but do not send traps.											
<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.											

## config hosts6

Parameter	Description	Type	Size	Default								
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified	::								
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified	::/0								
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-	any								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Accept queries from and send traps to this SNMP manager.</td> </tr> <tr> <td><i>query</i></td> <td>Accept queries from this SNMP manager but do not send traps.</td> </tr> <tr> <td><i>trap</i></td> <td>Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.	<i>query</i>	Accept queries from this SNMP manager but do not send traps.	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.			
Option	Description											
<i>any</i>	Accept queries from and send traps to this SNMP manager.											
<i>query</i>	Accept queries from this SNMP manager but do not send traps.											
<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.											

## config system snmp user

SNMP user configuration.

```
config system snmp user
  Description: SNMP user configuration.
  edit <name>
    set status [enable|disable]
    set trap-status [enable|disable]
    set trap-lport {integer}
    set trap-rport {integer}
    set queries [enable|disable]
    set query-port {integer}
```

```

set notify-hosts {ipv4-address}
set notify-hosts6 {ipv6-address}
set source-ip {ipv4-address}
set source-ipv6 {ipv6-address}
set ha-direct [enable|disable]
set events {option1}, {option2}, ...
set security-level [no-auth-no-priv|auth-no-priv|...]
set auth-proto [md5|sha|...]
set auth-pwd {password}
set priv-proto [aes|des|...]
set priv-pwd {password}
next
end

```

## config system snmp user

Parameter	Description	Type	Size	Default						
status	Enable/disable this SNMP user.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-status	Enable/disable traps for this SNMP user.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-lport	SNMPv3 local trap port .	integer	Minimum value: 0 Maximum value: 65535	162						
trap-rport	SNMPv3 trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162						
queries	Enable/disable SNMP queries for this user.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161						
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified							
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified							
source-ip	Source IP for SNMP trap.	ipv4-address	Not Specified	0.0.0.0						
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified	::						
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log- full intf-ip vpn- tun-up vpn- tun-down ha- switch ha-hb- failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm-if-change bgp- established bgp- backward- transition ha- member-up ha-member- down ent- conf-change av-conserve av-bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open faz- disconnect wc-ap-up wc- ap-down fswctl- session-up fswctl- session-down load-balance- real-server- down per- cpu-high dhcp pool- usage **

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>cpu-high</i>	Send a trap when CPU usage is high.		
	<i>mem-low</i>	Send a trap when available memory is low.		
	<i>log-full</i>	Send a trap when log disk space becomes low.		
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.		
	<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.		
	<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.		
	<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.		
	<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.		
	<i>ips-signature</i>	Send a trap when IPS detects an attack.		
	<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.		
	<i>av-virus</i>	Send a trap when AntiVirus finds a virus.		
	<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.		
	<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.		
	<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.		
	<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.		
	<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.		
	<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.		
	<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.		
	<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.		
	<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.		
	<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ips-pkg-update</i></td> <td>Send a trap when the IPS signature database or engine is updated.</td> </tr> <tr> <td><i>ips-fail-open</i></td> <td>Send a trap when the IPS network buffer is full.</td> </tr> <tr> <td><i>faz-disconnect</i></td> <td>Send a trap when a FortiAnalyzer disconnects from the FortiGate.</td> </tr> <tr> <td><i>wc-ap-up</i></td> <td>Send a trap when a managed FortiAP comes up.</td> </tr> <tr> <td><i>wc-ap-down</i></td> <td>Send a trap when a managed FortiAP goes down.</td> </tr> <tr> <td><i>fswctl-session-up</i></td> <td>Send a trap when a FortiSwitch controller session comes up.</td> </tr> <tr> <td><i>fswctl-session-down</i></td> <td>Send a trap when a FortiSwitch controller session goes down.</td> </tr> <tr> <td><i>load-balance-real-server-down</i></td> <td>Send a trap when a server load balance real server goes down.</td> </tr> <tr> <td><i>device-new</i></td> <td>Send a trap when a new device is found.</td> </tr> <tr> <td><i>per-cpu-high</i></td> <td>Send a trap when per-CPU usage is high.</td> </tr> <tr> <td><i>dhcp</i></td> <td>Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.</td> </tr> <tr> <td><i>pool-usage</i></td> <td>Send a trap about ippool usage.</td> </tr> </tbody> </table>	Option	Description	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.	<i>device-new</i>	Send a trap when a new device is found.	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.	<i>pool-usage</i>	Send a trap about ippool usage.			
Option	Description																													
<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.																													
<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.																													
<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.																													
<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.																													
<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.																													
<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.																													
<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.																													
<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.																													
<i>device-new</i>	Send a trap when a new device is found.																													
<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.																													
<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.																													
<i>pool-usage</i>	Send a trap about ippool usage.																													
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-auth-no-priv</i></td> <td>Message with no authentication and no privacy (encryption).</td> </tr> <tr> <td><i>auth-no-priv</i></td> <td>Message with authentication but no privacy (encryption).</td> </tr> <tr> <td><i>auth-priv</i></td> <td>Message with authentication and privacy (encryption).</td> </tr> </tbody> </table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).																					
Option	Description																													
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).																													
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).																													
<i>auth-priv</i>	Message with authentication and privacy (encryption).																													
auth-PROTO	Authentication protocol.	option	-	sha																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>HMAC-MD5-96 authentication protocol.</td> </tr> <tr> <td><i>sha</i></td> <td>HMAC-SHA-96 authentication protocol.</td> </tr> <tr> <td><i>sha224</i></td> <td>HMAC-SHA224 authentication protocol.</td> </tr> <tr> <td><i>sha256</i></td> <td>HMAC-SHA256 authentication protocol.</td> </tr> <tr> <td><i>sha384</i></td> <td>HMAC-SHA384 authentication protocol.</td> </tr> <tr> <td><i>sha512</i></td> <td>HMAC-SHA512 authentication protocol.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	HMAC-MD5-96 authentication protocol.	<i>sha</i>	HMAC-SHA-96 authentication protocol.	<i>sha224</i>	HMAC-SHA224 authentication protocol.	<i>sha256</i>	HMAC-SHA256 authentication protocol.	<i>sha384</i>	HMAC-SHA384 authentication protocol.	<i>sha512</i>	HMAC-SHA512 authentication protocol.															
Option	Description																													
<i>md5</i>	HMAC-MD5-96 authentication protocol.																													
<i>sha</i>	HMAC-SHA-96 authentication protocol.																													
<i>sha224</i>	HMAC-SHA224 authentication protocol.																													
<i>sha256</i>	HMAC-SHA256 authentication protocol.																													
<i>sha384</i>	HMAC-SHA384 authentication protocol.																													
<i>sha512</i>	HMAC-SHA512 authentication protocol.																													

Parameter	Description	Type	Size	Default
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes
	<b>Option</b>	<b>Description</b>		
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.		
	<i>des</i>	CBC-DES symmetric encryption protocol.		
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.		
	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

\*\* Values may differ between models.

## config system autoupdate push-update

Configure push updates.

```
config system autoupdate push-update
  Description: Configure push updates.
  set status [enable|disable]
  set override [enable|disable]
  set address {string}
  set port {integer}
end
```

## config system autoupdate push-update

Parameter	Description	Type	Size	Default
status	Enable/disable push updates.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override	Enable/disable push update override server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		



Parameter	Description	Type	Size	Default
address	IPv4 or IPv6 address used by FortiGuard servers to send push updates to this FortiGate.	string	Maximum length: 63	0.0.0.0
port	Push update override port. (Do not overlap with other service ports)	integer	Minimum value: 0 Maximum value: 65535	9443

## config system autoupdate schedule

Configure update schedule.

```
config system autoupdate schedule
  Description: Configure update schedule.
  set status [enable|disable]
  set frequency [every|daily|...]
  set time {user}
  set day [Sunday|Monday|...]
end
```

## config system autoupdate schedule

Parameter	Description	Type	Size	Default								
status	Enable/disable scheduled updates.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
frequency	Update frequency.	option	-	every								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>every</i></td> <td>Time interval.</td> </tr> <tr> <td><i>daily</i></td> <td>Every day.</td> </tr> <tr> <td><i>weekly</i></td> <td>Every week.</td> </tr> </tbody> </table>	Option	Description	<i>every</i>	Time interval.	<i>daily</i>	Every day.	<i>weekly</i>	Every week.			
Option	Description											
<i>every</i>	Time interval.											
<i>daily</i>	Every day.											
<i>weekly</i>	Every week.											
time	Update time.	user	Not Specified									
day	Update day.	option	-	Monday								

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Sunday</i></td> <td>Update every Sunday.</td> </tr> <tr> <td><i>Monday</i></td> <td>Update every Monday.</td> </tr> <tr> <td><i>Tuesday</i></td> <td>Update every Tuesday.</td> </tr> <tr> <td><i>Wednesday</i></td> <td>Update every Wednesday.</td> </tr> <tr> <td><i>Thursday</i></td> <td>Update every Thursday.</td> </tr> <tr> <td><i>Friday</i></td> <td>Update every Friday.</td> </tr> <tr> <td><i>Saturday</i></td> <td>Update every Saturday.</td> </tr> </tbody> </table>	Option	Description	<i>Sunday</i>	Update every Sunday.	<i>Monday</i>	Update every Monday.	<i>Tuesday</i>	Update every Tuesday.	<i>Wednesday</i>	Update every Wednesday.	<i>Thursday</i>	Update every Thursday.	<i>Friday</i>	Update every Friday.	<i>Saturday</i>	Update every Saturday.			
Option	Description																			
<i>Sunday</i>	Update every Sunday.																			
<i>Monday</i>	Update every Monday.																			
<i>Tuesday</i>	Update every Tuesday.																			
<i>Wednesday</i>	Update every Wednesday.																			
<i>Thursday</i>	Update every Thursday.																			
<i>Friday</i>	Update every Friday.																			
<i>Saturday</i>	Update every Saturday.																			

## config system autoupdate tunneling

Configure web proxy tunnelling for the FDN.

```
config system autoupdate tunneling
  Description: Configure web proxy tunnelling for the FDN.
  set status [enable|disable]
  set address {string}
  set port {integer}
  set username {string}
  set password {password}
end
```

## config system autoupdate tunneling

Parameter	Description	Type	Size	Default						
status	Enable/disable web proxy tunnelling.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
address	Web proxy IP address or FQDN.	string	Maximum length: 63							
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default
username	Web proxy username.	string	Maximum length: 49	
password	Web proxy password.	password	Not Specified	

## config system session-ttl

Configure global session TTL timers for this FortiGate.

```
config system session-ttl
  Description: Configure global session TTL timers for this FortiGate.
  set default {user}
  config port
    Description: Session TTL port.
    edit <id>
      set protocol {integer}
      set start-port {integer}
      set end-port {integer}
      set timeout {user}
    next
  end
end
```

## config system session-ttl

Parameter	Description	Type	Size	Default
default	Default timeout.	user	Not Specified	

## config port

Parameter	Description	Type	Size	Default
protocol	Protocol .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535	0
timeout	Session timeout (TTL).	user	Not Specified	

## config system dhcp server

Configure DHCP servers.

```

config system dhcp server
  Description: Configure DHCP servers.
  edit <id>
    set status [disable|enable]
    set lease-time {integer}
    set mac-acl-default-action [assign|block]
    set forticlient-on-net-status [disable|enable]
    set dns-service [local|default|...]
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-server3 {ipv4-address}
    set dns-server4 {ipv4-address}
    set wifi-ac-service [specify|local]
    set wifi-ac1 {ipv4-address}
    set wifi-ac2 {ipv4-address}
    set wifi-ac3 {ipv4-address}
    set ntp-service [local|default|...]
    set ntp-server1 {ipv4-address}
    set ntp-server2 {ipv4-address}
    set ntp-server3 {ipv4-address}
    set domain {string}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
    set default-gateway {ipv4-address}
    set next-server {ipv4-address}
    set netmask {ipv4-netmask}
    set interface {string}
  config ip-range
    Description: DHCP IP range configuration.
    edit <id>
      set start-ip {ipv4-address}
      set end-ip {ipv4-address}
    next
  end
  set timezone-option [disable|default|...]
  set timezone [01|02|...]
  set tftp-server <tftp-server1>, <tftp-server2>, ...
  set filename {string}
  config options
    Description: DHCP options.

```

```

edit <id>
    set code {integer}
    set type [hex|string|...]
    set value {string}
    set ip {user}
next
end
set server-type [regular|ipsec]
set ip-mode [range|usrgrp]
set conflicted-ip-timeout {integer}
set ipsec-lease-hold {integer}
set auto-configuration [disable|enable]
set dhcp-settings-from-fortiipam [disable|enable]
set auto-managed-status [disable|enable]
set ddns-update [disable|enable]
set ddns-update-override [disable|enable]
set ddns-server-ip {ipv4-address}
set ddns-zone {string}
set ddns-auth [disable|tsig]
set ddns-keyname {string}
set ddns-key {user}
set ddns-ttl {integer}
set vci-match [disable|enable]
set vci-string <vci-string1>, <vci-string2>, ...
config exclude-range
    Description: Exclude one or more ranges of IP addresses from being assigned to
        clients.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
config reserved-address
    Description: Options for the DHCP server to assign IP settings to specific MAC
        addresses.
    edit <id>
        set type [mac|option82]
        set ip {ipv4-address}
        set mac {mac-address}
        set action [assign|block|...]
        set circuit-id-type [hex|string]
        set circuit-id {string}
        set remote-id-type [hex|string]
        set remote-id {string}
        set description {var-string}
    next
end
next
end

```

## config system dhcp server

Parameter	Description	Type	Size	Default								
status	Enable/disable this DHCP configuration.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not use this DHCP server configuration.</td> </tr> <tr> <td><i>enable</i></td> <td>Use this DHCP server configuration.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not use this DHCP server configuration.	<i>enable</i>	Use this DHCP server configuration.					
Option	Description											
<i>disable</i>	Do not use this DHCP server configuration.											
<i>enable</i>	Use this DHCP server configuration.											
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800								
mac-acl-default-action	MAC access control default action (allow or block assigning IP settings).	option	-	assign								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>assign</i></td> <td>Allow the DHCP server to assign IP settings to clients on the MAC access control list.</td> </tr> <tr> <td><i>block</i></td> <td>Block the DHCP server from assigning IP settings to clients on the MAC access control list.</td> </tr> </tbody> </table>	Option	Description	<i>assign</i>	Allow the DHCP server to assign IP settings to clients on the MAC access control list.	<i>block</i>	Block the DHCP server from assigning IP settings to clients on the MAC access control list.					
Option	Description											
<i>assign</i>	Allow the DHCP server to assign IP settings to clients on the MAC access control list.											
<i>block</i>	Block the DHCP server from assigning IP settings to clients on the MAC access control list.											
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable FortiClient On-Net Status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable FortiClient On-Net Status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable FortiClient On-Net Status.	<i>enable</i>	Enable FortiClient On-Net Status.					
Option	Description											
<i>disable</i>	Disable FortiClient On-Net Status.											
<i>enable</i>	Enable FortiClient On-Net Status.											
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>local</i></td> <td>IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.</td> </tr> <tr> <td><i>default</i></td> <td>Clients are assigned the FortiGate's configured DNS servers.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify up to 3 DNS servers in the DHCP server configuration.</td> </tr> </tbody> </table>	Option	Description	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.			
Option	Description											
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.											
<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.											
<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.											
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0								
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default								
dns-server3	DNS server 3.	ipv4-address	Not Specified	0.0.0.0								
dns-server4	DNS server 4.	ipv4-address	Not Specified	0.0.0.0								
wifi-ac-service	Options for assigning WiFi Access Controllers to DHCP clients	option	-	specify								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>specify</i></td> <td>Specify up to 3 WiFi Access Controllers in the DHCP server configuration.</td> </tr> <tr> <td><i>local</i></td> <td>IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.</td> </tr> </tbody> </table>	Option	Description	<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.					
Option	Description											
<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.											
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.											
wifi-ac1	WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0								
wifi-ac2	WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0								
wifi-ac3	WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0								
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-	specify								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>local</i></td> <td>IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.</td> </tr> <tr> <td><i>default</i></td> <td>Clients are assigned the FortiGate's configured NTP servers.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify up to 3 NTP servers in the DHCP server configuration.</td> </tr> </tbody> </table>	Option	Description	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.	<i>default</i>	Clients are assigned the FortiGate's configured NTP servers.	<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.			
Option	Description											
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.											
<i>default</i>	Clients are assigned the FortiGate's configured NTP servers.											
<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.											
ntp-server1	NTP server 1.	ipv4-address	Not Specified	0.0.0.0								
ntp-server2	NTP server 2.	ipv4-address	Not Specified	0.0.0.0								
ntp-server3	NTP server 3.	ipv4-address	Not Specified	0.0.0.0								
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35									
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0								
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default																																
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified	0.0.0.0																																
next-server	IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.	ipv4-address	Not Specified	0.0.0.0																																
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified	0.0.0.0																																
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15																																	
timezone-option	Options for the DHCP server to set the client's time zone.	option	-	disable																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not set the client's time zone.</td> </tr> <tr> <td><i>default</i></td> <td>Clients are assigned the FortiGate's configured time zone.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify the time zone to be assigned to DHCP clients.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not set the client's time zone.	<i>default</i>	Clients are assigned the FortiGate's configured time zone.	<i>specify</i>	Specify the time zone to be assigned to DHCP clients.																											
Option	Description																																			
<i>disable</i>	Do not set the client's time zone.																																			
<i>default</i>	Clients are assigned the FortiGate's configured time zone.																																			
<i>specify</i>	Specify the time zone to be assigned to DHCP clients.																																			
timezone	Select the time zone to be assigned to DHCP clients.	option	-	00																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>01</td> <td>(GMT-11:00) Midway Island, Samoa</td> </tr> <tr> <td>02</td> <td>(GMT-10:00) Hawaii</td> </tr> <tr> <td>03</td> <td>(GMT-9:00) Alaska</td> </tr> <tr> <td>04</td> <td>(GMT-8:00) Pacific Time (US &amp; Canada)</td> </tr> <tr> <td>05</td> <td>(GMT-7:00) Arizona</td> </tr> <tr> <td>81</td> <td>(GMT-7:00) Baja California Sur, Chihuahua</td> </tr> <tr> <td>06</td> <td>(GMT-7:00) Mountain Time (US &amp; Canada)</td> </tr> <tr> <td>07</td> <td>(GMT-6:00) Central America</td> </tr> <tr> <td>08</td> <td>(GMT-6:00) Central Time (US &amp; Canada)</td> </tr> <tr> <td>09</td> <td>(GMT-6:00) Mexico City</td> </tr> <tr> <td>10</td> <td>(GMT-6:00) Saskatchewan</td> </tr> <tr> <td>11</td> <td>(GMT-5:00) Bogota, Lima, Quito</td> </tr> <tr> <td>12</td> <td>(GMT-5:00) Eastern Time (US &amp; Canada)</td> </tr> <tr> <td>13</td> <td>(GMT-5:00) Indiana (East)</td> </tr> <tr> <td>74</td> <td>(GMT-4:00) Caracas</td> </tr> </tbody> </table>	Option	Description	01	(GMT-11:00) Midway Island, Samoa	02	(GMT-10:00) Hawaii	03	(GMT-9:00) Alaska	04	(GMT-8:00) Pacific Time (US & Canada)	05	(GMT-7:00) Arizona	81	(GMT-7:00) Baja California Sur, Chihuahua	06	(GMT-7:00) Mountain Time (US & Canada)	07	(GMT-6:00) Central America	08	(GMT-6:00) Central Time (US & Canada)	09	(GMT-6:00) Mexico City	10	(GMT-6:00) Saskatchewan	11	(GMT-5:00) Bogota, Lima, Quito	12	(GMT-5:00) Eastern Time (US & Canada)	13	(GMT-5:00) Indiana (East)	74	(GMT-4:00) Caracas			
Option	Description																																			
01	(GMT-11:00) Midway Island, Samoa																																			
02	(GMT-10:00) Hawaii																																			
03	(GMT-9:00) Alaska																																			
04	(GMT-8:00) Pacific Time (US & Canada)																																			
05	(GMT-7:00) Arizona																																			
81	(GMT-7:00) Baja California Sur, Chihuahua																																			
06	(GMT-7:00) Mountain Time (US & Canada)																																			
07	(GMT-6:00) Central America																																			
08	(GMT-6:00) Central Time (US & Canada)																																			
09	(GMT-6:00) Mexico City																																			
10	(GMT-6:00) Saskatchewan																																			
11	(GMT-5:00) Bogota, Lima, Quito																																			
12	(GMT-5:00) Eastern Time (US & Canada)																																			
13	(GMT-5:00) Indiana (East)																																			
74	(GMT-4:00) Caracas																																			



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	14	(GMT-4:00) Atlantic Time (Canada)		
	77	(GMT-4:00) Georgetown		
	15	(GMT-4:00) La Paz		
	87	(GMT-4:00) Paraguay		
	16	(GMT-3:00) Santiago		
	17	(GMT-3:30) Newfoundland		
	18	(GMT-3:00) Brasilia		
	19	(GMT-3:00) Buenos Aires		
	20	(GMT-3:00) Nuuk (Greenland)		
	75	(GMT-3:00) Uruguay		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Athens, Sofia, Vilnius		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	44	(GMT+4:30) Kabul		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepara		
	48	(GMT+5:45) Kathmandu		
	45	(GMT+5:00) Ekaterinburg		
	49	(GMT+6:00) Almaty, Novosibirsk		
	50	(GMT+6:00) Astana, Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		
	58	(GMT+8:00) Perth		
	59	(GMT+8:00) Taipei		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul		
	62	(GMT+9:30) Adelaide		
	63	(GMT+9:30) Darwin		

Parameter	Description	Type	Size	Default																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>61</td> <td>(GMT+9:00) Yakutsk</td> </tr> <tr> <td>64</td> <td>(GMT+10:00) Brisbane</td> </tr> <tr> <td>65</td> <td>(GMT+10:00) Canberra, Melbourne, Sydney</td> </tr> <tr> <td>66</td> <td>(GMT+10:00) Guam, Port Moresby</td> </tr> <tr> <td>67</td> <td>(GMT+10:00) Hobart</td> </tr> <tr> <td>68</td> <td>(GMT+10:00) Vladivostok</td> </tr> <tr> <td>69</td> <td>(GMT+10:00) Magadan</td> </tr> <tr> <td>70</td> <td>(GMT+11:00) Solomon Is., New Caledonia</td> </tr> <tr> <td>71</td> <td>(GMT+12:00) Auckland, Wellington</td> </tr> <tr> <td>72</td> <td>(GMT+12:00) Fiji, Kamchatka, Marshall Is.</td> </tr> <tr> <td>00</td> <td>(GMT+12:00) Eniwetok, Kwajalein</td> </tr> <tr> <td>82</td> <td>(GMT+12:45) Chatham Islands</td> </tr> <tr> <td>73</td> <td>(GMT+13:00) Nuku'alofa</td> </tr> <tr> <td>86</td> <td>(GMT+13:00) Samoa</td> </tr> <tr> <td>76</td> <td>(GMT+14:00) Kiritimati</td> </tr> </tbody> </table>	Option	Description	61	(GMT+9:00) Yakutsk	64	(GMT+10:00) Brisbane	65	(GMT+10:00) Canberra, Melbourne, Sydney	66	(GMT+10:00) Guam, Port Moresby	67	(GMT+10:00) Hobart	68	(GMT+10:00) Vladivostok	69	(GMT+10:00) Magadan	70	(GMT+11:00) Solomon Is., New Caledonia	71	(GMT+12:00) Auckland, Wellington	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.	00	(GMT+12:00) Eniwetok, Kwajalein	82	(GMT+12:45) Chatham Islands	73	(GMT+13:00) Nuku'alofa	86	(GMT+13:00) Samoa	76	(GMT+14:00) Kiritimati			
Option	Description																																			
61	(GMT+9:00) Yakutsk																																			
64	(GMT+10:00) Brisbane																																			
65	(GMT+10:00) Canberra, Melbourne, Sydney																																			
66	(GMT+10:00) Guam, Port Moresby																																			
67	(GMT+10:00) Hobart																																			
68	(GMT+10:00) Vladivostok																																			
69	(GMT+10:00) Magadan																																			
70	(GMT+11:00) Solomon Is., New Caledonia																																			
71	(GMT+12:00) Auckland, Wellington																																			
72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.																																			
00	(GMT+12:00) Eniwetok, Kwajalein																																			
82	(GMT+12:45) Chatham Islands																																			
73	(GMT+13:00) Nuku'alofa																																			
86	(GMT+13:00) Samoa																																			
76	(GMT+14:00) Kiritimati																																			
tftp-server <tftp-server>	One or more hostnames or IP addresses of the TFTP servers in quotes separated by spaces. TFTP server.	string	Maximum length: 63																																	
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127																																	
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-	regular																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>regular</i></td> <td>Regular DHCP service.</td> </tr> <tr> <td><i>ipsec</i></td> <td>DHCP over IPsec service.</td> </tr> </tbody> </table>	Option	Description	<i>regular</i>	Regular DHCP service.	<i>ipsec</i>	DHCP over IPsec service.																													
Option	Description																																			
<i>regular</i>	Regular DHCP service.																																			
<i>ipsec</i>	DHCP over IPsec service.																																			
ip-mode	Method used to assign client IP.	option	-	range																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>range</i></td> <td>Use range defined by start-ip/end-ip to assign client IP.</td> </tr> <tr> <td><i>usrgrp</i></td> <td>Use user-group defined method to assign client IP.</td> </tr> </tbody> </table>	Option	Description	<i>range</i>	Use range defined by start-ip/end-ip to assign client IP.	<i>usrgrp</i>	Use user-group defined method to assign client IP.																													
Option	Description																																			
<i>range</i>	Use range defined by start-ip/end-ip to assign client IP.																																			
<i>usrgrp</i>	Use user-group defined method to assign client IP.																																			

Parameter	Description	Type	Size	Default
conflicted-ip-timeout	Time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused.	integer	Minimum value: 60 Maximum value: 8640000	1800
ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 0 Maximum value: 8640000	60
auto-configuration	Enable/disable auto configuration.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable auto configuration.		
	<i>enable</i>	Enable auto configuration.		
dhcp-settings-from-fortipam	Enable/disable populating of DHCP server settings from FortiPAM.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable populating of DHCP server settings from FortiPAM.		
	<i>enable</i>	Enable populating of DHCP server settings from FortiPAM.		
auto-managed-status	Enable/disable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.		
	<i>enable</i>	Enable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.		
ddns-update	Enable/disable DDNS update for DHCP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DDNS update for DHCP.		
	<i>enable</i>	Enable DDNS update for DHCP.		
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DDNS update override for DHCP.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable DDNS update override for DHCP.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DDNS update override for DHCP.	<i>enable</i>	Enable DDNS update override for DHCP.			
Option	Description									
<i>disable</i>	Disable DDNS update override for DHCP.									
<i>enable</i>	Enable DDNS update override for DHCP.									
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified	0.0.0.0						
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64							
ddns-auth	DDNS authentication mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DDNS authentication.</td> </tr> <tr> <td><i>tsig</i></td> <td>TSIG based on RFC2845.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DDNS authentication.	<i>tsig</i>	TSIG based on RFC2845.			
Option	Description									
<i>disable</i>	Disable DDNS authentication.									
<i>tsig</i>	TSIG based on RFC2845.									
ddns-keyname	DDNS update key name.	string	Maximum length: 64							
ddns-key	DDNS update key (base 64 encoding).	user	Not Specified							
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400	300						
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable VCI matching.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable VCI matching.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable VCI matching.	<i>enable</i>	Enable VCI matching.			
Option	Description									
<i>disable</i>	Disable VCI matching.									
<i>enable</i>	Enable VCI matching.									
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255							

### config ip-range

Parameter	Description	Type	Size	Default
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0

### config options

Parameter	Description	Type	Size	Default										
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0										
type	DHCP option type.	option	-	hex										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hex</i></td> <td>DHCP option in hex.</td> </tr> <tr> <td><i>string</i></td> <td>DHCP option in string.</td> </tr> <tr> <td><i>ip</i></td> <td>DHCP option in IP.</td> </tr> <tr> <td><i>fqdn</i></td> <td>DHCP option in domain search option format.</td> </tr> </tbody> </table>	Option	Description	<i>hex</i>	DHCP option in hex.	<i>string</i>	DHCP option in string.	<i>ip</i>	DHCP option in IP.	<i>fqdn</i>	DHCP option in domain search option format.			
Option	Description													
<i>hex</i>	DHCP option in hex.													
<i>string</i>	DHCP option in string.													
<i>ip</i>	DHCP option in IP.													
<i>fqdn</i>	DHCP option in domain search option format.													
value	DHCP option value.	string	Maximum length: 312											
ip	DHCP option IPs.	user	Not Specified											

### config exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0

### config reserved-address

Parameter	Description	Type	Size	Default						
type	DHCP reserved-address type.	option	-	mac						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mac</i></td> <td>Match with MAC address.</td> </tr> <tr> <td><i>option82</i></td> <td>Match with DHCP option 82.</td> </tr> </tbody> </table>	Option	Description	<i>mac</i>	Match with MAC address.	<i>option82</i>	Match with DHCP option 82.			
Option	Description									
<i>mac</i>	Match with MAC address.									
<i>option82</i>	Match with DHCP option 82.									

Parameter	Description	Type	Size	Default								
ip	IP address to be reserved for the MAC address.	ipv4-address	Not Specified	0.0.0.0								
mac	MAC address of the client that will get the reserved IP address.	mac-address	Not Specified	00:00:00:00:00:00								
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-	reserved								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>assign</i></td> <td>Configure the client with this MAC address like any other client.</td> </tr> <tr> <td><i>block</i></td> <td>Block the DHCP server from assigning IP settings to the client with this MAC address.</td> </tr> <tr> <td><i>reserved</i></td> <td>Assign the reserved IP address to the client with this MAC address.</td> </tr> </tbody> </table>	Option	Description	<i>assign</i>	Configure the client with this MAC address like any other client.	<i>block</i>	Block the DHCP server from assigning IP settings to the client with this MAC address.	<i>reserved</i>	Assign the reserved IP address to the client with this MAC address.			
Option	Description											
<i>assign</i>	Configure the client with this MAC address like any other client.											
<i>block</i>	Block the DHCP server from assigning IP settings to the client with this MAC address.											
<i>reserved</i>	Assign the reserved IP address to the client with this MAC address.											
circuit-id-type	DHCP option type.	option	-	string								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hex</i></td> <td>DHCP option in hex.</td> </tr> <tr> <td><i>string</i></td> <td>DHCP option in string.</td> </tr> </tbody> </table>	Option	Description	<i>hex</i>	DHCP option in hex.	<i>string</i>	DHCP option in string.					
Option	Description											
<i>hex</i>	DHCP option in hex.											
<i>string</i>	DHCP option in string.											
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312									
remote-id-type	DHCP option type.	option	-	string								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hex</i></td> <td>DHCP option in hex.</td> </tr> <tr> <td><i>string</i></td> <td>DHCP option in string.</td> </tr> </tbody> </table>	Option	Description	<i>hex</i>	DHCP option in hex.	<i>string</i>	DHCP option in string.					
Option	Description											
<i>hex</i>	DHCP option in hex.											
<i>string</i>	DHCP option in string.											
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312									
description	Description.	var-string	Maximum length: 255									

## config system dhcp6 server

Configure DHCPv6 servers.

```
config system dhcp6 server
  Description: Configure DHCPv6 servers.
  edit <id>
    set status [disable|enable]
    set rapid-commit [disable|enable]
    set lease-time {integer}
```

```

set dns-service [delegated|default|...]
set dns-search-list [delegated|specify]
set dns-server1 {ipv6-address}
set dns-server2 {ipv6-address}
set dns-server3 {ipv6-address}
set dns-server4 {ipv6-address}
set domain {string}
set subnet {ipv6-prefix}
set interface {string}
set option1 {user}
set option2 {user}
set option3 {user}
set upstream-interface {string}
set ip-mode [range|delegated]
config prefix-range
  Description: DHCP prefix configuration.
  edit <id>
    set start-prefix {ipv6-address}
    set end-prefix {ipv6-address}
    set prefix-length {integer}
  next
end
config ip-range
  Description: DHCP IP range configuration.
  edit <id>
    set start-ip {ipv6-address}
    set end-ip {ipv6-address}
  next
end
next
end

```

## config system dhcp6 server

Parameter	Description	Type	Size	Default						
status	Enable/disable this DHCPv6 configuration.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Enable this DHCPv6 server configuration.</td> </tr> <tr> <td><i>enable</i></td> <td>Disable this DHCPv6 server configuration.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable this DHCPv6 server configuration.	<i>enable</i>	Disable this DHCPv6 server configuration.			
Option	Description									
<i>disable</i>	Enable this DHCPv6 server configuration.									
<i>enable</i>	Disable this DHCPv6 server configuration.									
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not allow rapid commit.</td> </tr> <tr> <td><i>enable</i></td> <td>Allow rapid commit.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not allow rapid commit.	<i>enable</i>	Allow rapid commit.			
Option	Description									
<i>disable</i>	Do not allow rapid commit.									
<i>enable</i>	Allow rapid commit.									



Parameter	Description	Type	Size	Default								
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800								
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-	specify								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>delegated</i></td> <td>Delegated DNS settings.</td> </tr> <tr> <td><i>default</i></td> <td>Clients are assigned the FortiGate's configured DNS servers.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify up to 3 DNS servers in the DHCPv6 server configuration.</td> </tr> </tbody> </table>	Option	Description	<i>delegated</i>	Delegated DNS settings.	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.	<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.			
Option	Description											
<i>delegated</i>	Delegated DNS settings.											
<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.											
<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.											
dns-search-list	DNS search list options.	option	-	specify								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>delegated</i></td> <td>Delegated the DNS search list.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify the DNS search list.</td> </tr> </tbody> </table>	Option	Description	<i>delegated</i>	Delegated the DNS search list.	<i>specify</i>	Specify the DNS search list.					
Option	Description											
<i>delegated</i>	Delegated the DNS search list.											
<i>specify</i>	Specify the DNS search list.											
dns-server1	DNS server 1.	ipv6-address	Not Specified	::								
dns-server2	DNS server 2.	ipv6-address	Not Specified	::								
dns-server3	DNS server 3.	ipv6-address	Not Specified	::								
dns-server4	DNS server 4.	ipv6-address	Not Specified	::								
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35									
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified	::/0								
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15									
option1	Option 1.	user	Not Specified									
option2	Option 2.	user	Not Specified									
option3	Option 3.	user	Not Specified									

Parameter	Description	Type	Size	Default
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15	
ip-mode	Method used to assign client IP.	option	-	range
	<b>Option</b>	<b>Description</b>		
	<i>range</i>	Use range defined by start IP/end IP to assign client IP.		
	<i>delegated</i>	Use delegated prefix method to assign client IP.		

### config prefix-range

Parameter	Description	Type	Size	Default
start-prefix	Start of prefix range.	ipv6-address	Not Specified	::
end-prefix	End of prefix range.	ipv6-address	Not Specified	::
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128	0

### config ip-range

Parameter	Description	Type	Size	Default
start-ip	Start of IP range.	ipv6-address	Not Specified	::
end-ip	End of IP range.	ipv6-address	Not Specified	::

### config system modem



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64.

#### Configure MODEM.

```
config system modem
  Description: Configure MODEM.
  set status [enable|disable]
  set pin-init {string}
  set network-init {string}
  set lockdown-lac {string}
```

```

set mode [standalone|redundant]
set auto-dial [enable|disable]
set dial-on-demand [enable|disable]
set idle-timer {integer}
set redial [none|1|...]
set reset {integer}
set holddown-timer {integer}
set connect-timeout {integer}
set interface {string}
set wireless-port {integer}
set dont-send-CR1 [enable|disable]
set phone1 {string}
set dial-cmd1 {string}
set username1 {string}
set passwd1 {password}
set extra-init1 {string}
set peer-modem1 [generic|actiontec|...]
set ppp-echo-request1 [enable|disable]
set authtype1 {option1}, {option2}, ...
set dont-send-CR2 [enable|disable]
set phone2 {string}
set dial-cmd2 {string}
set username2 {string}
set passwd2 {password}
set extra-init2 {string}
set peer-modem2 [generic|actiontec|...]
set ppp-echo-request2 [enable|disable]
set authtype2 {option1}, {option2}, ...
set dont-send-CR3 [enable|disable]
set phone3 {string}
set dial-cmd3 {string}
set username3 {string}
set passwd3 {password}
set extra-init3 {string}
set peer-modem3 [generic|actiontec|...]
set ppp-echo-request3 [enable|disable]
set altmode [enable|disable]
set authtype3 {option1}, {option2}, ...
set traffic-check [enable|disable]
set action [dial|stop|...]
set distance {integer}
set priority {integer}
end

```

## config system modem

Parameter	Description	Type	Size	Default
status	Enable/disable Modem support (equivalent to bringing an interface up or down).	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
pin-init	AT command to set the PIN (AT+PIN=<pin>).	string	Maximum length: 127							
network-init	AT command to set the Network name/type (AT+COPS=<mode>,[<format>,<oper>[,<AcT>]]).	string	Maximum length: 127							
lockdown-lac	Allow connection only to the specified Location Area Code (LAC).	string	Maximum length: 127							
mode	Set MODEM operation mode to redundant or standalone.	option	-	standalone						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standalone</i></td> <td>Standalone.</td> </tr> <tr> <td><i>redundant</i></td> <td>Redundant for an interface.</td> </tr> </tbody> </table>	Option	Description	<i>standalone</i>	Standalone.	<i>redundant</i>	Redundant for an interface.			
Option	Description									
<i>standalone</i>	Standalone.									
<i>redundant</i>	Redundant for an interface.									
auto-dial	Enable/disable auto-dial after a reboot or disconnection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dial-on-demand	Enable/disable to dial the modem when packets are routed to the modem interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
idle-timer	MODEM connection idle time .	integer	Minimum value: 1 Maximum value: 9999	5						
redial	Redial limit .	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Forever.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Forever.					
Option	Description									
<i>none</i>	Forever.									

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>One attempt.</td> </tr> <tr> <td>2</td> <td>Two attempts.</td> </tr> <tr> <td>3</td> <td>Three attempts.</td> </tr> <tr> <td>4</td> <td>Four attempts.</td> </tr> <tr> <td>5</td> <td>Five attempts.</td> </tr> <tr> <td>6</td> <td>Six attempts.</td> </tr> <tr> <td>7</td> <td>Seven attempts.</td> </tr> <tr> <td>8</td> <td>Eight attempts.</td> </tr> <tr> <td>9</td> <td>Nine attempts.</td> </tr> <tr> <td>10</td> <td>Ten attempts.</td> </tr> </tbody> </table>	Option	Description	1	One attempt.	2	Two attempts.	3	Three attempts.	4	Four attempts.	5	Five attempts.	6	Six attempts.	7	Seven attempts.	8	Eight attempts.	9	Nine attempts.	10	Ten attempts.			
Option	Description																									
1	One attempt.																									
2	Two attempts.																									
3	Three attempts.																									
4	Four attempts.																									
5	Five attempts.																									
6	Six attempts.																									
7	Seven attempts.																									
8	Eight attempts.																									
9	Nine attempts.																									
10	Ten attempts.																									
reset	Number of dial attempts before resetting modem (0 = never reset).	integer	Minimum value: 0 Maximum value: 10	0																						
holddown-timer	Hold down timer in seconds .	integer	Minimum value: 1 Maximum value: 60	60																						
connect-timeout	Connection completion timeout .	integer	Minimum value: 30 Maximum value: 255	90																						
interface	Name of redundant interface.	string	Maximum length: 63																							
wireless-port	Enter wireless port number, 0 for default, 1 for first port, ...	integer	Minimum value: 0 Maximum value: 4294967295	0																						
dont-send-CR1	Do not send CR when connected (ISP1).	option	-	disable																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																			
Option	Description																									
<i>enable</i>	Enable setting.																									
<i>disable</i>	Disable setting.																									

Parameter	Description	Type	Size	Default
phone1	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
dial-cmd1	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63	
username1	User name to access the specified dialup account.	string	Maximum length: 63	
passwd1	Password to access the specified dialup account.	password	Not Specified	
extra-init1	Extra initialization string to ISP 1.	string	Maximum length: 127	
peer-modem1	Specify peer MODEM type for phone1.	option	-	generic
	<b>Option</b>	<b>Description</b>		
	<i>generic</i>	All other modem type.		
	<i>actiontec</i>	ActionTec modem.		
	<i>ascend_TNT</i>	Ascend TNT modem.		
ppp-echo-request1	Enable/disable PPP echo-request to ISP 1.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
authtype1	Allowed authentication types for ISP 1.	option	-	pap chap mschap mschapv2
	<b>Option</b>	<b>Description</b>		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
dont-send-CR2	Do not send CR when connected (ISP2).	option	-	disable

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
phone2	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63											
dial-cmd2	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63											
username2	User name to access the specified dialup account.	string	Maximum length: 63											
passwd2	Password to access the specified dialup account.	password	Not Specified											
extra-init2	Extra initialization string to ISP 2.	string	Maximum length: 127											
peer-modem2	Specify peer MODEM type for phone2.	option	-	generic										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>generic</i></td> <td>All other modem type.</td> </tr> <tr> <td><i>actiontec</i></td> <td>ActionTec modem.</td> </tr> <tr> <td><i>ascend_TNT</i></td> <td>Ascend TNT modem.</td> </tr> </tbody> </table>	Option	Description	<i>generic</i>	All other modem type.	<i>actiontec</i>	ActionTec modem.	<i>ascend_TNT</i>	Ascend TNT modem.					
Option	Description													
<i>generic</i>	All other modem type.													
<i>actiontec</i>	ActionTec modem.													
<i>ascend_TNT</i>	Ascend TNT modem.													
ppp-echo-request2	Enable/disable PPP echo-request to ISP 2.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
authtype2	Allowed authentication types for ISP 2.	option	-	pap chap mschap mschapv2										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pap</i></td> <td>PAP</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP</td> </tr> <tr> <td><i>mschap</i></td> <td>MSCHAP</td> </tr> <tr> <td><i>mschapv2</i></td> <td>MSCHAPv2</td> </tr> </tbody> </table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2			
Option	Description													
<i>pap</i>	PAP													
<i>chap</i>	CHAP													
<i>mschap</i>	MSCHAP													
<i>mschapv2</i>	MSCHAPv2													

Parameter	Description	Type	Size	Default								
dont-send-CR3	Do not send CR when connected (ISP3).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
phone3	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63									
dial-cmd3	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63									
username3	User name to access the specified dialup account.	string	Maximum length: 63									
passwd3	Password to access the specified dialup account.	password	Not Specified									
extra-init3	Extra initialization string to ISP 3.	string	Maximum length: 127									
peer-modem3	Specify peer MODEM type for phone3.	option	-	generic								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>generic</i></td> <td>All other modem type.</td> </tr> <tr> <td><i>actiontec</i></td> <td>ActionTec modem.</td> </tr> <tr> <td><i>ascend_TNT</i></td> <td>Ascend TNT modem.</td> </tr> </tbody> </table>	Option	Description	<i>generic</i>	All other modem type.	<i>actiontec</i>	ActionTec modem.	<i>ascend_TNT</i>	Ascend TNT modem.			
Option	Description											
<i>generic</i>	All other modem type.											
<i>actiontec</i>	ActionTec modem.											
<i>ascend_TNT</i>	Ascend TNT modem.											
ppp-echo-request3	Enable/disable PPP echo-request to ISP 3.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
altmode	Enable/disable altmode for installations using PPP in China.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											



Parameter	Description	Type	Size	Default										
authtype3	Allowed authentication types for ISP 3.	option	-	pap chap mschap mschapv2										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pap</i></td> <td>PAP</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP</td> </tr> <tr> <td><i>mschap</i></td> <td>MSCHAP</td> </tr> <tr> <td><i>mschapv2</i></td> <td>MSCHAPv2</td> </tr> </tbody> </table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2			
Option	Description													
<i>pap</i>	PAP													
<i>chap</i>	CHAP													
<i>mschap</i>	MSCHAP													
<i>mschapv2</i>	MSCHAPv2													
traffic-check	Enable/disable traffic-check.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
action	Dial up/stop MODEM.	option	-	stop										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dial</i></td> <td>Dial up number.</td> </tr> <tr> <td><i>stop</i></td> <td>Stop dialup.</td> </tr> <tr> <td><i>none</i></td> <td>No action.</td> </tr> </tbody> </table>	Option	Description	<i>dial</i>	Dial up number.	<i>stop</i>	Stop dialup.	<i>none</i>	No action.					
Option	Description													
<i>dial</i>	Dial up number.													
<i>stop</i>	Stop dialup.													
<i>none</i>	No action.													
distance	Distance of learned routes .	integer	Minimum value: 1 Maximum value: 255	1										
priority	Priority of learned routes .	integer	Minimum value: 0 Maximum value: 4294967295	0										

## config system 3g-modem custom



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64.

3G MODEM custom.

```
config system 3g-modem custom
```

```

Description: 3G MODEM custom.
edit <id>
    set vendor {string}
    set model {string}
    set vendor-id {user}
    set product-id {user}
    set class-id {user}
    set init-string {string}
    set modeswitch-string {string}
next
end

```

## config system 3g-modem custom

Parameter	Description	Type	Size	Default
vendor	MODEM vendor name.	string	Maximum length: 35	
model	MODEM model name.	string	Maximum length: 35	
vendor-id	USB vendor ID in hexadecimal format (0000-ffff).	user	Not Specified	
product-id	USB product ID in hexadecimal format (0000-ffff).	user	Not Specified	
class-id	USB interface class in hexadecimal format (00-ff).	user	Not Specified	
init-string	Init string in hexadecimal format (even length).	string	Maximum length: 127	
modeswitch-string	USB modeswitch arguments. e.g: '-v 1410 -p 9030 -V 1410 -P 9032 -u 3'	string	Maximum length: 127	

## config system status

System status.

```

config system status
    Description: System status.
end

```

## config system performance status

System performance status.

```

config system performance status
    Description: System performance status.
end

```

---

## config system performance top

Display information about the top CPU processes.

```
config system performance top
  Description: Display information about the top CPU processes.
  set <delay> {string}
end
```

## config system performance top

Parameter	Description	Type	Size	Default
<delay>	Delay in seconds .	string	Maximum length: -1	

## config system performance firewall packet-distribution

Show distribution statistics.

```
config system performance firewall packet-distribution
  Description: Show distribution statistics.
end
```

## config system performance firewall statistics

Show traffic stats.

```
config system performance firewall statistics
  Description: Show traffic stats.
end
```

## config system session

System IPv4 session.

```
config system session
  Description: System IPv4 session.
end
```

## config system session6

System IPv6 session.

```
config system session6
  Description: System IPv6 session.
end
```

---

## config system cmdb

System CMDB information.

```
config system cmdb
  Description: System CMDB information.
end
```

## config system fortiguard-service

Configuration of FortiGuard services.

```
config system fortiguard-service
  Description: Configuration of FortiGuard services.
end
```

## config system fortianalyzer-connectivity

FortiAnalyzer Connectivity.

```
config system fortianalyzer-connectivity
  Description: FortiAnalyzer Connectivity.
end
```

## config system checksum status

System checksum.

```
config system checksum status
  Description: System checksum.
end
```

## config system mgmt-csum

System checksum for FortiManager use only.

```
config system mgmt-csum
  Description: System checksum for FortiManager use only.
end
```

## config system ha-nonsync-csum

System checksum for FortiManager use only.

```
config system ha-nonsync-csum
  Description: System checksum for FortiManager use only.
end
```

---

## config system fortiguard-log-service

Configuration of FortiCloud log service.

```
config system fortiguard-log-service
  Description: Configuration of FortiCloud log service.
end
```

## config system central-mgmt

Configuration of Central Management Service.

```
config system central-mgmt
  Description: Configuration of Central Management Service.
end
```

## config system alias

Configure alias command.

```
config system alias
  Description: Configure alias command.
  edit <name>
    set command {var-string}
  next
end
```

## config system alias

Parameter	Description	Type	Size	Default
command	Command list to execute.	var-string	Maximum length: 255	

## config system auto-script

Configure auto script.

```
config system auto-script
  Description: Configure auto script.
  edit <name>
    set interval {integer}
    set repeat {integer}
    set start [manual|auto]
    set script {var-string}
    set output-size {integer}
    set timeout {integer}
  next
end
```

## config system auto-script

Parameter	Description	Type	Size	Default						
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0						
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1						
start	Script starting mode.	option	-	manual						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>manual</i></td><td>Starting manually.</td></tr><tr><td><i>auto</i></td><td>Starting automatically.</td></tr></tbody></table>	Option	Description	<i>manual</i>	Starting manually.	<i>auto</i>	Starting automatically.			
Option	Description									
<i>manual</i>	Starting manually.									
<i>auto</i>	Starting automatically.									
script	List of FortiOS CLI commands to repeat.	var-string	Maximum length: 1023							
output-size	Number of megabytes to limit script output to .	integer	Minimum value: 10 Maximum value: 1024	10						
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0						

## config system info admin status

Show logged in administrators.

```
config system info admin status
  Description: Show logged in administrators.
end
```

## config system info admin ssh

Show SSH status.

```
config system info admin ssh
  Description: Show SSH status.
end
```

## config system management-tunnel

Management tunnel configuration.

```
config system management-tunnel
  Description: Management tunnel configuration.
  set status [enable|disable]
  set allow-config-restore [enable|disable]
  set allow-push-configuration [enable|disable]
  set allow-push-firmware [enable|disable]
  set allow-collect-statistics [enable|disable]
  set authorized-manager-only [enable|disable]
  set serial-number {user}
end
```

## config system management-tunnel

Parameter	Description	Type	Size	Default						
status	Enable/disable FGFM tunnel.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable management tunnel.</td></tr><tr><td><i>disable</i></td><td>Disable management tunnel.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable management tunnel.	<i>disable</i>	Disable management tunnel.			
Option	Description									
<i>enable</i>	Enable management tunnel.									
<i>disable</i>	Disable management tunnel.									
allow-config-restore	Enable/disable allow config restore.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable allow config restore.</td></tr><tr><td><i>disable</i></td><td>Disable allow config restore.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable allow config restore.	<i>disable</i>	Disable allow config restore.			
Option	Description									
<i>enable</i>	Enable allow config restore.									
<i>disable</i>	Disable allow config restore.									
allow-push-configuration	Enable/disable push configuration.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable push configuration.</td></tr><tr><td><i>disable</i></td><td>Disable push configuration.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable push configuration.	<i>disable</i>	Disable push configuration.			
Option	Description									
<i>enable</i>	Enable push configuration.									
<i>disable</i>	Disable push configuration.									
allow-push-firmware	Enable/disable push firmware.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable push firmware.</td></tr><tr><td><i>disable</i></td><td>Disable push firmware.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable push firmware.	<i>disable</i>	Disable push firmware.			
Option	Description									
<i>enable</i>	Enable push firmware.									
<i>disable</i>	Disable push firmware.									

Parameter	Description	Type	Size	Default						
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable collection of run time statistics.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable collection of run time statistics.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable collection of run time statistics.	<i>disable</i>	Disable collection of run time statistics.			
Option	Description									
<i>enable</i>	Enable collection of run time statistics.									
<i>disable</i>	Disable collection of run time statistics.									
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable restriction of authorized manager only.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable restriction of authorized manager only.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable restriction of authorized manager only.	<i>disable</i>	Disable restriction of authorized manager only.			
Option	Description									
<i>enable</i>	Enable restriction of authorized manager only.									
<i>disable</i>	Disable restriction of authorized manager only.									
serial-number	Serial number.	user	Not Specified							

## config system fortimanager

Configure FortiManager.

```

config system fortimanager
  Description: Configure FortiManager.
  set ip {ipv4-address-any}
  set vdom {string}
  set ipsec [enable|disable]
  set central-management [enable|disable]
  set central-mgmt-auto-backup [enable|disable]
  set central-mgmt-schedule-config-restore [enable|disable]
  set central-mgmt-schedule-script-restore [enable|disable]
end

```

## config system fortimanager

Parameter	Description	Type	Size	Default
ip	IP address.	ipv4-address-any	Not Specified	0.0.0.0
vdom	Virtual domain name.	string	Maximum length: 31	root
ipsec	Enable/disable FortiManager IPsec tunnel.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiManager IPsec tunnel.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiManager IPsec tunnel.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiManager IPsec tunnel.	<i>disable</i>	Disable FortiManager IPsec tunnel.			
Option	Description									
<i>enable</i>	Enable FortiManager IPsec tunnel.									
<i>disable</i>	Disable FortiManager IPsec tunnel.									
central-management	Enable/disable FortiManager central management.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable central management.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable central management.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable central management.	<i>disable</i>	Disable central management.			
Option	Description									
<i>enable</i>	Enable central management.									
<i>disable</i>	Disable central management.									
central-mgmt-auto-backup	Enable/disable central management auto backup.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auto backup.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable auto backup.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auto backup.	<i>disable</i>	Disable auto backup.			
Option	Description									
<i>enable</i>	Enable auto backup.									
<i>disable</i>	Disable auto backup.									
central-mgmt-schedule-config-restore	Enable/disable central management schedule config restore.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable central management scheduled restore.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable central management scheduled restore.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable central management scheduled restore.	<i>disable</i>	Disable central management scheduled restore.			
Option	Description									
<i>enable</i>	Enable central management scheduled restore.									
<i>disable</i>	Disable central management scheduled restore.									
central-mgmt-schedule-script-restore	Enable/disable central management schedule script restore.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable central management scheduled restore.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable central management scheduled restore.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable central management scheduled restore.	<i>disable</i>	Disable central management scheduled restore.			
Option	Description									
<i>enable</i>	Enable central management scheduled restore.									
<i>disable</i>	Disable central management scheduled restore.									

## config system fm

Configure FM.

```
config system fm
  Description: Configure FM.
  set status [enable|disable]
  set id {string}
  set ip {ipv4-address}
```

```

set vdom {string}
set auto-backup [enable|disable]
set scheduled-config-restore [enable|disable]
set ipsec [enable|disable]
end

```

## config system fm

Parameter	Description	Type	Size	Default						
status	Enable/disable FM.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FM.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FM.	<i>disable</i>	Disable FM.			
Option	Description									
<i>enable</i>	Enable FM.									
<i>disable</i>	Disable FM.									
id	ID.	string	Maximum length: 35							
ip	IP address.	ipv4-address	Not Specified	0.0.0.0						
vdom	VDOM.	string	Maximum length: 31	root						
auto-backup	Enable/disable automatic backup.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic backup.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic backup.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic backup.	<i>disable</i>	Disable automatic backup.			
Option	Description									
<i>enable</i>	Enable automatic backup.									
<i>disable</i>	Disable automatic backup.									
scheduled-config-restore	Enable/disable scheduled configuration restore.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable scheduled configuration restore.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable scheduled configuration restore.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable scheduled configuration restore.	<i>disable</i>	Disable scheduled configuration restore.			
Option	Description									
<i>enable</i>	Enable scheduled configuration restore.									
<i>disable</i>	Disable scheduled configuration restore.									
ipsec	Enable/disable IPsec.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec.	<i>disable</i>	Disable IPsec.			
Option	Description									
<i>enable</i>	Enable IPsec.									
<i>disable</i>	Disable IPsec.									

## config system central-management

Configure central management.

```

config system central-management
  Description: Configure central management.
  set mode [normal|backup]
  set type [fortimanager|fortiguard|...]
  set schedule-config-restore [enable|disable]
  set schedule-script-restore [enable|disable]
  set allow-push-configuration [enable|disable]
  set allow-push-firmware [enable|disable]
  set allow-remote-firmware-upgrade [enable|disable]
  set allow-monitor [enable|disable]
  set serial-number {user}
  set fmg {user}
  set fmg-source-ip {ipv4-address}
  set fmg-source-ip6 {ipv6-address}
  set local-cert {string}
  set ca-cert {user}
  set vdom {string}
config server-list
  Description: Additional servers that the FortiGate can use for updates (for AV, IPS,
  updates) and ratings (for web filter and antispam ratings) servers.
  edit <id>
    set server-type {option1}, {option2}, ...
    set addr-type [ipv4|ipv6|...]
    set server-address {ipv4-address}
    set server-address6 {ipv6-address}
    set fqdn {string}
  next
end
set fmg-update-port [8890|443]
set include-default-servers [enable|disable]
set enc-algorithm [default|high|...]
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config system central-management

Parameter	Description	Type	Size	Default						
mode	Central management mode.	option	-	normal						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>normal</i></td> <td>Manage and configure this FortiGate from FortiManager.</td> </tr> <tr> <td><i>backup</i></td> <td>Manage and configure this FortiGate locally and back up its configuration to FortiManager.</td> </tr> </tbody> </table>	Option	Description	<i>normal</i>	Manage and configure this FortiGate from FortiManager.	<i>backup</i>	Manage and configure this FortiGate locally and back up its configuration to FortiManager.			
Option	Description									
<i>normal</i>	Manage and configure this FortiGate from FortiManager.									
<i>backup</i>	Manage and configure this FortiGate locally and back up its configuration to FortiManager.									
type	Central management type.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortimanager</i></td> <td>FortiManager.</td> </tr> </tbody> </table>	Option	Description	<i>fortimanager</i>	FortiManager.					
Option	Description									
<i>fortimanager</i>	FortiManager.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard</i></td> <td>Central management of this FortiGate using FortiCloud.</td> </tr> <tr> <td><i>none</i></td> <td>No central management.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard</i>	Central management of this FortiGate using FortiCloud.	<i>none</i>	No central management.			
Option	Description									
<i>fortiguard</i>	Central management of this FortiGate using FortiCloud.									
<i>none</i>	No central management.									
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiGate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable scheduled configuration restore.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable scheduled configuration restore.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable scheduled configuration restore.	<i>disable</i>	Disable scheduled configuration restore.			
Option	Description									
<i>enable</i>	Enable scheduled configuration restore.									
<i>disable</i>	Disable scheduled configuration restore.									
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiGate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable scheduled script restore.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable scheduled script restore.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable scheduled script restore.	<i>disable</i>	Disable scheduled script restore.			
Option	Description									
<i>enable</i>	Enable scheduled script restore.									
<i>disable</i>	Disable scheduled script restore.									
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiGate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable push configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable push configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable push configuration.	<i>disable</i>	Disable push configuration.			
Option	Description									
<i>enable</i>	Enable push configuration.									
<i>disable</i>	Disable push configuration.									
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiGate.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable push firmware.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable push firmware.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable push firmware.	<i>disable</i>	Disable push firmware.			
Option	Description									
<i>enable</i>	Enable push firmware.									
<i>disable</i>	Disable push firmware.									
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiGate from the central management server.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable remote firmware upgrade.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable remote firmware upgrade.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable remote firmware upgrade.	<i>disable</i>	Disable remote firmware upgrade.			
Option	Description									
<i>enable</i>	Enable remote firmware upgrade.									
<i>disable</i>	Disable remote firmware upgrade.									

Parameter	Description	Type	Size	Default						
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiGate	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable remote monitoring of device.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable remote monitoring of device.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable remote monitoring of device.	<i>disable</i>	Disable remote monitoring of device.			
Option	Description									
<i>enable</i>	Enable remote monitoring of device.									
<i>disable</i>	Disable remote monitoring of device.									
serial-number	Serial number.	user	Not Specified							
fmg	IP address or FQDN of the FortiManager.	user	Not Specified							
fmg-source-ip	IPv4 source address that this FortiGate uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0						
fmg-source-ip6	IPv6 source address that this FortiGate uses when communicating with FortiManager.	ipv6-address	Not Specified	::						
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35							
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified							
vdom	Virtual domain (VDM) name to use when communicating with FortiManager.	string	Maximum length: 31	root						
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-	8890						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>8890</i></td> <td>Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.</td> </tr> <tr> <td><i>443</i></td> <td>Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.</td> </tr> </tbody> </table>	Option	Description	<i>8890</i>	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.	<i>443</i>	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.			
Option	Description									
<i>8890</i>	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.									
<i>443</i>	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.									
include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable inclusion of public FortiGuard servers in the override server list.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable inclusion of public FortiGuard servers in the override server list.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable inclusion of public FortiGuard servers in the override server list.	<i>disable</i>	Disable inclusion of public FortiGuard servers in the override server list.			
Option	Description									
<i>enable</i>	Enable inclusion of public FortiGuard servers in the override server list.									
<i>disable</i>	Disable inclusion of public FortiGuard servers in the override server list.									
enc-algorithm	Encryption strength for communications between the FortiGate and central management.	option	-	high						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>High strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD.</td> </tr> <tr> <td><i>high</i></td> <td>128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA.</td> </tr> <tr> <td><i>low</i></td> <td>64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CDBC-SHA, DES-CBC-SHA, DES-CBC-MD5.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	High strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD.	<i>high</i>	128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA.	<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CDBC-SHA, DES-CBC-SHA, DES-CBC-MD5.			
Option	Description											
<i>default</i>	High strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD.											
<i>high</i>	128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA.											
<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CDBC-SHA, DES-CBC-SHA, DES-CBC-MD5.											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

### config server-list

Parameter	Description	Type	Size	Default								
server-type	FortiGuard service type.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>update</i></td> <td>AV, IPS, and AV-query update server.</td> </tr> <tr> <td><i>rating</i></td> <td>Web filter and anti-spam rating server.</td> </tr> </tbody> </table>	Option	Description	<i>update</i>	AV, IPS, and AV-query update server.	<i>rating</i>	Web filter and anti-spam rating server.					
Option	Description											
<i>update</i>	AV, IPS, and AV-query update server.											
<i>rating</i>	Web filter and anti-spam rating server.											
addr-type	Indicate whether the FortiGate communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>IPv4 address.</td> </tr> <tr> <td><i>ipv6</i></td> <td>IPv6 address.</td> </tr> <tr> <td><i>fqdn</i></td> <td>FQDN.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	IPv4 address.	<i>ipv6</i>	IPv6 address.	<i>fqdn</i>	FQDN.			
Option	Description											
<i>ipv4</i>	IPv4 address.											
<i>ipv6</i>	IPv6 address.											
<i>fqdn</i>	FQDN.											
server-address	IPv4 address of override server.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default
server-address6	IPv6 address of override server.	ipv6-address	Not Specified	::
fqdn	FQDN address of override server.	string	Maximum length: 255	

## config system zone

Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.

```
config system zone
```

```
Description: Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.
```

```
edit <name>
```

```
config tagging
```

```
Description: Config object tagging.
```

```
edit <name>
```

```
set category {string}
```

```
set tags <name1>, <name2>, ...
```

```
next
```

```
end
```

```
set description {string}
```

```
set intrazone [allow|deny]
```

```
set interface <interface-name1>, <interface-name2>, ...
```

```
next
```

```
end
```

## config system zone

Parameter	Description	Type	Size	Default						
description	Description.	string	Maximum length: 127							
intrazone	Allow or deny traffic routing between different interfaces in the same zone .	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow traffic between interfaces in the zone.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny traffic between interfaces in the zone.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow traffic between interfaces in the zone.	<i>deny</i>	Deny traffic between interfaces in the zone.			
Option	Description									
<i>allow</i>	Allow traffic between interfaces in the zone.									
<i>deny</i>	Deny traffic between interfaces in the zone.									
interface <interface-name>	Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined. Select interfaces to add to the zone.	string	Maximum length: 79							

## config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config system geoip-country

Define geoip country name-ID table.

```
config system geoip-country
  Description: Define geoip country name-ID table.
  edit <id>
    set name {string}
  next
end
```

## config system geoip-country

Parameter	Description	Type	Size	Default
name	Country name.	string	Maximum length: 63	

## config system sdn-connector

Configure connection to SDN Connector.

```
config system sdn-connector
  Description: Configure connection to SDN Connector.
  edit <name>
    set status [disable|enable]
    set type [aci|alicloud|...]
    set use-metadata-iam [disable|enable]
    set ha-status [disable|enable]
    set verify-certificate [disable|enable]
    set server {string}
    set server-list <ip1>, <ip2>, ...
    set server-port {integer}
    set username {string}
    set password {password_aes256}
    set vcenter-server {string}
    set vcenter-username {string}
    set vcenter-password {password_aes256}
    set access-key {string}
    set secret-key {password}
    set region {string}
    set vpc-id {string}
```



```

set tenant-id {string}
set client-id {string}
set client-secret {password}
set subscription-id {string}
set resource-group {string}
set login-endpoint {string}
set resource-url {string}
set azure-region [global|china|...]
config nic
    Description: Configure Azure network interface.
    edit <name>
        config ip
            Description: Configure IP configuration.
            edit <name>
                set public-ip {string}
                set resource-group {string}
            next
        end
    next
end
config route-table
    Description: Configure Azure route table.
    edit <name>
        set subscription-id {string}
        set resource-group {string}
        config route
            Description: Configure Azure route.
            edit <name>
                set next-hop {string}
            next
        end
    next
end
set user-id {string}
set compartment-id {string}
set oci-region {string}
set oci-region-type [commercial|government]
set oci-cert {string}
set oci-fingerprint {string}
config external-ip
    Description: Configure GCP external IP.
    edit <name>
        next
end
config route
    Description: Configure GCP route.
    edit <name>
        next
end
config gcp-project-list
    Description: Configure GCP project list.
    edit <id>
        set gcp-zone-list <name1>, <name2>, ...
    next
end
set service-account {string}
set private-key {user}

```

```

set secret-token {user}
set domain {string}
set group-name {string}
set api-key {password}
set compute-generation {integer}
set ibm-region [us-south|us-east|...]
set update-interval {integer}
next
end

```

## config system sdn-connector

Parameter	Description	Type	Size	Default																														
status	Enable/disable connection to the remote SDN connector.	option	-	enable																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable connection to this SDN Connector.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable connection to this SDN Connector.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable connection to this SDN Connector.	<i>enable</i>	Enable connection to this SDN Connector.																											
Option	Description																																	
<i>disable</i>	Disable connection to this SDN Connector.																																	
<i>enable</i>	Enable connection to this SDN Connector.																																	
type	Type of SDN connector.	option	-	aws																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aci</i></td> <td>Application Centric Infrastructure (ACI).</td> </tr> <tr> <td><i>alicloud</i></td> <td>AliCloud Service (ACS).</td> </tr> <tr> <td><i>aws</i></td> <td>Amazon Web Services (AWS).</td> </tr> <tr> <td><i>azure</i></td> <td>Microsoft Azure.</td> </tr> <tr> <td><i>gcp</i></td> <td>Google Cloud Platform (GCP).</td> </tr> <tr> <td><i>nsx</i></td> <td>VMware NSX.</td> </tr> <tr> <td><i>nuage</i></td> <td>Nuage VSP.</td> </tr> <tr> <td><i>oci</i></td> <td>Oracle Cloud Infrastructure.</td> </tr> <tr> <td><i>openstack</i></td> <td>OpenStack.</td> </tr> <tr> <td><i>kubernetes</i></td> <td>Kubernetes.</td> </tr> <tr> <td><i>vmware</i></td> <td>VMware vSphere (vCenter &amp; ESXi).</td> </tr> <tr> <td><i>sepm</i></td> <td>Symantec Endpoint Protection Manager.</td> </tr> <tr> <td><i>aci-direct</i></td> <td>Application Centric Infrastructure (ACI Direct Connection).</td> </tr> <tr> <td><i>ibm</i></td> <td>IBM Cloud Infrastructure.</td> </tr> </tbody> </table>	Option	Description	<i>aci</i>	Application Centric Infrastructure (ACI).	<i>alicloud</i>	AliCloud Service (ACS).	<i>aws</i>	Amazon Web Services (AWS).	<i>azure</i>	Microsoft Azure.	<i>gcp</i>	Google Cloud Platform (GCP).	<i>nsx</i>	VMware NSX.	<i>nuage</i>	Nuage VSP.	<i>oci</i>	Oracle Cloud Infrastructure.	<i>openstack</i>	OpenStack.	<i>kubernetes</i>	Kubernetes.	<i>vmware</i>	VMware vSphere (vCenter & ESXi).	<i>sepm</i>	Symantec Endpoint Protection Manager.	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).	<i>ibm</i>	IBM Cloud Infrastructure.			
Option	Description																																	
<i>aci</i>	Application Centric Infrastructure (ACI).																																	
<i>alicloud</i>	AliCloud Service (ACS).																																	
<i>aws</i>	Amazon Web Services (AWS).																																	
<i>azure</i>	Microsoft Azure.																																	
<i>gcp</i>	Google Cloud Platform (GCP).																																	
<i>nsx</i>	VMware NSX.																																	
<i>nuage</i>	Nuage VSP.																																	
<i>oci</i>	Oracle Cloud Infrastructure.																																	
<i>openstack</i>	OpenStack.																																	
<i>kubernetes</i>	Kubernetes.																																	
<i>vmware</i>	VMware vSphere (vCenter & ESXi).																																	
<i>sepm</i>	Symantec Endpoint Protection Manager.																																	
<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).																																	
<i>ibm</i>	IBM Cloud Infrastructure.																																	
use-metadata-iam	Enable/disable use of IAM role from metadata to call API.	option	-	disable																														

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable using IAM role to call API.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable using IAM role to call API.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable using IAM role to call API.	<i>enable</i>	Enable using IAM role to call API.			
Option	Description									
<i>disable</i>	Disable using IAM role to call API.									
<i>enable</i>	Enable using IAM role to call API.									
ha-status	Enable/disable use for FortiGate HA service.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use for FortiGate HA service.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use for FortiGate HA service.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use for FortiGate HA service.	<i>enable</i>	Enable use for FortiGate HA service.			
Option	Description									
<i>disable</i>	Disable use for FortiGate HA service.									
<i>enable</i>	Enable use for FortiGate HA service.									
verify-certificate	Enable/disable server certificate verification.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable server certificate verification.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable server certificate verification.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable server certificate verification.	<i>enable</i>	Enable server certificate verification.			
Option	Description									
<i>disable</i>	Disable server certificate verification.									
<i>enable</i>	Enable server certificate verification.									
server	Server address of the remote SDN connector.	string	Maximum length: 127							
server-list <ip>	Server address list of the remote SDN connector. IPv4 address.	string	Maximum length: 15							
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535	0						
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64							
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified							
vcenter-server	vCenter server address for NSX quarantine.	string	Maximum length: 127							
vcenter-username	vCenter server username for NSX quarantine.	string	Maximum length: 64							
vcenter-password	vCenter server password for NSX quarantine.	password_aes256	Not Specified							
access-key	AWS / ACS access key ID.	string	Maximum length: 31							

Parameter	Description	Type	Size	Default												
secret-key	AWS / ACS secret access key.	password	Not Specified													
region	AWS / ACS region name.	string	Maximum length: 31													
vpc-id	AWS VPC ID.	string	Maximum length: 31													
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127													
client-id	Azure client ID (application ID).	string	Maximum length: 63													
client-secret	Azure client secret (application key).	password	Not Specified													
subscription-id	Azure subscription ID.	string	Maximum length: 63													
resource-group	Azure resource group.	string	Maximum length: 63													
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127													
resource-url	Azure Stack resource URL.	string	Maximum length: 127													
azure-region	Azure server region.	option	-	global												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Global Azure Server.</td> </tr> <tr> <td><i>china</i></td> <td>China Azure Server.</td> </tr> <tr> <td><i>germany</i></td> <td>Germany Azure Server.</td> </tr> <tr> <td><i>usgov</i></td> <td>US Government Azure Server.</td> </tr> <tr> <td><i>local</i></td> <td>Azure Stack Local Server.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Global Azure Server.	<i>china</i>	China Azure Server.	<i>germany</i>	Germany Azure Server.	<i>usgov</i>	US Government Azure Server.	<i>local</i>	Azure Stack Local Server.			
Option	Description															
<i>global</i>	Global Azure Server.															
<i>china</i>	China Azure Server.															
<i>germany</i>	Germany Azure Server.															
<i>usgov</i>	US Government Azure Server.															
<i>local</i>	Azure Stack Local Server.															
user-id	User ID.	string	Maximum length: 127													
compartment-id	Compartment ID.	string	Maximum length: 127													
oci-region	OCI server region.	string	Maximum length: 31													
oci-region-type	OCI region type.	option	-	commercial												

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>commercial</i></td> <td>Commercial region.</td> </tr> <tr> <td><i>government</i></td> <td>Government region.</td> </tr> </tbody> </table>	Option	Description	<i>commercial</i>	Commercial region.	<i>government</i>	Government region.											
Option	Description																	
<i>commercial</i>	Commercial region.																	
<i>government</i>	Government region.																	
oci-cert	OCI certificate.	string	Maximum length: 63															
oci-fingerprint	OCI pubkey fingerprint.	string	Maximum length: 63															
service-account	GCP service account email.	string	Maximum length: 127															
private-key	Private key of GCP service account.	user	Not Specified															
secret-token	Secret token of Kubernetes service account.	user	Not Specified															
domain	Domain name.	string	Maximum length: 127															
group-name	Group name of computers.	string	Maximum length: 127															
api-key	IBM cloud API key or service ID API key.	password	Not Specified															
compute-generation	Compute generation for IBM cloud infrastructure.	integer	Minimum value: 1 Maximum value: 2	2														
ibm-region	IBM cloud region name.	option	-	us-south														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>us-south</i></td> <td>US South (Dallas) Server.</td> </tr> <tr> <td><i>us-east</i></td> <td>US East (Washington DC) Server.</td> </tr> <tr> <td><i>germany</i></td> <td>Germany (Frankfurt) Server.</td> </tr> <tr> <td><i>great-britain</i></td> <td>Great Britain (London) Server.</td> </tr> <tr> <td><i>japan</i></td> <td>Japan (Tokyo) Server. (GEN1 support only)</td> </tr> <tr> <td><i>australia</i></td> <td>Australia (Sydney) Server. (GEN1 support only)</td> </tr> </tbody> </table>	Option	Description	<i>us-south</i>	US South (Dallas) Server.	<i>us-east</i>	US East (Washington DC) Server.	<i>germany</i>	Germany (Frankfurt) Server.	<i>great-britain</i>	Great Britain (London) Server.	<i>japan</i>	Japan (Tokyo) Server. (GEN1 support only)	<i>australia</i>	Australia (Sydney) Server. (GEN1 support only)			
Option	Description																	
<i>us-south</i>	US South (Dallas) Server.																	
<i>us-east</i>	US East (Washington DC) Server.																	
<i>germany</i>	Germany (Frankfurt) Server.																	
<i>great-britain</i>	Great Britain (London) Server.																	
<i>japan</i>	Japan (Tokyo) Server. (GEN1 support only)																	
<i>australia</i>	Australia (Sydney) Server. (GEN1 support only)																	
update-interval	Dynamic object update interval .	integer	Minimum value: 0 Maximum value: 3600	60														

## config ip

Parameter	Description	Type	Size	Default
public-ip	Public IP name.	string	Maximum length: 63	
resource-group	Resource group of Azure public IP.	string	Maximum length: 63	

## config route-table

Parameter	Description	Type	Size	Default
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63	
resource-group	Resource group of Azure route table.	string	Maximum length: 63	

## config route

Parameter	Description	Type	Size	Default
next-hop	Next hop address.	string	Maximum length: 127	

## config route

Parameter	Description	Type	Size	Default
next-hop	Next hop address.	string	Maximum length: 127	

## config gcp-project-list

Parameter	Description	Type	Size	Default
gcp-zone-list <name>	Configure GCP zone list. GCP zone name.	string	Maximum length: 127	

## config system ipv6-tunnel

Configure IPv6/IPv4 in IPv6 tunnel.

```
config system ipv6-tunnel
  Description: Configure IPv6/IPv4 in IPv6 tunnel.
  edit <name>
    set source {ipv6-address}
    set destination {ipv6-address}
    set interface {string}
```

```

    set auto-asic-offload [enable|disable]
  next
end

```

## config system ipv6-tunnel

Parameter	Description	Type	Size	Default
source	Local IPv6 address of the tunnel.	ipv6-address	Not Specified	::
destination	Remote IPv6 address of the tunnel.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable

Option	Description
<i>enable</i>	Enable auto ASIC offloading.
<i>disable</i>	Disable ASIC offloading.

\* This parameter may not exist in some models.

## config system external-resource

Configure external resource.

```

config system external-resource
  Description: Configure external resource.
  edit <name>
    set status [enable|disable]
    set type [category|address|...]
    set category {integer}
    set username {string}
    set password {password}
    set comments {var-string}
    set resource {string}
    set user-agent {string}
    set refresh-rate {integer}
    set source-ip {ipv4-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
  next
end

```

## config system external-resource

Parameter	Description	Type	Size	Default										
status	Enable/disable user resource.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable user resource.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable user resource.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable user resource.	<i>disable</i>	Disable user resource.							
Option	Description													
<i>enable</i>	Enable user resource.													
<i>disable</i>	Disable user resource.													
type	User resource type.	option	-	category										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>category</i></td> <td>FortiGuard category.</td> </tr> <tr> <td><i>address</i></td> <td>Firewall IP address.</td> </tr> <tr> <td><i>domain</i></td> <td>Domain Name.</td> </tr> <tr> <td><i>malware</i></td> <td>Malware hash.</td> </tr> </tbody> </table>	Option	Description	<i>category</i>	FortiGuard category.	<i>address</i>	Firewall IP address.	<i>domain</i>	Domain Name.	<i>malware</i>	Malware hash.			
Option	Description													
<i>category</i>	FortiGuard category.													
<i>address</i>	Firewall IP address.													
<i>domain</i>	Domain Name.													
<i>malware</i>	Malware hash.													
category	User resource category.	integer	Minimum value: 192 Maximum value: 221	0										
username	HTTP basic authentication user name.	string	Maximum length: 64											
password	HTTP basic authentication password.	password	Not Specified											
comments	Comment.	var-string	Maximum length: 255											
resource	URI of external resource.	string	Maximum length: 511											
user-agent	HTTP User-Agent header .	string	Maximum length: 127	curl/7.58.0										
refresh-rate	Time interval to refresh external resource .	integer	Minimum value: 1 Maximum value: 43200	5										
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system ips-urlfilter-dns

Configure IPS URL filter DNS servers.

```
config system ips-urlfilter-dns
  Description: Configure IPS URL filter DNS servers.
  edit <address>
    set status [enable|disable]
    set ipv6-capability [enable|disable]
  next
end
```

## config system ips-urlfilter-dns

Parameter	Description	Type	Size	Default						
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this DNS server for IPS URL filter DNS queries.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this DNS server for IPS URL filter DNS queries.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this DNS server for IPS URL filter DNS queries.	<i>disable</i>	Disable this DNS server for IPS URL filter DNS queries.			
Option	Description									
<i>enable</i>	Enable this DNS server for IPS URL filter DNS queries.									
<i>disable</i>	Disable this DNS server for IPS URL filter DNS queries.									
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

## config system ips-urlfilter-dns6

Configure IPS URL filter IPv6 DNS servers.

```
config system ips-urlfilter-dns6
```

```

Description: Configure IPS URL filter IPv6 DNS servers.
edit <address6>
    set status [enable|disable]
next
end

```

## config system ips-urlfilter-dns6

Parameter	Description	Type	Size	Default						
status	Enable/disable this server for IPv6 DNS queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

## config system network-visibility

Configure network visibility settings.

```

config system network-visibility
Description: Configure network visibility settings.
set destination-visibility [disable|enable]
set source-location [disable|enable]
set destination-hostname-visibility [disable|enable]
set hostname-ttl {integer}
set hostname-limit {integer}
set destination-location [disable|enable]
end

```

## config system network-visibility

Parameter	Description	Type	Size	Default						
destination-visibility	Enable/disable logging of destination visibility.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of destination visibility.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of destination visibility.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of destination visibility.	<i>enable</i>	Enable logging of destination visibility.			
Option	Description									
<i>disable</i>	Disable logging of destination visibility.									
<i>enable</i>	Enable logging of destination visibility.									
source-location	Enable/disable logging of source geographical location visibility.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of source geographical location visibility.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of source geographical location visibility.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of source geographical location visibility.	<i>enable</i>	Enable logging of source geographical location visibility.			
Option	Description									
<i>disable</i>	Disable logging of source geographical location visibility.									
<i>enable</i>	Enable logging of source geographical location visibility.									
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of destination hostname visibility.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of destination hostname visibility.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of destination hostname visibility.	<i>enable</i>	Enable logging of destination hostname visibility.			
Option	Description									
<i>disable</i>	Disable logging of destination hostname visibility.									
<i>enable</i>	Enable logging of destination hostname visibility.									
hostname-ttl	TTL of hostname table entries .	integer	Minimum value: 60 Maximum value: 86400	86400						
hostname-limit	Limit of the number of hostname table entries .	integer	Minimum value: 0 Maximum value: 50000	5000						
destination-location	Enable/disable logging of destination geographical location visibility.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable logging of destination geographical location visibility.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable logging of destination geographical location visibility.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable logging of destination geographical location visibility.	<i>enable</i>	Enable logging of destination geographical location visibility.			
Option	Description									
<i>disable</i>	Disable logging of destination geographical location visibility.									
<i>enable</i>	Enable logging of destination geographical location visibility.									

## config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set interface {string}
    set ip-version [4|6]
    set remote-gw6 {ipv6-address}
    set local-gw6 {ipv6-address}
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address-any}
    set sequence-number-transmission [disable|enable]
    set sequence-number-reception [disable|enable]
    set checksum-transmission [disable|enable]
```

```

set checksum-reception [disable|enable]
set key-outbound {integer}
set key-inbound {integer}
set dscp-copying [disable|enable]
set diffservcode {user}
set keepalive-interval {integer}
set keepalive-failtimes {integer}
next
end

```

## config system gre-tunnel

Parameter	Description	Type	Size	Default						
interface	Interface name.	string	Maximum length: 15							
ip-version	IP version to use for VPN interface.	option	-	4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Use IPv4 addressing for gateways.</td> </tr> <tr> <td>6</td> <td>Use IPv6 addressing for gateways.</td> </tr> </tbody> </table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.			
Option	Description									
4	Use IPv4 addressing for gateways.									
6	Use IPv6 addressing for gateways.									
remote-gw6	IPv6 address of the remote gateway.	ipv6-address	Not Specified	::						
local-gw6	IPv6 address of the local gateway.	ipv6-address	Not Specified	::						
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified	0.0.0.0						
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified	0.0.0.0						
sequence-number-transmission *	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Include sequence numbers in transmitted GRE packets.</td> </tr> <tr> <td><i>enable</i></td> <td>Do not include sequence numbers in transmitted GRE packets.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Include sequence numbers in transmitted GRE packets.	<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.			
Option	Description									
<i>disable</i>	Include sequence numbers in transmitted GRE packets.									
<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.									
sequence-number-reception *	Enable/disable validating sequence numbers in received GRE packets.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not validate sequence number in received GRE packets.</td> </tr> <tr> <td><i>enable</i></td> <td>Validate sequence numbers in received GRE packets.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not validate sequence number in received GRE packets.	<i>enable</i>	Validate sequence numbers in received GRE packets.			
Option	Description									
<i>disable</i>	Do not validate sequence number in received GRE packets.									
<i>enable</i>	Validate sequence numbers in received GRE packets.									
checksum-transmission *	Enable/disable including checksums in transmitted GRE packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not include checksums in transmitted GRE packets.</td> </tr> <tr> <td><i>enable</i></td> <td>Include checksums in transmitted GRE packets.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not include checksums in transmitted GRE packets.	<i>enable</i>	Include checksums in transmitted GRE packets.			
Option	Description									
<i>disable</i>	Do not include checksums in transmitted GRE packets.									
<i>enable</i>	Include checksums in transmitted GRE packets.									
checksum-reception *	Enable/disable validating checksums in received GRE packets.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not validate checksums in received GRE packets.</td> </tr> <tr> <td><i>enable</i></td> <td>Validate checksums in received GRE packets.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not validate checksums in received GRE packets.	<i>enable</i>	Validate checksums in received GRE packets.			
Option	Description									
<i>disable</i>	Do not validate checksums in received GRE packets.									
<i>enable</i>	Validate checksums in received GRE packets.									
key-outbound *	Include this key in transmitted GRE packets .	integer	Minimum value: 0 Maximum value: 4294967295	0						
key-inbound *	Require received GRE packets contain this key .	integer	Minimum value: 0 Maximum value: 4294967295	0						
dscp-copying	Enable/disable DSCP copying.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable DSCP copying.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable DSCP copying.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable DSCP copying.	<i>enable</i>	Enable DSCP copying.			
Option	Description									
<i>disable</i>	Disable DSCP copying.									
<i>enable</i>	Enable DSCP copying.									
diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified							
keepalive-interval	Keepalive message interval .	integer	Minimum value: 0 Maximum value: 32767	0						

Parameter	Description	Type	Size	Default
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down .	integer	Minimum value: 1 Maximum value: 255	10

\* This parameter may not exist in some models.

## config system ipsec-aggregate

Configure an aggregate of IPsec tunnels.

```
config system ipsec-aggregate
  Description: Configure an aggregate of IPsec tunnels.
  edit <name>
    set member <tunnel-name1>, <tunnel-name2>, ...
    set algorithm [L3|L4|...]
  next
end
```

## config system ipsec-aggregate

Parameter	Description	Type	Size	Default
member <tunnel-name>	Member tunnels of the aggregate. Tunnel name.	string	Maximum length: 79	
algorithm	Frame distribution algorithm.	option	-	round-robin

Option	Description
<i>L3</i>	Use layer 3 address for distribution.
<i>L4</i>	Use layer 4 information for distribution.
<i>round-robin</i>	Per-packet round-robin distribution.
<i>redundant</i>	Use first tunnel that is up for all traffic.
<i>weighted-round-robin</i>	Weighted round-robin distribution.

## config system ipip-tunnel

Configure IP in IP Tunneling.

```
config system ipip-tunnel
  Description: Configure IP in IP Tunneling.
  edit <name>
    set interface {string}
    set remote-gw {ipv4-address}
```

```

    set local-gw {ipv4-address-any}
    set auto-asic-offload [enable|disable]
  next
end

```

## config system ipip-tunnel

Parameter	Description	Type	Size	Default
interface	Interface name that is associated with the incoming traffic from available options.	string	Maximum length: 15	
remote-gw	IPv4 address for the remote gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	IPv4 address for the local gateway.	ipv4-address-any	Not Specified	0.0.0.0
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable

Option	Description
<i>enable</i>	Enable auto ASIC offloading.
<i>disable</i>	Disable ASIC offloading.

\* This parameter may not exist in some models.

## config system mobile-tunnel

Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.

```

config system mobile-tunnel
  Description: Configure Mobile tunnels, an implementation of Network Mobility (NEMO)
              extensions for Mobile IPv4 RFC5177.
  edit <name>
    set status [disable|enable]
    set roaming-interface {string}
    set home-agent {ipv4-address}
    set home-address {ipv4-address}
    set renew-interval {integer}
    set lifetime {integer}
    set reg-interval {integer}
    set reg-retry {integer}
    set n-mhae-spi {integer}
    set n-mhae-key-type [ascii|base64]
    set n-mhae-key {user}
    set hash-algorithm {option}
    set tunnel-mode {option}
  config network
    Description: NEMO network configuration.
    edit <id>
      set interface {string}

```

```

        set prefix {ipv4-classnet}
    next
end
next
end

```

## config system mobile-tunnel

Parameter	Description	Type	Size	Default						
status	Enable/disable this mobile tunnel.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this mobile tunnel.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this mobile tunnel.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this mobile tunnel.	<i>enable</i>	Enable this mobile tunnel.			
Option	Description									
<i>disable</i>	Disable this mobile tunnel.									
<i>enable</i>	Enable this mobile tunnel.									
roaming-interface	Select the associated interface name from available options.	string	Maximum length: 15							
home-agent	IPv4 address of the NEMO HA (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0						
home-address	Home IP address (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0						
renew-interval	Time before lifetime expiration to send NEMO HA re-registration .	integer	Minimum value: 5 Maximum value: 60	60						
lifetime	NEMO HA registration request lifetime .	integer	Minimum value: 180 Maximum value: 65535	65535						
reg-interval	NEMO HA registration interval .	integer	Minimum value: 5 Maximum value: 300	5						
reg-retry	Maximum number of NEMO HA registration retries .	integer	Minimum value: 1 Maximum value: 30	3						
n-mhae-spi	NEMO authentication SPI .	integer	Minimum value: 0 Maximum value: 4294967295	256						



Parameter	Description	Type	Size	Default						
n-mhae-key-type	NEMO authentication key type (ascii or base64).	option	-	ascii						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ascii</i></td> <td>The authentication key is an ASCII string.</td> </tr> <tr> <td><i>base64</i></td> <td>The authentication key is Base64 encoded.</td> </tr> </tbody> </table>	Option	Description	<i>ascii</i>	The authentication key is an ASCII string.	<i>base64</i>	The authentication key is Base64 encoded.			
Option	Description									
<i>ascii</i>	The authentication key is an ASCII string.									
<i>base64</i>	The authentication key is Base64 encoded.									
n-mhae-key	NEMO authentication key.	user	Not Specified							
hash-algorithm	Hash Algorithm (Keyed MD5).	option	-	hmac-md5						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hmac-md5</i></td> <td>Keyed MD5.</td> </tr> </tbody> </table>	Option	Description	<i>hmac-md5</i>	Keyed MD5.					
Option	Description									
<i>hmac-md5</i>	Keyed MD5.									
tunnel-mode	NEMO tunnel mode (GRE tunnel).	option	-	gre						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>gre</i></td> <td>GRE tunnel.</td> </tr> </tbody> </table>	Option	Description	<i>gre</i>	GRE tunnel.					
Option	Description									
<i>gre</i>	GRE tunnel.									

## config network

Parameter	Description	Type	Size	Default
interface	Select the associated interface name from available options.	string	Maximum length: 15	
prefix	Class IP and Netmask with correction (Format:xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/x).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config system pppoe-interface

Configure the PPPoE interfaces.

```

config system pppoe-interface
  Description: Configure the PPPoE interfaces.
  edit <name>
    set dial-on-demand [enable|disable]
    set ipv6 [enable|disable]
    set device {string}
    set username {string}
    set password {password}
    set auth-type [auto|pap|...]
    set ipunnumbered {ipv4-address}
    set pppoe-unnumbered-negotiate [enable|disable]
    set idle-timeout {integer}
    set disc-retry-timeout {integer}
  
```

```

set padt-retry-timeout {integer}
set service-name {string}
set ac-name {string}
set lcp-echo-interval {integer}
set lcp-max-echo-fails {integer}
next
end

```

## config system pppoe-interface

Parameter	Description	Type	Size	Default												
dial-on-demand	Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE interface.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dial on demand.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dial on demand.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dial on demand.	<i>disable</i>	Disable dial on demand.									
Option	Description															
<i>enable</i>	Enable dial on demand.															
<i>disable</i>	Disable dial on demand.															
ipv6	Enable/disable IPv6 Control Protocol (IPv6CP).	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPv6CP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPv6CP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPv6CP.	<i>disable</i>	Disable IPv6CP.									
Option	Description															
<i>enable</i>	Enable IPv6CP.															
<i>disable</i>	Disable IPv6CP.															
device	Name for the physical interface.	string	Maximum length: 15													
username	User name.	string	Maximum length: 64													
password	Enter the password.	password	Not Specified													
auth-type	PPP authentication type to use.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically choose the authentication method.</td> </tr> <tr> <td><i>pap</i></td> <td>PAP authentication.</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP authentication.</td> </tr> <tr> <td><i>mschapv1</i></td> <td>MS-CHAPv1 authentication.</td> </tr> <tr> <td><i>mschapv2</i></td> <td>MS-CHAPv2 authentication.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically choose the authentication method.	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.			
Option	Description															
<i>auto</i>	Automatically choose the authentication method.															
<i>pap</i>	PAP authentication.															
<i>chap</i>	CHAP authentication.															
<i>mschapv1</i>	MS-CHAPv1 authentication.															
<i>mschapv2</i>	MS-CHAPv2 authentication.															
ipunnumbered	PPPoE unnumbered IP.	ipv4-address	Not Specified	0.0.0.0												

Parameter	Description	Type	Size	Default						
pppoe- unnumbered- negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PPPoE unnumbered negotiation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PPPoE unnumbered negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PPPoE unnumbered negotiation.	<i>disable</i>	Disable PPPoE unnumbered negotiation.			
Option	Description									
<i>enable</i>	Enable PPPoE unnumbered negotiation.									
<i>disable</i>	Disable PPPoE unnumbered negotiation.									
idle-timeout	PPPoE auto disconnect after idle timeout .	integer	Minimum value: 0 Maximum value: 4294967295	0						
disc-retry- timeout	PPPoE discovery init timeout value in .	integer	Minimum value: 0 Maximum value: 4294967295	1						
padt-retry- timeout	PPPoE terminate timeout value in .	integer	Minimum value: 0 Maximum value: 4294967295	1						
service-name	PPPoE service name.	string	Maximum length: 63							
ac-name	PPPoE AC name.	string	Maximum length: 63							
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5						
lcp-max-echo- fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3						

## config system vxlan

Configure VXLAN devices.

```
config system vxlan
  Description: Configure VXLAN devices.
  edit <name>
    set interface {string}
```

```

set vni {integer}
set ip-version [ipv4-unicast|ipv6-unicast|...]
set remote-ip <ip1>, <ip2>, ...
set remote-ip6 <ip61>, <ip62>, ...
set dstport {integer}
set multicast-ttl {integer}
next
end

```

## config system vxlan

Parameter	Description	Type	Size	Default										
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15											
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215	0										
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast or multicast.	option	-	ipv4-unicast										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4-unicast</i></td> <td>Use IPv4 unicast addressing over the VXLAN.</td> </tr> <tr> <td><i>ipv6-unicast</i></td> <td>Use IPv6 unicast addressing over the VXLAN.</td> </tr> <tr> <td><i>ipv4-multicast</i></td> <td>Use IPv4 multicast addressing over the VXLAN.</td> </tr> <tr> <td><i>ipv6-multicast</i></td> <td>Use IPv6 multicast addressing over the VXLAN.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the VXLAN.	<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the VXLAN.	<i>ipv4-multicast</i>	Use IPv4 multicast addressing over the VXLAN.	<i>ipv6-multicast</i>	Use IPv6 multicast addressing over the VXLAN.			
Option	Description													
<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the VXLAN.													
<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the VXLAN.													
<i>ipv4-multicast</i>	Use IPv4 multicast addressing over the VXLAN.													
<i>ipv6-multicast</i>	Use IPv6 multicast addressing over the VXLAN.													
remote-ip <ip>	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN. IPv4 address.	string	Maximum length: 15											
remote-ip6 <ip6>	IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN. IPv6 address.	string	Maximum length: 45											
dstport	VXLAN destination port .	integer	Minimum value: 1 Maximum value: 65535	4789										
multicast-ttl	VXLAN multicast TTL .	integer	Minimum value: 1 Maximum value: 255	0										

## config system geneve

Configure GENEVE devices.

```
config system geneve
  Description: Configure GENEVE devices.
  edit <name>
    set interface {string}
    set vni {integer}
    set type [ethernet|ppp]
    set ip-version [ipv4-unicast|ipv6-unicast]
    set remote-ip {ipv4-address}
    set remote-ip6 {ipv6-address}
    set dstport {integer}
  next
end
```

## config system geneve

Parameter	Description	Type	Size	Default						
interface	Outgoing interface for GENEVE encapsulated traffic.	string	Maximum length: 15							
vni	GENEVE network ID.	integer	Minimum value: 0 Maximum value: 16777215	0						
type	GENEVE type.	option	-	ethernet						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ethernet</i></td><td>Internal packet includes Ethernet header.</td></tr><tr><td><i>ppp</i></td><td>Internal packet does not include Ethernet header.</td></tr></tbody></table>	Option	Description	<i>ethernet</i>	Internal packet includes Ethernet header.	<i>ppp</i>	Internal packet does not include Ethernet header.			
Option	Description									
<i>ethernet</i>	Internal packet includes Ethernet header.									
<i>ppp</i>	Internal packet does not include Ethernet header.									
ip-version	IP version to use for the GENEVE interface and so for communication over the GENEVE. IPv4 or IPv6 unicast.	option	-	ipv4-unicast						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ipv4-unicast</i></td><td>Use IPv4 unicast addressing over the GENEVE.</td></tr><tr><td><i>ipv6-unicast</i></td><td>Use IPv6 unicast addressing over the GENEVE.</td></tr></tbody></table>	Option	Description	<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the GENEVE.	<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the GENEVE.			
Option	Description									
<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the GENEVE.									
<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the GENEVE.									
remote-ip	IPv4 address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv4-address	Not Specified	0.0.0.0						
remote-ip6	IPv6 IP address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv6-address	Not Specified	::						

Parameter	Description	Type	Size	Default
dstport	GENEVE destination port .	integer	Minimum value: 1 Maximum value: 65535	6081

## config system virtual-wire-pair

Configure virtual wire pairs.

```
config system virtual-wire-pair
  Description: Configure virtual wire pairs.
  edit <name>
    set member <interface-name1>, <interface-name2>, ...
    set wildcard-vlan [enable|disable]
    set vlan-filter {user}
  next
end
```

## config system virtual-wire-pair

Parameter	Description	Type	Size	Default						
member <interface-name>	Interfaces belong to the virtual-wire-pair. Interface name.	string	Maximum length: 79							
wildcard-vlan	Enable/disable wildcard VLAN.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable wildcard VLAN.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable wildcard VLAN.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable wildcard VLAN.	<i>disable</i>	Disable wildcard VLAN.			
Option	Description									
<i>enable</i>	Enable wildcard VLAN.									
<i>disable</i>	Disable wildcard VLAN.									
vlan-filter	Set VLAN filters.	user	Not Specified							

## config system dns-database

Configure DNS databases.

```
config system dns-database
  Description: Configure DNS databases.
  edit <name>
    set status [enable|disable]
    set domain {string}
    set allow-transfer {user}
    set type [master|slave]
    set view [shadow|public]
```

```

set ip-master {ipv4-address-any}
set primary-name {string}
set contact {string}
set ttl {integer}
set authoritative [enable|disable]
set forwarder {user}
set source-ip {ipv4-address}
set rr-max {integer}
config dns-entry
  Description: DNS entry.
  edit <id>
    set status [enable|disable]
    set type [A|NS|...]
    set ttl {integer}
    set preference {integer}
    set ip {ipv4-address-any}
    set ipv6 {ipv6-address}
    set hostname {string}
    set canonical-name {string}
  next
end
next
end

```

## config system dns-database

Parameter	Description	Type	Size	Default						
status	Enable/disable this DNS zone.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
domain	Domain name.	string	Maximum length: 255							
allow-transfer	DNS zone transfer IP address list.	user	Not Specified							
type	Zone type (master to manage entries directly, slave to import entries from other zones).	option	-	master						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>master</i></td> <td>Master DNS zone, to manage entries directly.</td> </tr> <tr> <td><i>slave</i></td> <td>Slave DNS zone, to import entries from other DNS zones.</td> </tr> </tbody> </table>	Option	Description	<i>master</i>	Master DNS zone, to manage entries directly.	<i>slave</i>	Slave DNS zone, to import entries from other DNS zones.			
Option	Description									
<i>master</i>	Master DNS zone, to manage entries directly.									
<i>slave</i>	Slave DNS zone, to import entries from other DNS zones.									
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-	shadow						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>shadow</i></td> <td>Shadow DNS zone to serve internal clients.</td> </tr> <tr> <td><i>public</i></td> <td>Public DNS zone to serve public clients.</td> </tr> </tbody> </table>	Option	Description	<i>shadow</i>	Shadow DNS zone to serve internal clients.	<i>public</i>	Public DNS zone to serve public clients.			
Option	Description									
<i>shadow</i>	Shadow DNS zone to serve internal clients.									
<i>public</i>	Public DNS zone to serve public clients.									
ip-master	IP address of master DNS server. Entries in this master DNS server and imported into the DNS zone.	ipv4-address-any	Not Specified	0.0.0.0						
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255	dns						
contact	Email address of the administrator for this zone. You can specify only the username (e.g. admin) or full email address (e.g. admin@test.com) When using a simple username, the domain of the email will be this zone.	string	Maximum length: 255	hostmaster						
ttl	Default time-to-live value for the entries of this DNS zone .	integer	Minimum value: 0 Maximum value: 2147483647	86400						
authoritative	Enable/disable authoritative zone.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable authoritative zone.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable authoritative zone.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable authoritative zone.	<i>disable</i>	Disable authoritative zone.			
Option	Description									
<i>enable</i>	Enable authoritative zone.									
<i>disable</i>	Disable authoritative zone.									
forwarder	DNS zone forwarder IP address list.	user	Not Specified							
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0						
rr-max	Maximum number of resource records .	integer	Minimum value: 10 Maximum value: 65536	16384						

### config dns-entry

Parameter	Description	Type	Size	Default
status	Enable/disable resource record status.	option	-	enable



Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable resource record status.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable resource record status.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable resource record status.	<i>disable</i>	Disable resource record status.													
Option	Description																			
<i>enable</i>	Enable resource record status.																			
<i>disable</i>	Disable resource record status.																			
type	Resource record type.	option	-	A																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>A</i></td> <td>Host type.</td> </tr> <tr> <td><i>NS</i></td> <td>Name server type.</td> </tr> <tr> <td><i>CNAME</i></td> <td>Canonical name type.</td> </tr> <tr> <td><i>MX</i></td> <td>Mail exchange type.</td> </tr> <tr> <td><i>AAAA</i></td> <td>IPv6 host type.</td> </tr> <tr> <td><i>PTR</i></td> <td>Pointer type.</td> </tr> <tr> <td><i>PTR_V6</i></td> <td>IPv6 pointer type.</td> </tr> </tbody> </table>	Option	Description	<i>A</i>	Host type.	<i>NS</i>	Name server type.	<i>CNAME</i>	Canonical name type.	<i>MX</i>	Mail exchange type.	<i>AAAA</i>	IPv6 host type.	<i>PTR</i>	Pointer type.	<i>PTR_V6</i>	IPv6 pointer type.			
Option	Description																			
<i>A</i>	Host type.																			
<i>NS</i>	Name server type.																			
<i>CNAME</i>	Canonical name type.																			
<i>MX</i>	Mail exchange type.																			
<i>AAAA</i>	IPv6 host type.																			
<i>PTR</i>	Pointer type.																			
<i>PTR_V6</i>	IPv6 pointer type.																			
ttl	Time-to-live for this entry .	integer	Minimum value: 0 Maximum value: 2147483647	0																
preference	DNS entry preference, 0 is the highest preference	integer	Minimum value: 0 Maximum value: 65535	10																
ip	IPv4 address of the host.	ipv4-address-any	Not Specified	0.0.0.0																
ipv6	IPv6 address of the host.	ipv6-address	Not Specified	::																
hostname	Name of the host.	string	Maximum length: 255																	
canonical-name	Canonical name of the host.	string	Maximum length: 255																	

## config system dns-server

Configure DNS servers.

```
config system dns-server
  Description: Configure DNS servers.
  edit <name>
```

```

    set mode [recursive|non-recursive|...]
    set dnsfilter-profile {string}
  next
end

```

## config system dns-server

Parameter	Description	Type	Size	Default								
mode	DNS server mode.	option	-	recursive								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>recursive</i></td> <td>Shadow DNS database and forward.</td> </tr> <tr> <td><i>non-recursive</i></td> <td>Public DNS database only.</td> </tr> <tr> <td><i>forward-only</i></td> <td>Forward only.</td> </tr> </tbody> </table>	Option	Description	<i>recursive</i>	Shadow DNS database and forward.	<i>non-recursive</i>	Public DNS database only.	<i>forward-only</i>	Forward only.			
Option	Description											
<i>recursive</i>	Shadow DNS database and forward.											
<i>non-recursive</i>	Public DNS database only.											
<i>forward-only</i>	Forward only.											
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35									

## config system resource-limits

Configure resource limits.

```

config system resource-limits
  Description: Configure resource limits.
  set session {integer}
  set ipsec-phase1 {integer}
  set ipsec-phase2 {integer}
  set ipsec-phase1-interface {integer}
  set ipsec-phase2-interface {integer}
  set dialup-tunnel {integer}
  set firewall-policy {integer}
  set firewall-address {integer}
  set firewall-addrgrp {integer}
  set custom-service {integer}
  set service-group {integer}
  set onetime-schedule {integer}
  set recurring-schedule {integer}
  set user {integer}
  set user-group {integer}
  set sslvpn {integer}
  set proxy {integer}
  set log-disk-quota {integer}
end

```

## config system resource-limits

Parameter	Description	Type	Size	Default
session	Maximum number of sessions.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1	Maximum number of VPN IPsec phase1 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2	Maximum number of VPN IPsec phase2 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2-interface	Maximum number of VPN IPsec phase2 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
dialup-tunnel	Maximum number of dial-up tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-policy	Maximum number of firewall policies (policy, policy46, policy64, DoS-policy4, DoS-policy6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-addrgrp	Maximum number of firewall address groups (IPv4, IPv6).	integer	Minimum value: 0 Maximum value: 4294967295	
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295	
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
recurring-schedule	Maximum number of firewall recurring schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
user	Maximum number of local users.	integer	Minimum value: 0 Maximum value: 4294967295	
user-group	Maximum number of user groups.	integer	Minimum value: 0 Maximum value: 4294967295	
sslvpn	Maximum number of SSL-VPN.	integer	Minimum value: 0 Maximum value: 4294967295	
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295	
log-disk-quota	Log disk quota in MB.	integer	Minimum value: 0 Maximum value: 4294967295**	

\*\* Values may differ between models.

## config system vdom-property

Configure VDOM property.

```
config system vdom-property
  Description: Configure VDOM property.
  edit <name>
    set description {string}
    set snmp-index {integer}
    set session {user}
```

```

set ipsec-phase1 {user}
set ipsec-phase2 {user}
set ipsec-phase1-interface {user}
set ipsec-phase2-interface {user}
set dialup-tunnel {user}
set firewall-policy {user}
set firewall-address {user}
set firewall-addrgrp {user}
set custom-service {user}
set service-group {user}
set onetime-schedule {user}
set recurring-schedule {user}
set user {user}
set user-group {user}
set sslvpn {user}
set proxy {user}
set log-disk-quota {user}
next
end

```

## config system vdom-property

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
snmp-index	Permanent SNMP Index of the virtual domain .	integer	Minimum value: 1 Maximum value: 2147483647	0
session	Maximum guaranteed number of sessions.	user	Not Specified	
ipsec-phase1	Maximum guaranteed number of VPN IPsec phase 1 tunnels.	user	Not Specified	
ipsec-phase2	Maximum guaranteed number of VPN IPsec phase 2 tunnels.	user	Not Specified	
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified	
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified	
dialup-tunnel	Maximum guaranteed number of dial-up tunnels.	user	Not Specified	
firewall-policy	Maximum guaranteed number of firewall policies (policy, policy46, policy64, DoS-policy4, DoS-policy6, multicast).	user	Not Specified	
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified	

Parameter	Description	Type	Size	Default
firewall-addrgrp	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified	
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified	
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified	
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified	
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified	
user	Maximum guaranteed number of local users.	user	Not Specified	
user-group	Maximum guaranteed number of user groups.	user	Not Specified	
sslvpn	Maximum guaranteed number of SSL-VPNs.	user	Not Specified	
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified	
log-disk-quota	Log disk quota in MB (range depends on how much disk space is available).	user	Not Specified	

## config system sdwan

Configure redundant Internet connections with multiple outbound links and health-check profiles.

```

config system sdwan
  Description: Configure redundant Internet connections with multiple outbound links and
    health-check profiles.
  set status [disable|enable]
  set load-balance-mode [source-ip-based|weight-based|...]
  set duplication-max-num {integer}
  set neighbor-hold-down [enable|disable]
  set neighbor-hold-down-time {integer}
  set neighbor-hold-boot-time {integer}
  set fail-detect [enable|disable]
  set fail-alert-interfaces <name1>, <name2>, ...
config zone
  Description: Configure SD-WAN zones.
  edit <name>
    set service-sla-tie-break [cfg-order|fib-best-match]
  next
end
config members
  Description: FortiGate interfaces added to the SD-WAN.
  edit <seq-num>
    set interface {string}
    set zone {string}
    set gateway {ipv4-address}
    set source {ipv4-address}

```

```

set gateway6 {ipv6-address}
set source6 {ipv6-address}
set cost {integer}
set weight {integer}
set priority {integer}
set spillover-threshold {integer}
set ingress-spillover-threshold {integer}
set volume-ratio {integer}
set status [disable|enable]
set comment {var-string}
next
end
config health-check
  Description: SD-WAN status checking or health checking. Identify a server on the
    Internet and determine how SD-WAN verifies that the FortiGate can communicate
    with it.
edit <name>
  set probe-packets [disable|enable]
  set addr-mode [ipv4|ipv6]
  set system-dns [disable|enable]
  set server {string}
  set protocol [ping|tcp-echo|...]
  set port {integer}
  set quality-measured-method [half-open|half-close]
  set security-mode [none|authentication]
  set user {string}
  set password {password}
  set packet-size {integer}
  set ha-priority {integer}
  set ftp-mode [passive|port]
  set ftp-file {string}
  set http-get {string}
  set http-agent {string}
  set http-match {string}
  set dns-request-domain {string}
  set dns-match-ip {ipv4-address}
  set interval {integer}
  set probe-timeout {integer}
  set failtime {integer}
  set recoverytime {integer}
  set probe-count {integer}
  set diffservcode {user}
  set update-cascade-interface [enable|disable]
  set update-static-route [enable|disable]
  set sla-fail-log-period {integer}
  set sla-pass-log-period {integer}
  set threshold-warning-packetloss {integer}
  set threshold-alert-packetloss {integer}
  set threshold-warning-latency {integer}
  set threshold-alert-latency {integer}
  set threshold-warning-jitter {integer}
  set threshold-alert-jitter {integer}
  set members <seq-num1>, <seq-num2>, ...
config sla
  Description: Service level agreement (SLA).
  edit <id>
    set link-cost-factor {option1}, {option2}, ...

```

```

        set latency-threshold {integer}
        set jitter-threshold {integer}
        set packetloss-threshold {integer}
    next
end
next
end
config neighbor
    Description: Create SD-WAN neighbor from BGP neighbor table to control route
        advertisements according to SLA status.
    edit <ip>
        set member {integer}
        set role [standalone|primary|...]
        set health-check {string}
        set sla-id {integer}
    next
end
config service
    Description: Create SD-WAN rules (also called services) to control how sessions are
        distributed to interfaces in the SD-WAN.
    edit <id>
        set name {string}
        set addr-mode [ipv4|ipv6]
        set input-device <name1>, <name2>, ...
        set input-device-negate [enable|disable]
        set mode [auto|manual|...]
        set minimum-sla-meet-members {integer}
        set hash-mode [round-robin|source-ip-based|...]
        set role [standalone|primary|...]
        set standalone-action [enable|disable]
        set quality-link {integer}
        set tos {user}
        set tos-mask {user}
        set protocol {integer}
        set start-port {integer}
        set end-port {integer}
        set route-tag {integer}
        set dst <name1>, <name2>, ...
        set dst-negate [enable|disable]
        set src <name1>, <name2>, ...
        set dst6 <name1>, <name2>, ...
        set src6 <name1>, <name2>, ...
        set src-negate [enable|disable]
        set users <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set internet-service [enable|disable]
        set internet-service-custom <name1>, <name2>, ...
        set internet-service-custom-group <name1>, <name2>, ...
        set internet-service-name <name1>, <name2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-app-ctrl <id1>, <id2>, ...
        set internet-service-app-ctrl-group <name1>, <name2>, ...
        set health-check <name1>, <name2>, ...
        set link-cost-factor [latency|jitter|...]
        set packet-loss-weight {integer}
        set latency-weight {integer}
        set jitter-weight {integer}

```



```

set bandwidth-weight {integer}
set link-cost-threshold {integer}
set hold-down-time {integer}
set dscp-forward [enable|disable]
set dscp-reverse [enable|disable]
set dscp-forward-tag {user}
set dscp-reverse-tag {user}
config sla
    Description: Service level agreement (SLA).
    edit <health-check>
        set id {integer}
    next
end
set priority-members <seq-num1>, <seq-num2>, ...
set status [enable|disable]
set gateway [enable|disable]
set default [enable|disable]
set sla-compare-method [order|number]
set tie-break [zone|cfg-order|...]
set use-shortcut-sla [enable|disable]
next
end
config duplication
    Description: Create SD-WAN duplication rule.
    edit <id>
        set service-id <id1>, <id2>, ...
        set srcaddr <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set srcintf <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set service <name1>, <name2>, ...
        set packet-duplication [disable|force|...]
        set packet-de-duplication [enable|disable]
    next
end
end

```

## config system sdwan

Parameter	Description	Type	Size	Default						
status	Enable/disable SD-WAN.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SD-WAN.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable SD-WAN.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SD-WAN.	<i>enable</i>	Enable SD-WAN.			
Option	Description									
<i>disable</i>	Disable SD-WAN.									
<i>enable</i>	Enable SD-WAN.									
load-balance-mode	Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.	option	-	source-ip-based						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>source-ip-based</i></td> <td>Source IP load balancing. All traffic from a source IP is sent to the same interface.</td> </tr> <tr> <td><i>weight-based</i></td> <td>Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.</td> </tr> <tr> <td><i>usage-based</i></td> <td>Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.</td> </tr> <tr> <td><i>source-dest-ip-based</i></td> <td>Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.</td> </tr> <tr> <td><i>measured-volume-based</i></td> <td>Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.</td> </tr> </tbody> </table>	Option	Description	<i>source-ip-based</i>	Source IP load balancing. All traffic from a source IP is sent to the same interface.	<i>weight-based</i>	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.	<i>usage-based</i>	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.	<i>source-dest-ip-based</i>	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.	<i>measured-volume-based</i>	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.			
Option	Description															
<i>source-ip-based</i>	Source IP load balancing. All traffic from a source IP is sent to the same interface.															
<i>weight-based</i>	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.															
<i>usage-based</i>	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.															
<i>source-dest-ip-based</i>	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.															
<i>measured-volume-based</i>	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.															
duplication-max-num	Maximum number of interface members a packet is duplicated in the SD-WAN zone .	integer	Minimum value: 2 Maximum value: 4	2												
neighbor-hold-down	Enable/disable hold switching from the secondary neighbor to the primary neighbor.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable hold switching from the secondary neighbor to the primary neighbor.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable hold switching from the secondary neighbor to the primary neighbor.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable hold switching from the secondary neighbor to the primary neighbor.	<i>disable</i>	Disable hold switching from the secondary neighbor to the primary neighbor.									
Option	Description															
<i>enable</i>	Enable hold switching from the secondary neighbor to the primary neighbor.															
<i>disable</i>	Disable hold switching from the secondary neighbor to the primary neighbor.															
neighbor-hold-down-time	Waiting period in seconds when switching from the secondary neighbor to the primary neighbor when hold-down is disabled. .	integer	Minimum value: 0 Maximum value: 10000000	0												
neighbor-hold-boot-time	Waiting period in seconds when switching from the primary neighbor to the secondary neighbor from the neighbor start. .	integer	Minimum value: 0 Maximum value: 10000000	0												
fail-detect	Enable/disable SD-WAN Internet connection status checking (failure detection).	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable status checking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable status checking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable status checking.	<i>disable</i>	Disable status checking.									
Option	Description															
<i>enable</i>	Enable status checking.															
<i>disable</i>	Disable status checking.															



Parameter	Description	Type	Size	Default						
weight	Weight of this interface for weighted load balancing. More traffic is directed to interfaces with higher weights.	integer	Minimum value: 1 Maximum value: 255	1						
priority	Priority of the interface . Used for SD-WAN rules or priority rules.	integer	Minimum value: 0 Maximum value: 65535	0						
spillover-threshold	Egress spillover threshold for this interface . When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0						
ingress-spillover-threshold	Ingress spillover threshold for this interface . When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0						
volume-ratio	Measured volume ratio .	integer	Minimum value: 1 Maximum value: 255	1						
status	Enable/disable this interface in the SD-WAN.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable this interface in the SD-WAN.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable this interface in the SD-WAN.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable this interface in the SD-WAN.	<i>enable</i>	Enable this interface in the SD-WAN.			
Option	Description									
<i>disable</i>	Disable this interface in the SD-WAN.									
<i>enable</i>	Enable this interface in the SD-WAN.									
comment	Comments.	var-string	Maximum length: 255							

### config health-check

Parameter	Description	Type	Size	Default						
probe-packets	Enable/disable transmission of probe packets.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable transmission of probe packets.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable transmission of probe packets.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable transmission of probe packets.	<i>enable</i>	Enable transmission of probe packets.			
Option	Description									
<i>disable</i>	Disable transmission of probe packets.									
<i>enable</i>	Enable transmission of probe packets.									

Parameter	Description	Type	Size	Default																		
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>IPv4 mode.</td> </tr> <tr> <td><i>ipv6</i></td> <td>IPv6 mode.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	IPv4 mode.	<i>ipv6</i>	IPv6 mode.															
Option	Description																					
<i>ipv4</i>	IPv4 mode.																					
<i>ipv6</i>	IPv6 mode.																					
system-dns	Enable/disable system DNS as the probe server.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable system DNS as the probe server.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable system DNS as the probe server.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable system DNS as the probe server.	<i>enable</i>	Enable system DNS as the probe server.															
Option	Description																					
<i>disable</i>	Disable system DNS as the probe server.																					
<i>enable</i>	Enable system DNS as the probe server.																					
server	IP address or FQDN name of the server.	string	Maximum length: 79																			
protocol	Protocol used to determine if the FortiGate can communicate with the server.	option	-	ping																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>Use PING to test the link with the server.</td> </tr> <tr> <td><i>tcp-echo</i></td> <td>Use TCP echo to test the link with the server.</td> </tr> <tr> <td><i>udp-echo</i></td> <td>Use UDP echo to test the link with the server.</td> </tr> <tr> <td><i>http</i></td> <td>Use HTTP-GET to test the link with the server.</td> </tr> <tr> <td><i>twamp</i></td> <td>Use TWAMP to test the link with the server.</td> </tr> <tr> <td><i>dns</i></td> <td>Use DNS query to test the link with the server.</td> </tr> <tr> <td><i>tcp-connect</i></td> <td>Use a full TCP connection to test the link with the server.</td> </tr> <tr> <td><i>ftp</i></td> <td>Use FTP to test the link with the server.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>tcp-echo</i>	Use TCP echo to test the link with the server.	<i>udp-echo</i>	Use UDP echo to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>twamp</i>	Use TWAMP to test the link with the server.	<i>dns</i>	Use DNS query to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.	<i>ftp</i>	Use FTP to test the link with the server.			
Option	Description																					
<i>ping</i>	Use PING to test the link with the server.																					
<i>tcp-echo</i>	Use TCP echo to test the link with the server.																					
<i>udp-echo</i>	Use UDP echo to test the link with the server.																					
<i>http</i>	Use HTTP-GET to test the link with the server.																					
<i>twamp</i>	Use TWAMP to test the link with the server.																					
<i>dns</i>	Use DNS query to test the link with the server.																					
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.																					
<i>ftp</i>	Use FTP to test the link with the server.																					
port	Port number used to communicate with the server over the selected protocol .	integer	Minimum value: 0 Maximum value: 65535	0																		
quality-measured-method	Method to measure the quality of tcp-connect.	option	-	half-open																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>half-open</i></td> <td>Measure the round trip between syn and ack.</td> </tr> <tr> <td><i>half-close</i></td> <td>Measure the round trip between fin and ack.</td> </tr> </tbody> </table>	Option	Description	<i>half-open</i>	Measure the round trip between syn and ack.	<i>half-close</i>	Measure the round trip between fin and ack.			
Option	Description									
<i>half-open</i>	Measure the round trip between syn and ack.									
<i>half-close</i>	Measure the round trip between fin and ack.									
security-mode	Twamp controller security mode.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Unauthenticated mode.</td> </tr> <tr> <td><i>authentication</i></td> <td>Authenticated mode.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.			
Option	Description									
<i>none</i>	Unauthenticated mode.									
<i>authentication</i>	Authenticated mode.									
user	The user name to access probe server.	string	Maximum length: 64							
password	Twamp controller password in authentication mode	password	Not Specified							
packet-size	Packet size of a twamp test session,	integer	Minimum value: 64 Maximum value: 1024	64						
ha-priority	HA election priority .	integer	Minimum value: 1 Maximum value: 50	1						
ftp-mode	FTP mode.	option	-	passive						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>passive</i></td> <td>The FTP health-check initiates and establishes the data connection.</td> </tr> <tr> <td><i>port</i></td> <td>The FTP server initiates and establishes the data connection.</td> </tr> </tbody> </table>	Option	Description	<i>passive</i>	The FTP health-check initiates and establishes the data connection.	<i>port</i>	The FTP server initiates and establishes the data connection.			
Option	Description									
<i>passive</i>	The FTP health-check initiates and establishes the data connection.									
<i>port</i>	The FTP server initiates and establishes the data connection.									
ftp-file	Full path and file name on the FTP server to download for FTP health-check to probe.	string	Maximum length: 254							
http-get	URL used to communicate with the server if the protocol is HTTP.	string	Maximum length: 1024	/						
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/						
http-match	Response string expected from the server if the protocol is HTTP.	string	Maximum length: 1024							
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255	www.example.com						



Parameter	Description	Type	Size	Default
sla-fail-log-period	Time interval in seconds that SLA fail log messages will be generated .	integer	Minimum value: 0 Maximum value: 3600	0
sla-pass-log-period	Time interval in seconds that SLA pass log messages will be generated .	integer	Minimum value: 0 Maximum value: 3600	0
threshold-warning-packetloss	Warning threshold for packet loss .	integer	Minimum value: 0 Maximum value: 100	0
threshold-alert-packetloss	Alert threshold for packet loss .	integer	Minimum value: 0 Maximum value: 100	0
threshold-warning-latency	Warning threshold for latency .	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-latency	Alert threshold for latency .	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-warning-jitter	Warning threshold for jitter .	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-jitter	Alert threshold for jitter .	integer	Minimum value: 0 Maximum value: 4294967295	0
members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	



## config sla

Parameter	Description	Type	Size	Default
id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config neighbor

Parameter	Description	Type	Size	Default								
member	Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0								
role	Role of neighbor.	option	-	standalone								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>standalone</i></td><td>Standalone neighbor.</td></tr><tr><td><i>primary</i></td><td>Primary neighbor.</td></tr><tr><td><i>secondary</i></td><td>Secondary neighbor.</td></tr></tbody></table>	Option	Description	<i>standalone</i>	Standalone neighbor.	<i>primary</i>	Primary neighbor.	<i>secondary</i>	Secondary neighbor.			
Option	Description											
<i>standalone</i>	Standalone neighbor.											
<i>primary</i>	Primary neighbor.											
<i>secondary</i>	Secondary neighbor.											
health-check	SD-WAN health-check name.	string	Maximum length: 35									
sla-id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								

## config service

Parameter	Description	Type	Size	Default						
name	SD-WAN rule name.	string	Maximum length: 35							
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ipv4</i></td><td>IPv4 mode.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 mode.</td></tr></tbody></table>	Option	Description	<i>ipv4</i>	IPv4 mode.	<i>ipv6</i>	IPv6 mode.			
Option	Description									
<i>ipv4</i>	IPv4 mode.									
<i>ipv6</i>	IPv6 mode.									

Parameter	Description	Type	Size	Default												
input-device <name>	Source interface name. Interface name.	string	Maximum length: 79													
input-device- negate	Enable/disable negation of input device match.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable negation of input device match.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable negation of input device match.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negation of input device match.	<i>disable</i>	Disable negation of input device match.									
Option	Description															
<i>enable</i>	Enable negation of input device match.															
<i>disable</i>	Disable negation of input device match.															
mode	Control how the SD-WAN rule sets the priority of interfaces in the SD-WAN.	option	-	manual												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Assign interfaces a priority based on quality.</td> </tr> <tr> <td><i>manual</i></td> <td>Assign interfaces a priority manually.</td> </tr> <tr> <td><i>priority</i></td> <td>Assign interfaces a priority based on the link-cost-factor quality of the interface.</td> </tr> <tr> <td><i>sla</i></td> <td>Assign interfaces a priority based on selected SLA settings.</td> </tr> <tr> <td><i>load-balance</i></td> <td>Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Assign interfaces a priority based on quality.	<i>manual</i>	Assign interfaces a priority manually.	<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.	<i>sla</i>	Assign interfaces a priority based on selected SLA settings.	<i>load-balance</i>	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.			
Option	Description															
<i>auto</i>	Assign interfaces a priority based on quality.															
<i>manual</i>	Assign interfaces a priority manually.															
<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.															
<i>sla</i>	Assign interfaces a priority based on selected SLA settings.															
<i>load-balance</i>	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.															
minimum-sla- meet- members	Minimum number of members which meet SLA.	integer	Minimum value: 0 Maximum value: 255	0												
hash-mode	Hash algorithm for selected priority members for load balance mode.	option	-	round-robin												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>round-robin</i></td> <td>All traffic are distributed to selected interfaces in equal portions and circular order.</td> </tr> <tr> <td><i>source-ip-based</i></td> <td>All traffic from a source IP is sent to the same interface.</td> </tr> <tr> <td><i>source-dest-ip- based</i></td> <td>All traffic from a source IP to a destination IP is sent to the same interface.</td> </tr> <tr> <td><i>inbandwidth</i></td> <td>All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.</td> </tr> <tr> <td><i>outbandwidth</i></td> <td>All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.</td> </tr> </tbody> </table>	Option	Description	<i>round-robin</i>	All traffic are distributed to selected interfaces in equal portions and circular order.	<i>source-ip-based</i>	All traffic from a source IP is sent to the same interface.	<i>source-dest-ip- based</i>	All traffic from a source IP to a destination IP is sent to the same interface.	<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.	<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.			
Option	Description															
<i>round-robin</i>	All traffic are distributed to selected interfaces in equal portions and circular order.															
<i>source-ip-based</i>	All traffic from a source IP is sent to the same interface.															
<i>source-dest-ip- based</i>	All traffic from a source IP to a destination IP is sent to the same interface.															
<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.															
<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bibandwidth</i></td> <td>All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.</td> </tr> </tbody> </table>	Option	Description	<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.							
Option	Description											
<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.											
role	Service role to work with neighbor.	option	-	standalone								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standalone</i></td> <td>Standalone service.</td> </tr> <tr> <td><i>primary</i></td> <td>Primary service for primary neighbor.</td> </tr> <tr> <td><i>secondary</i></td> <td>Secondary service for secondary neighbor.</td> </tr> </tbody> </table>	Option	Description	<i>standalone</i>	Standalone service.	<i>primary</i>	Primary service for primary neighbor.	<i>secondary</i>	Secondary service for secondary neighbor.			
Option	Description											
<i>standalone</i>	Standalone service.											
<i>primary</i>	Primary service for primary neighbor.											
<i>secondary</i>	Secondary service for secondary neighbor.											
standalone-action	Enable/disable service when selected neighbor role is standalone while service role is not standalone.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable service when selected neighbor role is standalone.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable service when selected neighbor role is standalone.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable service when selected neighbor role is standalone.	<i>disable</i>	Disable service when selected neighbor role is standalone.					
Option	Description											
<i>enable</i>	Enable service when selected neighbor role is standalone.											
<i>disable</i>	Disable service when selected neighbor role is standalone.											
quality-link	Quality grade.	integer	Minimum value: 0 Maximum value: 255	0								
tos	Type of service bit pattern.	user	Not Specified									
tos-mask	Type of service evaluated bits.	user	Not Specified									
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0								
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535	1								
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535	65535								

Parameter	Description	Type	Size	Default						
route-tag	IPv4 route map route-tag.	integer	Minimum value: 0 Maximum value: 4294967295	0						
dst <name>	Destination address name. Address or address group name.	string	Maximum length: 79							
dst-negate	Enable/disable negation of destination address match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable destination address negation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable destination address negation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable destination address negation.	<i>disable</i>	Disable destination address negation.			
Option	Description									
<i>enable</i>	Enable destination address negation.									
<i>disable</i>	Disable destination address negation.									
src <name>	Source address name. Address or address group name.	string	Maximum length: 79							
dst6 <name>	Destination address6 name. Address6 or address6 group name.	string	Maximum length: 79							
src6 <name>	Source address6 name. Address6 or address6 group name.	string	Maximum length: 79							
src-negate	Enable/disable negation of source address match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source address negation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source address negation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source address negation.	<i>disable</i>	Disable source address negation.			
Option	Description									
<i>enable</i>	Enable source address negation.									
<i>disable</i>	Disable source address negation.									
users <name>	User name. User name.	string	Maximum length: 79							
groups <name>	User groups. Group name.	string	Maximum length: 79							
internet-service	Enable/disable use of Internet service for application-based load balancing.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable cloud service to support application-based load balancing.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable cloud service to support application-based load balancing.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable cloud service to support application-based load balancing.	<i>disable</i>	Disable cloud service to support application-based load balancing.			
Option	Description									
<i>enable</i>	Enable cloud service to support application-based load balancing.									
<i>disable</i>	Disable cloud service to support application-based load balancing.									

Parameter	Description	Type	Size	Default
internet-service-custom <name>	Custom Internet service name list. Custom Internet service name.	string	Maximum length: 79	
internet-service-custom-group <name>	Custom Internet Service group list. Custom Internet Service group name.	string	Maximum length: 79	
internet-service-name <name>	Internet service name list. Internet service name.	string	Maximum length: 79	
internet-service-group <name>	Internet Service group list. Internet Service group name.	string	Maximum length: 79	
internet-service-app-ctrl <id>	Application control based Internet Service ID list. Application control based Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	
internet-service-app-ctrl-group <name>	Application control based Internet Service group list. Application control based Internet Service group name.	string	Maximum length: 79	
health-check <name>	Health check list. Health check name.	string	Maximum length: 79	
link-cost-factor	Link cost factor.	option	-	latency

Option	Description
<i>latency</i>	Select link based on latency.
<i>jitter</i>	Select link based on jitter.
<i>packet-loss</i>	Select link based on packet loss.
<i>inbandwidth</i>	Select link based on available bandwidth of incoming traffic.
<i>outbandwidth</i>	Select link based on available bandwidth of outgoing traffic.
<i>bibandwidth</i>	Select link based on available bandwidth of bidirectional traffic.
<i>custom-profile-1</i>	Select link based on customized profile.

Parameter	Description	Type	Size	Default						
packet-loss-weight	Coefficient of packet-loss in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0						
latency-weight	Coefficient of latency in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0						
jitter-weight	Coefficient of jitter in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0						
bandwidth-weight	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0						
link-cost-threshold	Percentage threshold change of link cost values that will result in policy route regeneration .	integer	Minimum value: 0 Maximum value: 10000000	10						
hold-down-time	Waiting period in seconds when switching from the back-up member to the primary member .	integer	Minimum value: 0 Maximum value: 10000000	0						
dscp-forward	Enable/disable forward traffic DSCP tag.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of forward DSCP tag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of forward DSCP tag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of forward DSCP tag.	<i>disable</i>	Disable use of forward DSCP tag.			
Option	Description									
<i>enable</i>	Enable use of forward DSCP tag.									
<i>disable</i>	Disable use of forward DSCP tag.									
dscp-reverse	Enable/disable reverse traffic DSCP tag.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of reverse DSCP tag.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of reverse DSCP tag.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of reverse DSCP tag.	<i>disable</i>	Disable use of reverse DSCP tag.			
Option	Description									
<i>enable</i>	Enable use of reverse DSCP tag.									
<i>disable</i>	Disable use of reverse DSCP tag.									

Parameter	Description	Type	Size	Default
dscp-forward-tag	Forward traffic DSCP tag.	user	Not Specified	
dscp-reverse-tag	Reverse traffic DSCP tag.	user	Not Specified	
priority-members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	
status	Enable/disable SD-WAN service.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SD-WAN service.		
	<i>disable</i>	Disable SD-WAN service.		
gateway	Enable/disable SD-WAN service gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SD-WAN service gateway.		
	<i>disable</i>	Disable SD-WAN service gateway.		
default	Enable/disable use of SD-WAN as default service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of SD-WAN as default service.		
	<i>disable</i>	Disable use of SD-WAN as default service.		
sla-compare-method	Method to compare SLA value for SLA mode.	option	-	order
	<b>Option</b>	<b>Description</b>		
	<i>order</i>	Compare SLA value based on the order of health-check.		
	<i>number</i>	Compare SLA value based on the number of satisfied health-check. Limits health-checks to only configured member interfaces.		
tie-break	Method of selecting member if more than one meets the SLA.	option	-	zone
	<b>Option</b>	<b>Description</b>		
	<i>zone</i>	Use the setting that is configured for the members' zone.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>cfg-order</i></td> <td>Members that meet the SLA are selected in the order they are configured.</td> </tr> <tr> <td><i>fib-best-match</i></td> <td>Members that meet the SLA are selected that match the longest prefix in the routing table.</td> </tr> </tbody> </table>	Option	Description	<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.	<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.			
Option	Description									
<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.									
<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.									
use-shortcut-sla	Enable/disable use of ADVPN shortcut for quality comparison.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of ADVPN shortcut for quality comparison.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of ADVPN shortcut for quality comparison.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of ADVPN shortcut for quality comparison.	<i>disable</i>	Disable use of ADVPN shortcut for quality comparison.			
Option	Description									
<i>enable</i>	Enable use of ADVPN shortcut for quality comparison.									
<i>disable</i>	Disable use of ADVPN shortcut for quality comparison.									

### config sla

Parameter	Description	Type	Size	Default
id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config duplication

Parameter	Description	Type	Size	Default
service-id <id>	SD-WAN service rule ID list. SD-WAN service rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	
srcaddr <name>	Source address or address group names. Address or address group name.	string	Maximum length: 79	
dstaddr <name>	Destination address or address group names. Address or address group name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79	
dstaddr6 <name>	Destination address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79	
srcintf <name>	Incoming (ingress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79	



Parameter	Description	Type	Size	Default								
<code>dstintf</code> <name>	Outgoing (egress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79									
<code>service</code> <name>	Service and service group name. Service and service group name.	string	Maximum length: 79									
<code>packet-duplication</code>	Configure packet duplication method.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet duplication.</td> </tr> <tr> <td><i>force</i></td> <td>Duplicate packets across all interface members of the SD-WAN zone.</td> </tr> <tr> <td><i>on-demand</i></td> <td>Duplicate packets across all interface members of the SD-WAN zone based on the link quality.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet duplication.	<i>force</i>	Duplicate packets across all interface members of the SD-WAN zone.	<i>on-demand</i>	Duplicate packets across all interface members of the SD-WAN zone based on the link quality.			
Option	Description											
<i>disable</i>	Disable packet duplication.											
<i>force</i>	Duplicate packets across all interface members of the SD-WAN zone.											
<i>on-demand</i>	Duplicate packets across all interface members of the SD-WAN zone based on the link quality.											
<code>packet-de-duplication</code>	Enable/disable discarding of packets that have been duplicated.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable discarding of packets that have been duplicated.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable discarding of packets that have been duplicated.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable discarding of packets that have been duplicated.	<i>disable</i>	Disable discarding of packets that have been duplicated.					
Option	Description											
<i>enable</i>	Enable discarding of packets that have been duplicated.											
<i>disable</i>	Disable discarding of packets that have been duplicated.											

## config system speed-test-server

Configure speed test server list.

```

config system speed-test-server
  Description: Configure speed test server list.
  edit <name>
    set timestamp {integer}
    config host
      Description: Hosts of the server.
      edit <id>
        set ip {ipv4-address}
        set port {integer}
        set user {string}
        set password {password}
      next
    end
  next
end

```

## config system speed-test-server

Parameter	Description	Type	Size	Default
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config host

Parameter	Description	Type	Size	Default
ip	Server host IPv4 address.	ipv4-address	Not Specified	0.0.0.0
port	Server host port number to communicate with client.	integer	Minimum value: 1 Maximum value: 65535	5204
user	Speed test host user name.	string	Maximum length: 64	
password	Speed test host password.	password	Not Specified	

## config system lldp network-policy

Configure LLDP network policy.

```
config system lldp network-policy
  Description: Configure LLDP network policy.
  edit <name>
    set comment {var-string}
    config voice
      Description: Voice.
      set status [disable|enable]
      set tag [none|dot1q|...]
      set vlan {integer}
      set priority {integer}
      set dscp {integer}
    end
    config voice-signaling
      Description: Voice signaling.
      set status [disable|enable]
      set tag [none|dot1q|...]
      set vlan {integer}
      set priority {integer}
      set dscp {integer}
    end
  end
```

---

```
config guest
  Description: Guest.
  set status [disable|enable]
  set tag [none|dot1q|...]
  set vlan {integer}
  set priority {integer}
  set dscp {integer}
end
config guest-voice-signaling
  Description: Guest Voice Signaling.
  set status [disable|enable]
  set tag [none|dot1q|...]
  set vlan {integer}
  set priority {integer}
  set dscp {integer}
end
config softphone
  Description: Softphone.
  set status [disable|enable]
  set tag [none|dot1q|...]
  set vlan {integer}
  set priority {integer}
  set dscp {integer}
end
config video-conferencing
  Description: Video Conferencing.
  set status [disable|enable]
  set tag [none|dot1q|...]
  set vlan {integer}
  set priority {integer}
  set dscp {integer}
end
config streaming-video
  Description: Streaming Video.
  set status [disable|enable]
  set tag [none|dot1q|...]
  set vlan {integer}
  set priority {integer}
  set dscp {integer}
end
config video-signaling
  Description: Video Signaling.
  set status [disable|enable]
  set tag [none|dot1q|...]
  set vlan {integer}
  set priority {integer}
  set dscp {integer}
end
next
end
```

## config system lldp network-policy

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	

## config voice

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable advertising this LLDP network policy.</td></tr><tr><td><i>enable</i></td><td>Enable advertising this LLDP network policy.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>Advertise that untagged frames should be used.</td></tr><tr><td><i>dot1q</i></td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td><i>dot1p</i></td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></tbody></table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

## config voice-signaling

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable advertising this LLDP network policy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable advertising this LLDP network policy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Advertise that untagged frames should be used.</td> </tr> <tr> <td><i>dot1q</i></td> <td>Advertise that 802.1Q (VLAN) tagging should be used.</td> </tr> <tr> <td><i>dot1p</i></td> <td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

### config guest

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable advertising this LLDP network policy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable advertising this LLDP network policy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Advertise that untagged frames should be used.</td> </tr> <tr> <td><i>dot1q</i></td> <td>Advertise that 802.1Q (VLAN) tagging should be used.</td> </tr> <tr> <td><i>dot1p</i></td> <td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											

Parameter	Description	Type	Size	Default
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

### config guest-voice-signaling

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable advertising this LLDP network policy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable advertising this LLDP network policy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Advertise that untagged frames should be used.</td> </tr> <tr> <td><i>dot1q</i></td> <td>Advertise that 802.1Q (VLAN) tagging should be used.</td> </tr> <tr> <td><i>dot1p</i></td> <td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

## config softphone

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable advertising this LLDP network policy.</td></tr><tr><td><i>enable</i></td><td>Enable advertising this LLDP network policy.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>none</i></td><td>Advertise that untagged frames should be used.</td></tr><tr><td><i>dot1q</i></td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td><i>dot1p</i></td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></tbody></table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

## config video-conferencing

Parameter	Description	Type	Size	Default						
status	Enable/disable advertising this policy.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable advertising this LLDP network policy.</td></tr><tr><td><i>enable</i></td><td>Enable advertising this LLDP network policy.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.			
Option	Description									
<i>disable</i>	Disable advertising this LLDP network policy.									
<i>enable</i>	Enable advertising this LLDP network policy.									
tag	Advertise tagged or untagged traffic.	option	-	none						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Advertise that untagged frames should be used.</td> </tr> <tr> <td><i>dot1q</i></td> <td>Advertise that 802.1Q (VLAN) tagging should be used.</td> </tr> <tr> <td><i>dot1p</i></td> <td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

### config streaming-video

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable advertising this LLDP network policy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable advertising this LLDP network policy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Advertise that untagged frames should be used.</td> </tr> <tr> <td><i>dot1q</i></td> <td>Advertise that 802.1Q (VLAN) tagging should be used.</td> </tr> <tr> <td><i>dot1p</i></td> <td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								



Parameter	Description	Type	Size	Default
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

## config video-signaling

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable advertising this LLDP network policy.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable advertising this LLDP network policy.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.					
Option	Description											
<i>disable</i>	Disable advertising this LLDP network policy.											
<i>enable</i>	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Advertise that untagged frames should be used.</td> </tr> <tr> <td><i>dot1q</i></td> <td>Advertise that 802.1Q (VLAN) tagging should be used.</td> </tr> <tr> <td><i>dot1p</i></td> <td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
<i>none</i>	Advertise that untagged frames should be used.											
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.											
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

## config system standalone-cluster

Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.

```
config system standalone-cluster
```

```

Description: Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.
set standalone-group-id {integer}
set group-member-id {integer}
set layer2-connection [available|unavailable]
set session-sync-dev {user}
set encryption [enable|disable]
set psksecret {password-3}
end

```

## config system standalone-cluster

Parameter	Description	Type	Size	Default						
standalone-group-id	Cluster group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255	0						
group-member-id	Cluster member ID .	integer	Minimum value: 0 Maximum value: 15	0						
layer2-connection	Indicate whether layer 2 connections are present among FGSP members.	option	-	unavailable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>available</i></td> <td>There exist layer 2 connections among FGSP members.</td> </tr> <tr> <td><i>unavailable</i></td> <td>There does not exist layer 2 connection among FGSP members.</td> </tr> </tbody> </table>		Option	Description	<i>available</i>	There exist layer 2 connections among FGSP members.	<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.		
Option	Description									
<i>available</i>	There exist layer 2 connections among FGSP members.									
<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.									
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified							
encryption	Enable/disable encryption when synchronizing sessions.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable encryption when synchronizing sessions.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable encryption when synchronizing sessions.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable encryption when synchronizing sessions.	<i>disable</i>	Disable encryption when synchronizing sessions.		
Option	Description									
<i>enable</i>	Enable encryption when synchronizing sessions.									
<i>disable</i>	Disable encryption when synchronizing sessions.									
psksecret	Pre-shared secret for session synchronization (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							

## config system cluster-sync

Configure FortiGate Session Life Support Protocol (FGSP) session synchronization.

```

config system cluster-sync
  Description: Configure FortiGate Session Life Support Protocol (FGSP) session
  synchronization.

```

```

edit <sync-id>
  set peervd {string}
  set peerip {ipv4-address}
  set syncvd <name1>, <name2>, ...
  set down-intfs-before-sess-sync <name1>, <name2>, ...
  set hb-interval {integer}
  set hb-lost-threshold {integer}
  set ipsec-tunnel-sync [enable|disable]
  set slave-add-ike-routes [enable|disable]
  config session-sync-filter
    Description: Add one or more filters if you only want to synchronize some sessions.
    Use the filter to configure the types of sessions to synchronize.
    set srcintf {string}
    set dstintf {string}
    set srcaddr {ipv4-classnet-any}
    set dstaddr {ipv4-classnet-any}
    set srcaddr6 {ipv6-network}
    set dstaddr6 {ipv6-network}
    config custom-service
      Description: Only sessions using these custom services are synchronized. Use
      source and destination port ranges to define these custome services.
      edit <id>
        set src-port-range {user}
        set dst-port-range {user}
      next
    end
  end
end
next
end

```

## config system cluster-sync

Parameter	Description	Type	Size	Default
peervd	VDOM that contains the session synchronization link interface on the peer unit. Usually both peers would have the same peervd.	string	Maximum length: 31	root
peerip	IP address of the interface on the peer unit that is used for the session synchronization link.	ipv4-address	Not Specified	0.0.0.0
syncvd <name>	Sessions from these VDOMs are synchronized using this session synchronization configuration. VDOM name.	string	Maximum length: 79	
down-intfs-before-sess-sync <name>	List of interfaces to be turned down before session synchronization is complete. Interface name.	string	Maximum length: 79	
hb-interval	Heartbeat interval .	integer	Minimum value: 1 Maximum value: 10	2

Parameter	Description	Type	Size	Default						
hb-lost-threshold	Lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 10	3						
ipsec-tunnel-sync	Enable/disable IPsec tunnel synchronization.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec tunnel synchronization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec tunnel synchronization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec tunnel synchronization.	<i>disable</i>	Disable IPsec tunnel synchronization.			
Option	Description									
<i>enable</i>	Enable IPsec tunnel synchronization.									
<i>disable</i>	Disable IPsec tunnel synchronization.									
slave-add-ike-routes	Enable/disable IKE route announcement on the backup unit.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Add IKE routes to the backup unit.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not add IKE routes to the backup unit.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Add IKE routes to the backup unit.	<i>disable</i>	Do not add IKE routes to the backup unit.			
Option	Description									
<i>enable</i>	Add IKE routes to the backup unit.									
<i>disable</i>	Do not add IKE routes to the backup unit.									

### config session-sync-filter

Parameter	Description	Type	Size	Default
srcintf	Only sessions from this interface are synchronized. You can only enter one interface name. To synchronize sessions for multiple source interfaces, add multiple filters.	string	Maximum length: 15	
dstintf	Only sessions to this interface are synchronized. You can only enter one interface name. To synchronize sessions to multiple destination interfaces, add multiple filters.	string	Maximum length: 15	
srcaddr	Only sessions from this IPv4 address are synchronized. You can only enter one address. To synchronize sessions from multiple source addresses, add multiple filters.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dstaddr	Only sessions to this IPv4 address are synchronized. You can only enter one address. To synchronize sessions for multiple destination addresses, add multiple filters.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
srcaddr6	Only sessions from this IPv6 address are synchronized. You can only enter one address. To synchronize sessions from multiple source addresses, add multiple filters.	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default
dstaddr6	Only sessions to this IPv6 address are synchronized. You can only enter one address. To synchronize sessions for multiple destination addresses, add multiple filters.	ipv6-network	Not Specified	::/0

### config custom-service

Parameter	Description	Type	Size	Default
src-port-range	Custom service source port range.	user	Not Specified	0-0
dst-port-range	Custom service destination port range.	user	Not Specified	0-0

## config system fortiguard

Configure FortiGuard services.

```

config system fortiguard
  Description: Configure FortiGuard services.
  set fortiguard-anycast [enable|disable]
  set fortiguard-anycast-source [fortinet|aws|...]
  set protocol [udp|http|...]
  set port [8888|53|...]
  set load-balance-servers {integer}
  set auto-join-forticloud [enable|disable]
  set update-server-location [usa|any]
  set sandbox-region {string}
  set antispam-force-off [enable|disable]
  set antispam-cache [enable|disable]
  set antispam-cache-ttl {integer}
  set antispam-cache-mpercent {integer}
  set antispam-license {integer}
  set antispam-expiration {integer}
  set antispam-timeout {integer}
  set outbreak-prevention-force-off [enable|disable]
  set outbreak-prevention-cache [enable|disable]
  set outbreak-prevention-cache-ttl {integer}
  set outbreak-prevention-cache-mpercent {integer}
  set outbreak-prevention-license {integer}
  set outbreak-prevention-expiration {integer}
  set outbreak-prevention-timeout {integer}
  set webfilter-force-off [enable|disable]
  set webfilter-cache [enable|disable]
  set webfilter-cache-ttl {integer}
  set webfilter-license {integer}
  set webfilter-expiration {integer}
  set webfilter-timeout {integer}
  set sdns-server-ip {user}
  set sdns-server-port {integer}
  set anycast-sdns-server-ip {ipv4-address}

```

```

set anycast-sdns-server-port {integer}
set sdns-options {option1}, {option2}, ...
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set proxy-server-ip {ipv4-address}
set proxy-server-port {integer}
set proxy-username {string}
set proxy-password {password}
set ddns-server-ip {ipv4-address}
set ddns-server-port {integer}
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

## config system fortiguard

Parameter	Description	Type	Size	Default								
fortiguard-anycast	Enable/disable use of FortiGuard's anycast network.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of FortiGuard's anycast network.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of FortiGuard's anycast network.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of FortiGuard's anycast network.	<i>disable</i>	Disable use of FortiGuard's anycast network.					
Option	Description											
<i>enable</i>	Enable use of FortiGuard's anycast network.											
<i>disable</i>	Disable use of FortiGuard's anycast network.											
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortinet</i></td> <td>Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.</td> </tr> <tr> <td><i>aws</i></td> <td>Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.</td> </tr> <tr> <td><i>debug</i></td> <td>Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.</td> </tr> </tbody> </table>	Option	Description	<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.	<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.	<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.			
Option	Description											
<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.											
<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.											
<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.											
protocol	Protocol used to communicate with the FortiGuard servers.	option	-	https								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>udp</i></td> <td>UDP for server communication (for use by FortiGuard or FortiManager).</td> </tr> <tr> <td><i>http</i></td> <td>HTTP for server communication (for use only by FortiManager).</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS for server communication (for use by FortiGuard or FortiManager).</td> </tr> </tbody> </table>	Option	Description	<i>udp</i>	UDP for server communication (for use by FortiGuard or FortiManager).	<i>http</i>	HTTP for server communication (for use only by FortiManager).	<i>https</i>	HTTPS for server communication (for use by FortiGuard or FortiManager).			
Option	Description											
<i>udp</i>	UDP for server communication (for use by FortiGuard or FortiManager).											
<i>http</i>	HTTP for server communication (for use only by FortiManager).											
<i>https</i>	HTTPS for server communication (for use by FortiGuard or FortiManager).											

Parameter	Description	Type	Size	Default										
port	Port used to communicate with the FortiGuard servers.	option	-	443										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>8888</td> <td>port 8888 for server communication.</td> </tr> <tr> <td>53</td> <td>port 53 for server communication.</td> </tr> <tr> <td>80</td> <td>port 80 for server communication.</td> </tr> <tr> <td>443</td> <td>port 443 for server communication.</td> </tr> </tbody> </table>	Option	Description	8888	port 8888 for server communication.	53	port 53 for server communication.	80	port 80 for server communication.	443	port 443 for server communication.			
Option	Description													
8888	port 8888 for server communication.													
53	port 53 for server communication.													
80	port 80 for server communication.													
443	port 443 for server communication.													
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266	1										
auto-join-forticloud *	Automatically connect to and login to FortiCloud.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable automatic connection and login to FortiCloud.</td> </tr> <tr> <td>disable</td> <td>Disable automatic connection and login to FortiCloud.</td> </tr> </tbody> </table>	Option	Description	enable	Enable automatic connection and login to FortiCloud.	disable	Disable automatic connection and login to FortiCloud.							
Option	Description													
enable	Enable automatic connection and login to FortiCloud.													
disable	Disable automatic connection and login to FortiCloud.													
update-server-location	Signature update server location.	option	-	any										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>usa</td> <td>FGD servers in United States.</td> </tr> <tr> <td>any</td> <td>FGD servers in any location.</td> </tr> </tbody> </table>	Option	Description	usa	FGD servers in United States.	any	FGD servers in any location.							
Option	Description													
usa	FGD servers in United States.													
any	FGD servers in any location.													
sandbox-region	Cloud sandbox region.	string	Maximum length: 63											
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Turn off the FortiGuard antispam service.</td> </tr> <tr> <td>disable</td> <td>Allow the FortiGuard antispam service.</td> </tr> </tbody> </table>	Option	Description	enable	Turn off the FortiGuard antispam service.	disable	Allow the FortiGuard antispam service.							
Option	Description													
enable	Turn off the FortiGuard antispam service.													
disable	Allow the FortiGuard antispam service.													
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-	enable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard antispam request caching.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard antispam request caching.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard antispam request caching.	<i>disable</i>	Disable FortiGuard antispam request caching.			
Option	Description									
<i>enable</i>	Enable FortiGuard antispam request caching.									
<i>disable</i>	Disable FortiGuard antispam request caching.									
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds . Lower times reduce the cache size. Higher times may improve performance since the cache will have more entries.	integer	Minimum value: 300 Maximum value: 86400	1800						
antispam-cache-mpercent	Maximum percent of FortiGate memory the antispam cache is allowed to use .	integer	Minimum value: 1 Maximum value: 15	2						
antispam-license	Interval of time between license checks for the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
antispam-expiration	Expiration date of the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	0						
antispam-timeout	Antispam query time out .	integer	Minimum value: 1 Maximum value: 30	7						
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Turn off FortiGuard antivirus service.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow the FortiGuard antivirus service.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Turn off FortiGuard antivirus service.	<i>disable</i>	Allow the FortiGuard antivirus service.			
Option	Description									
<i>enable</i>	Turn off FortiGuard antivirus service.									
<i>disable</i>	Allow the FortiGuard antivirus service.									
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard antivirus caching.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard antivirus caching.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard antivirus caching.	<i>disable</i>	Disable FortiGuard antivirus caching.			
Option	Description									
<i>enable</i>	Enable FortiGuard antivirus caching.									
<i>disable</i>	Disable FortiGuard antivirus caching.									



Parameter	Description	Type	Size	Default						
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries .	integer	Minimum value: 300 Maximum value: 86400	300						
outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use .	integer	Minimum value: 1 Maximum value: 15	2						
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	0						
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out .	integer	Minimum value: 1 Maximum value: 30	7						
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Turn off the FortiGuard web filtering service.</td> </tr> <tr> <td><i>disable</i></td> <td>Allow the FortiGuard web filtering service to operate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Turn off the FortiGuard web filtering service.	<i>disable</i>	Allow the FortiGuard web filtering service to operate.			
Option	Description									
<i>enable</i>	Turn off the FortiGuard web filtering service.									
<i>disable</i>	Allow the FortiGuard web filtering service to operate.									
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGuard web filter caching.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGuard web filter caching.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGuard web filter caching.	<i>disable</i>	Disable FortiGuard web filter caching.			
Option	Description									
<i>enable</i>	Enable FortiGuard web filter caching.									
<i>disable</i>	Disable FortiGuard web filter caching.									
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds .	integer	Minimum value: 300 Maximum value: 86400	3600						

Parameter	Description	Type	Size	Default				
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295				
webfilter-expiration	Expiration date of the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0				
webfilter-timeout	Web filter query time out .	integer	Minimum value: 1 Maximum value: 30	15				
sdns-server-ip	IP address of the FortiGuard DNS rating server.	user	Not Specified					
sdns-server-port	Port to connect to on the FortiGuard DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	53				
anycast-sdns-server-ip	IP address of the FortiGuard anycast DNS rating server.	ipv4-address	Not Specified	0.0.0.0				
anycast-sdns-server-port	Port to connect to on the FortiGuard anycast DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	853				
sdns-options	Customization options for the FortiGuard DNS service.	option	-					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>include-question-section</i></td> <td>Include DNS question section in the FortiGuard DNS setup message.</td> </tr> </tbody> </table>		Option	Description	<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.		
Option	Description							
<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.							
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified	0.0.0.0				
source-ip6	Source IPv6 address used to communicate with FortiGuard.	ipv6-address	Not Specified	::				
proxy-server-ip	IP address of the proxy server.	ipv4-address	Not Specified	0.0.0.0				

Parameter	Description	Type	Size	Default								
proxy-server-port	Port used to communicate with the proxy server.	integer	Minimum value: 0 Maximum value: 65535	0								
proxy-username	Proxy user name.	string	Maximum length: 64									
proxy-password	Proxy user password.	password	Not Specified									
ddns-server-ip	IP address of the FortiDDNS server.	ipv4-address	Not Specified	0.0.0.0								
ddns-server-port	Port used to communicate with FortiDDNS servers.	integer	Minimum value: 1 Maximum value: 65535	443								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>		Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

\* This parameter may not exist in some models.

## config system ips

Configure IPS system settings.

```

config system ips
  Description: Configure IPS system settings.
  set signature-hold-time {user}
  set override-signature-hold-by-id [enable|disable]
end

```

## config system ips

Parameter	Description	Type	Size	Default
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h> .	user	Not Specified	0h
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable

Option	Description
<i>enable</i>	Allow the signatures specified by IDs to be triggered even if they are on hold.
<i>disable</i>	Do not trigger the signatures that are on hold.

## config system arp

IPv4 ARP table.

```
config system arp
  Description: IPv4 ARP table.
end
```

## config system email-server

Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features.

```
config system email-server
  Description: Configure the email server used by the FortiGate various things. For
  example, for sending email messages to users to support user authentication
  features.
  set type {option}
  set reply-to {string}
  set server {string}
  set port {integer}
  set source-ip {ipv4-address}
  set source-ip6 {ipv6-address}
  set authenticate [enable|disable]
  set validate-server [enable|disable]
  set username {string}
  set password {password}
  set security [none|starttls|...]
  set ssl-min-proto-version [default|SSLv3|...]
end
```

## config system email-server

Parameter	Description	Type	Size	Default						
type	Use FortiGuard Message service or custom email server.	option	-	custom						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>custom</i></td> <td>Use custom email server.</td> </tr> </tbody> </table>	Option	Description	<i>custom</i>	Use custom email server.					
Option	Description									
<i>custom</i>	Use custom email server.									
reply-to	Reply-To email address.	string	Maximum length: 63							
server	SMTP server IP address or hostname.	string	Maximum length: 63							
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535	25						
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified	::						
authenticate	Enable/disable authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.			
Option	Description									
<i>enable</i>	Enable authentication.									
<i>disable</i>	Disable authentication.									
validate-server	Enable/disable validation of server certificate.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable validation of server certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable validation of server certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable validation of server certificate.	<i>disable</i>	Disable validation of server certificate.			
Option	Description									
<i>enable</i>	Enable validation of server certificate.									
<i>disable</i>	Disable validation of server certificate.									
username	SMTP server user name for authentication.	string	Maximum length: 63							
password	SMTP server user password for authentication.	password	Not Specified							
security	Connection security used by the email server.	option	-	none						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>starttls</i></td> <td>STARTTLS.</td> </tr> <tr> <td><i>smtps</i></td> <td>SSL/TLS.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>starttls</i>	STARTTLS.	<i>smtps</i>	SSL/TLS.							
Option	Description															
<i>none</i>	None.															
<i>starttls</i>	STARTTLS.															
<i>smtps</i>	SSL/TLS.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

## config system alarm

Configure alarm.

```

config system alarm
  Description: Configure alarm.
  set status [enable|disable]
  set audible [enable|disable]
  config groups
    Description: Alarm groups.
    edit <id>
      set period {integer}
      set admin-auth-failure-threshold {integer}
      set admin-auth-lockout-threshold {integer}
      set user-auth-failure-threshold {integer}
      set user-auth-lockout-threshold {integer}
      set replay-attempt-threshold {integer}
      set self-test-failure-threshold {integer}
      set log-full-warning-threshold {integer}
      set encryption-failure-threshold {integer}
      set decryption-failure-threshold {integer}
      config fw-policy-violations
        Description: Firewall policy violations.
        edit <id>
          set threshold {integer}
          set src-ip {ipv4-address}
          set dst-ip {ipv4-address}
          set src-port {integer}
          set dst-port {integer}
        next
      end
    end
  end

```

```

    set fw-policy-id {integer}
    set fw-policy-id-threshold {integer}
  next
end
end

```

## config system alarm

Parameter	Description	Type	Size	Default						
status	Enable/disable alarm.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable alarm.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable alarm.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable alarm.	<i>disable</i>	Disable alarm.			
Option	Description									
<i>enable</i>	Enable alarm.									
<i>disable</i>	Disable alarm.									
audible	Enable/disable audible alarm.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable audible alarm.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable audible alarm.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable audible alarm.	<i>disable</i>	Disable audible alarm.			
Option	Description									
<i>enable</i>	Enable audible alarm.									
<i>disable</i>	Disable audible alarm.									

## config groups

Parameter	Description	Type	Size	Default
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
user-auth-failure-threshold	User authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0

Parameter	Description	Type	Size	Default
user-auth-lockout-threshold	User authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
replay-attempt-threshold	Replay attempt threshold.	integer	Minimum value: 0 Maximum value: 1024	0
self-test-failure-threshold	Self-test failure threshold.	integer	Minimum value: 0 Maximum value: 1	0
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024	0
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
decryption-failure-threshold	Decryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
fw-policy-id	Firewall policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
fw-policy-id-threshold	Firewall policy ID threshold.	integer	Minimum value: 0 Maximum value: 1024	0

### config fw-policy-violations

Parameter	Description	Type	Size	Default
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024	0



Parameter	Description	Type	Size	Default
src-ip	Source IP (0=all).	ipv4-address	Not Specified	0.0.0.0
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified	0.0.0.0
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0

## config system mac-address-table

Configure MAC address tables.

```
config system mac-address-table
  Description: Configure MAC address tables.
  edit <mac>
    set interface {string}
    set reply-substitute {mac-address}
  next
end
```

## config system mac-address-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified	00:00:00:00:00:00

## config system session-helper

Configure session helper.

```
config system session-helper
  Description: Configure session helper.
  edit <id>
    set name [ftp|tftp|...]
    set protocol {integer}
    set port {integer}
```

```
next
end
```

## config system session-helper

Parameter	Description	Type	Size	Default																																
name	Helper name.	option	-																																	
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>tftp</i></td><td>TFTP.</td></tr><tr><td><i>ras</i></td><td>RAS.</td></tr><tr><td><i>h323</i></td><td>H323.</td></tr><tr><td><i>tns</i></td><td>TNS.</td></tr><tr><td><i>mms</i></td><td>MMS.</td></tr><tr><td><i>sip</i></td><td>SIP.</td></tr><tr><td><i>pptp</i></td><td>PPTP.</td></tr><tr><td><i>rtsp</i></td><td>RTSP.</td></tr><tr><td><i>dns-udp</i></td><td>DNS UDP.</td></tr><tr><td><i>dns-tcp</i></td><td>DNS TCP.</td></tr><tr><td><i>pmap</i></td><td>PMAP.</td></tr><tr><td><i>rsh</i></td><td>RSH.</td></tr><tr><td><i>dcerpc</i></td><td>DCERPC.</td></tr><tr><td><i>mgcp</i></td><td>MGCP.</td></tr></tbody></table>	Option	Description	<i>ftp</i>	FTP.	<i>tftp</i>	TFTP.	<i>ras</i>	RAS.	<i>h323</i>	H323.	<i>tns</i>	TNS.	<i>mms</i>	MMS.	<i>sip</i>	SIP.	<i>pptp</i>	PPTP.	<i>rtsp</i>	RTSP.	<i>dns-udp</i>	DNS UDP.	<i>dns-tcp</i>	DNS TCP.	<i>pmap</i>	PMAP.	<i>rsh</i>	RSH.	<i>dcerpc</i>	DCERPC.	<i>mgcp</i>	MGCP.			
Option	Description																																			
<i>ftp</i>	FTP.																																			
<i>tftp</i>	TFTP.																																			
<i>ras</i>	RAS.																																			
<i>h323</i>	H323.																																			
<i>tns</i>	TNS.																																			
<i>mms</i>	MMS.																																			
<i>sip</i>	SIP.																																			
<i>pptp</i>	PPTP.																																			
<i>rtsp</i>	RTSP.																																			
<i>dns-udp</i>	DNS UDP.																																			
<i>dns-tcp</i>	DNS TCP.																																			
<i>pmap</i>	PMAP.																																			
<i>rsh</i>	RSH.																																			
<i>dcerpc</i>	DCERPC.																																			
<i>mgcp</i>	MGCP.																																			
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0																																
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0																																

## config system proxy-arp

Configure proxy-ARP.

```
config system proxy-arp
```

```

Description: Configure proxy-ARP.
edit <id>
    set interface {string}
    set ip {ipv4-address}
    set end-ip {ipv4-address}
next
end

```

## config system proxy-arp

Parameter	Description	Type	Size	Default
interface	Interface acting proxy-ARP.	string	Maximum length: 15	
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified	0.0.0.0
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified	0.0.0.0

## config system fips-cc

Configure FIPS-CC mode.

```

config system fips-cc
Description: Configure FIPS-CC mode.
set status [enable|disable]
set entropy-token [enable|disable|...]
set self-test-period {integer}
set key-generation-self-test [enable|disable]
end

```

## config system fips-cc

Parameter	Description	Type	Size	Default						
status	Enable/disable/fips-ciphers	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FIPS-CC mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FIPS-CC mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FIPS-CC mode.	<i>disable</i>	Disable FIPS-CC mode.			
Option	Description									
<i>enable</i>	Enable FIPS-CC mode.									
<i>disable</i>	Disable FIPS-CC mode.									
entropy-token	Enable/disable/dynamic entropy token.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable entropy token to be present during boot process.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable entropy token to be present during boot process.					
Option	Description									
<i>enable</i>	Enable entropy token to be present during boot process.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable entropy token to be present during boot process.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Dynamic detect entropy token to be present during boot process.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable entropy token to be present during boot process.	<i>dynamic</i>	Dynamic detect entropy token to be present during boot process.			
Option	Description									
<i>disable</i>	Disable entropy token to be present during boot process.									
<i>dynamic</i>	Dynamic detect entropy token to be present during boot process.									
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440	1440						
key-generation-self-test	Enable/disable self tests after key generation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable self tests after key generation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable self tests after key generation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable self tests after key generation.	<i>disable</i>	Disable self tests after key generation.			
Option	Description									
<i>enable</i>	Enable self tests after key generation.									
<i>disable</i>	Disable self tests after key generation.									

## config system tos-based-priority

Configure Type of Service (ToS) based priority table to set network traffic priorities.

```

config system tos-based-priority
  Description: Configure Type of Service (ToS) based priority table to set network traffic
  priorities.
  edit <id>
    set tos {integer}
    set priority [low|medium|...]
  next
end

```

## config system tos-based-priority

Parameter	Description	Type	Size	Default				
tos	Value of the ToS byte in the IP datagram header .	integer	Minimum value: 0 Maximum value: 15	0				
priority	ToS based priority level to low, medium or high .	option	-	high				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Low priority.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Low priority.			
Option	Description							
<i>low</i>	Low priority.							

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		

## config system dscp-based-priority

Configure DSCP based priority table.

```
config system dscp-based-priority
  Description: Configure DSCP based priority table.
  edit <id>
    set ds {integer}
    set priority [low|medium|...]
  next
end
```

## config system dscp-based-priority

Parameter	Description	Type	Size	Default
ds	DSCP.	integer	Minimum value: 0 Maximum value: 63	0
priority	DSCP based priority level.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		

## config system probe-response

Configure system probe response.

```
config system probe-response
  Description: Configure system probe response.
  set port {integer}
  set http-probe-value {string}
  set ttl-mode [reinit|decrease|...]
  set mode [none|http-probe|...]
  set security-mode [none|authentication]
  set password {password}
  set timeout {integer}
```

end

## config system probe-response

Parameter	Description	Type	Size	Default
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535	8008
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024	OK
ttl-mode	Mode for TWAMP packet TTL modification.	option	-	retain
	<b>Option</b>	<b>Description</b>		
	<i>reinit</i>	Reinitialize TTL.		
	<i>decrease</i>	Decrease TTL.		
mode	SLA response mode.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Disable probe.		
	<i>http-probe</i>	HTTP probe.		
security-mode	Twamp responder security mode.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Unauthenticated mode.		
password	Twamp responder password in authentication mode	password	Not Specified	
	<i>authentication</i>	Authenticated mode.		
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600	300

## config system link-monitor

Configure Link Health Monitor.

```

config system link-monitor
  Description: Configure Link Health Monitor.
  edit <name>
    set addr-mode [ipv4|ipv6]
    set srcintf {string}
    set server <address1>, <address2>, ...
    set protocol {option1}, {option2}, ...
    set port {integer}
    set gateway-ip {ipv4-address-any}
    set gateway-ip6 {ipv6-address}
    set source-ip {ipv4-address-any}
    set source-ip6 {ipv6-address}
    set http-get {string}
    set http-agent {string}
    set http-match {string}
    set interval {integer}
    set probe-timeout {integer}
    set failtime {integer}
    set recoverytime {integer}
    set probe-count {integer}
    set security-mode [none|authentication]
    set password {password}
    set packet-size {integer}
    set ha-priority {integer}
    set update-cascade-interface [enable|disable]
    set update-static-route [enable|disable]
    set status [enable|disable]
  next
end

```

## config system link-monitor

Parameter	Description	Type	Size	Default						
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>IPv4 mode.</td> </tr> <tr> <td><i>ipv6</i></td> <td>IPv6 mode.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	IPv4 mode.	<i>ipv6</i>	IPv6 mode.			
Option	Description									
<i>ipv4</i>	IPv4 mode.									
<i>ipv6</i>	IPv6 mode.									
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15							
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79							
protocol	Protocols used to monitor the server.	option	-	ping						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>PING link monitor.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	PING link monitor.					
Option	Description									
<i>ping</i>	PING link monitor.									

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp-echo</i></td> <td>TCP echo link monitor.</td> </tr> <tr> <td><i>udp-echo</i></td> <td>UDP echo link monitor.</td> </tr> <tr> <td><i>http</i></td> <td>HTTP-GET link monitor.</td> </tr> <tr> <td><i>twamp</i></td> <td>TWAMP link monitor.</td> </tr> </tbody> </table>	Option	Description	<i>tcp-echo</i>	TCP echo link monitor.	<i>udp-echo</i>	UDP echo link monitor.	<i>http</i>	HTTP-GET link monitor.	<i>twamp</i>	TWAMP link monitor.			
Option	Description													
<i>tcp-echo</i>	TCP echo link monitor.													
<i>udp-echo</i>	UDP echo link monitor.													
<i>http</i>	HTTP-GET link monitor.													
<i>twamp</i>	TWAMP link monitor.													
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0										
gateway-ip	Gateway IP address used to probe the server.	ipv4-address-any	Not Specified	0.0.0.0										
gateway-ip6	Gateway IPv6 address used to probe the server.	ipv6-address	Not Specified	::										
source-ip	Source IP address used in packet to the server.	ipv4-address-any	Not Specified	0.0.0.0										
source-ip6	Source IPv6 address used in packet to the server.	ipv6-address	Not Specified	::										
http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.	string	Maximum length: 1024	/										
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/Safari/										
http-match	String that you expect to see in the HTTP-GET requests of the traffic to be monitored.	string	Maximum length: 1024											
interval	Detection interval in milliseconds .	integer	Minimum value: 500 Maximum value: 3600000	500										
probe-timeout	Time to wait before a probe packet is considered lost .	integer	Minimum value: 500 Maximum value: 5000	500										



Parameter	Description	Type	Size	Default						
failtime	Number of retry attempts before the server is considered down	integer	Minimum value: 1 Maximum value: 3600	5						
recoverytime	Number of successful responses received before server is considered recovered .	integer	Minimum value: 1 Maximum value: 3600	5						
probe-count	Number of most recent probes that should be used to calculate latency and jitter .	integer	Minimum value: 5 Maximum value: 30	30						
security-mode	Twamp controller security mode.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Unauthenticated mode.</td> </tr> <tr> <td><i>authentication</i></td> <td>Authenticated mode.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.			
Option	Description									
<i>none</i>	Unauthenticated mode.									
<i>authentication</i>	Authenticated mode.									
password	Twamp controller password in authentication mode	password	Not Specified							
packet-size	Packet size of a twamp test session,	integer	Minimum value: 64 Maximum value: 1024	64						
ha-priority	HA election priority .	integer	Minimum value: 1 Maximum value: 50	1						
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable update cascade interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable update cascade interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable update cascade interface.	<i>disable</i>	Disable update cascade interface.			
Option	Description									
<i>enable</i>	Enable update cascade interface.									
<i>disable</i>	Disable update cascade interface.									
update-static-route	Enable/disable updating the static route.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable updating the static route.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable updating the static route.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable updating the static route.	<i>disable</i>	Disable updating the static route.			
Option	Description									
<i>enable</i>	Enable updating the static route.									
<i>disable</i>	Disable updating the static route.									
status	Enable/disable this link monitor.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this link monitor.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this link monitor.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this link monitor.	<i>disable</i>	Disable this link monitor.			
Option	Description									
<i>enable</i>	Enable this link monitor.									
<i>disable</i>	Disable this link monitor.									

## config system auto-install

Configure USB auto installation.

```

config system auto-install
  Description: Configure USB auto installation.
  set auto-install-config [enable|disable]
  set auto-install-image [enable|disable]
  set default-config-file {string}
  set default-image-file {string}
end

```

## config system auto-install

Parameter	Description	Type	Size	Default						
auto-install-config	Enable/disable auto install the config in USB disk.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable config.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable config.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.			
Option	Description									
<i>enable</i>	Enable config.									
<i>disable</i>	Disable config.									
auto-install-image	Enable/disable auto install the image in USB disk.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable config.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable config.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.			
Option	Description									
<i>enable</i>	Enable config.									
<i>disable</i>	Disable config.									
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fgt_system.conf						

Parameter	Description	Type	Size	Default
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out

## config system console

Configure console.

```
config system console
  Description: Configure console.
  set mode [batch|line]
  set baudrate [9600|19200|...]
  set output [standard|more]
  set login [enable|disable]
  set fortixplorer [enable|disable]
end
```

## config system console

Parameter	Description	Type	Size	Default												
mode	Console mode.	option	-	line												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>batch</i></td> <td>Batch mode.</td> </tr> <tr> <td><i>line</i></td> <td>Line mode.</td> </tr> </tbody> </table>	Option	Description	<i>batch</i>	Batch mode.	<i>line</i>	Line mode.									
Option	Description															
<i>batch</i>	Batch mode.															
<i>line</i>	Line mode.															
baudrate	Console baud rate.	option	-	9600												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>9600</i></td> <td>9600</td> </tr> <tr> <td><i>19200</i></td> <td>19200</td> </tr> <tr> <td><i>38400</i></td> <td>38400</td> </tr> <tr> <td><i>57600</i></td> <td>57600</td> </tr> <tr> <td><i>115200</i></td> <td>115200</td> </tr> </tbody> </table>	Option	Description	<i>9600</i>	9600	<i>19200</i>	19200	<i>38400</i>	38400	<i>57600</i>	57600	<i>115200</i>	115200			
Option	Description															
<i>9600</i>	9600															
<i>19200</i>	19200															
<i>38400</i>	38400															
<i>57600</i>	57600															
<i>115200</i>	115200															
output	Console output mode.	option	-	more												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standard</i></td> <td>Standard output.</td> </tr> <tr> <td><i>more</i></td> <td>More page output.</td> </tr> </tbody> </table>	Option	Description	<i>standard</i>	Standard output.	<i>more</i>	More page output.									
Option	Description															
<i>standard</i>	Standard output.															
<i>more</i>	More page output.															
login	Enable/disable serial console and FortiExplorer.	option	-	enable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Console login enable.</td> </tr> <tr> <td><i>disable</i></td> <td>Console login disable.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Console login enable.	<i>disable</i>	Console login disable.			
Option	Description									
<i>enable</i>	Console login enable.									
<i>disable</i>	Console login disable.									
fortiexplorer *	Enable/disable access for FortiExplorer.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiExplorer access.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiExplorer access.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiExplorer access.	<i>disable</i>	Disable FortiExplorer access.			
Option	Description									
<i>enable</i>	Enable FortiExplorer access.									
<i>disable</i>	Disable FortiExplorer access.									

\* This parameter may not exist in some models.

## config system ntp

Configure system NTP information.

```

config system ntp
  Description: Configure system NTP information.
  set ntpsync [enable|disable]
  set type [fortiguard|custom]
  set syncinterval {integer}
  config ntpserver
    Description: Configure the FortiGate to connect to any available third-party NTP
    server.
    edit <id>
      set server {string}
      set ntpv3 [enable|disable]
      set authentication [enable|disable]
      set key {password}
      set key-id {integer}
      set interface-select-method [auto|sdwan|...]
      set interface {string}
    next
  end
  set source-ip {ipv4-address}
  set source-ip6 {ipv6-address}
  set server-mode [enable|disable]
  set authentication [enable|disable]
  set key-type [MD5|SHA1]
  set key {password}
  set key-id {integer}
  set interface <interface-name1>, <interface-name2>, ...
end

```

## config system ntp

Parameter	Description	Type	Size	Default						
ntpsync	Enable/disable setting the FortiGate system time by synchronizing with an NTP Server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable synchronization with NTP Server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable synchronization with NTP Server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable synchronization with NTP Server.	<i>disable</i>	Disable synchronization with NTP Server.			
Option	Description									
<i>enable</i>	Enable synchronization with NTP Server.									
<i>disable</i>	Disable synchronization with NTP Server.									
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-	fortiguard						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard</i></td> <td>Use the FortiGuard NTP server.</td> </tr> <tr> <td><i>custom</i></td> <td>Use any other available NTP server.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard</i>	Use the FortiGuard NTP server.	<i>custom</i>	Use any other available NTP server.			
Option	Description									
<i>fortiguard</i>	Use the FortiGuard NTP server.									
<i>custom</i>	Use any other available NTP server.									
syncinterval	NTP synchronization interval .	integer	Minimum value: 1 Maximum value: 1440	60						
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address for communication to the NTP server.	ipv6-address	Not Specified	::						
server-mode	Enable/disable FortiGate NTP Server Mode. Your FortiGate becomes an NTP server for other devices on your network. The FortiGate relays NTP requests to its configured NTP server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiGate NTP Server Mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiGate NTP Server Mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiGate NTP Server Mode.	<i>disable</i>	Disable FortiGate NTP Server Mode.			
Option	Description									
<i>enable</i>	Enable FortiGate NTP Server Mode.									
<i>disable</i>	Disable FortiGate NTP Server Mode.									
authentication	Enable/disable authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.			
Option	Description									
<i>enable</i>	Enable authentication.									
<i>disable</i>	Disable authentication.									
key-type	Key type for authentication (MD5, SHA1).	option	-	MD5						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>MD5</i></td> <td>Use MD5 to authenticate the message.</td> </tr> <tr> <td><i>SHA1</i></td> <td>Use SHA1 to authenticate the message.</td> </tr> </tbody> </table>	Option	Description	<i>MD5</i>	Use MD5 to authenticate the message.	<i>SHA1</i>	Use SHA1 to authenticate the message.			
Option	Description									
<i>MD5</i>	Use MD5 to authenticate the message.									
<i>SHA1</i>	Use SHA1 to authenticate the message.									
key	Key for authentication.	password	Not Specified							
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0						
interface <interface-name>	FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79							

### config ntpserver

Parameter	Description	Type	Size	Default						
server	IP address or hostname of the NTP Server.	string	Maximum length: 63							
ntp3	Enable to use NTPv3 instead of NTPv4.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NTPv3.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NTPv3 (use NTPv4).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NTPv3.	<i>disable</i>	Disable NTPv3 (use NTPv4).			
Option	Description									
<i>enable</i>	Enable NTPv3.									
<i>disable</i>	Disable NTPv3 (use NTPv4).									
authentication	Enable/disable MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MD5(NTPv3)/SHA1(NTPv4) authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MD5(NTPv3)/SHA1(NTPv4) authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.	<i>disable</i>	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.			
Option	Description									
<i>enable</i>	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.									
<i>disable</i>	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.									
key	Key for MD5(NTPv3)/SHA1(NTPv4) authentication.	password	Not Specified							
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config system ptp

Configure system PTP information.

```
config system ptp
  Description: Configure system PTP information.
  set status [enable|disable]
  set mode [multicast|hybrid]
  set delay-mechanism [E2E|P2P]
  set request-interval {integer}
  set interface {string}
end
```

## config system ptp

Parameter	Description	Type	Size	Default						
status	Enable/disable setting the FortiGate system time by synchronizing with an PTP Server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable synchronization with PTP Server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable synchronization with PTP Server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable synchronization with PTP Server.	<i>disable</i>	Disable synchronization with PTP Server.			
Option	Description									
<i>enable</i>	Enable synchronization with PTP Server.									
<i>disable</i>	Disable synchronization with PTP Server.									
mode	Multicast transmission or hybrid transmission.	option	-	multicast						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>multicast</i></td> <td>Send PTP packets with multicast.</td> </tr> <tr> <td><i>hybrid</i></td> <td>Send PTP packets with unicast and multicast.</td> </tr> </tbody> </table>	Option	Description	<i>multicast</i>	Send PTP packets with multicast.	<i>hybrid</i>	Send PTP packets with unicast and multicast.			
Option	Description									
<i>multicast</i>	Send PTP packets with multicast.									
<i>hybrid</i>	Send PTP packets with unicast and multicast.									
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>E2E</i></td> <td>End to end delay detection.</td> </tr> <tr> <td><i>P2P</i></td> <td>Peer to peer delay detection.</td> </tr> </tbody> </table>	Option	Description	<i>E2E</i>	End to end delay detection.	<i>P2P</i>	Peer to peer delay detection.			
Option	Description									
<i>E2E</i>	End to end delay detection.									
<i>P2P</i>	Peer to peer delay detection.									
request-interval	The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.	integer	Minimum value: 1 Maximum value: 6	1						
interface	PTP slave will reply through this interface.	string	Maximum length: 15							

## config system wccp

Configure WCCP.

```

config system wccp
  Description: Configure WCCP.
  edit <service-id>
    set router-id {ipv4-address}
    set cache-id {ipv4-address}
    set group-address {ipv4-address-multicast}
    set server-list {user}
    set router-list {user}
    set ports-defined [source|destination]
    set server-type [forward|proxy]
    set ports {user}
    set authentication [enable|disable]
    set password {password}
    set forward-method [GRE|L2|...]
    set cache-engine-method [GRE|L2]
    set service-type [auto|standard|...]
    set primary-hash {option1}, {option2}, ...
    set priority {integer}
    set protocol {integer}
    set assignment-weight {integer}
    set assignment-bucket-format [wccp-v2|cisco-implementation]
    set return-method [GRE|L2|...]
    set assignment-method [HASH|MASK|...]
    set assignment-srcaddr-mask {ipv4-netmask-any}
    set assignment-dstaddr-mask {ipv4-netmask-any}
  next
end

```



## config system wccp

Parameter	Description	Type	Size	Default						
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiGate interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0						
cache-id	IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0						
group-address	IP multicast address used by the cache routers. For the FortiGate to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified	0.0.0.0						
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified							
router-list	IP addresses of one or more WCCP routers.	user	Not Specified							
ports-defined	Match method.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>source</i></td> <td>Source port match.</td> </tr> <tr> <td><i>destination</i></td> <td>Destination port match.</td> </tr> </tbody> </table>	Option	Description	<i>source</i>	Source port match.	<i>destination</i>	Destination port match.			
Option	Description									
<i>source</i>	Source port match.									
<i>destination</i>	Destination port match.									
server-type	Cache server type.	option	-	forward						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>forward</i></td> <td>Forward server.</td> </tr> <tr> <td><i>proxy</i></td> <td>Proxy server.</td> </tr> </tbody> </table>	Option	Description	<i>forward</i>	Forward server.	<i>proxy</i>	Proxy server.			
Option	Description									
<i>forward</i>	Forward server.									
<i>proxy</i>	Proxy server.									
ports	Service ports.	user	Not Specified							
authentication	Enable/disable MD5 authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MD5 authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MD5 authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MD5 authentication.	<i>disable</i>	Disable MD5 authentication.			
Option	Description									
<i>enable</i>	Enable MD5 authentication.									
<i>disable</i>	Disable MD5 authentication.									
password	Password for MD5 authentication.	password	Not Specified							
forward-method	Method used to forward traffic to the cache servers.	option	-	GRE						

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>GRE</i></td> <td>GRE encapsulation.</td> </tr> <tr> <td><i>L2</i></td> <td>L2 rewrite.</td> </tr> <tr> <td><i>any</i></td> <td>GRE or L2.</td> </tr> </tbody> </table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.	<i>any</i>	GRE or L2.					
Option	Description													
<i>GRE</i>	GRE encapsulation.													
<i>L2</i>	L2 rewrite.													
<i>any</i>	GRE or L2.													
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-	GRE										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>GRE</i></td> <td>GRE encapsulation.</td> </tr> <tr> <td><i>L2</i></td> <td>L2 rewrite.</td> </tr> </tbody> </table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.							
Option	Description													
<i>GRE</i>	GRE encapsulation.													
<i>L2</i>	L2 rewrite.													
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-	auto										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>auto</td> </tr> <tr> <td><i>standard</i></td> <td>Standard service.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Dynamic service.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	auto	<i>standard</i>	Standard service.	<i>dynamic</i>	Dynamic service.					
Option	Description													
<i>auto</i>	auto													
<i>standard</i>	Standard service.													
<i>dynamic</i>	Dynamic service.													
primary-hash	Hash method.	option	-	dst-ip										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>src-ip</i></td> <td>Source IP hash.</td> </tr> <tr> <td><i>dst-ip</i></td> <td>Destination IP hash.</td> </tr> <tr> <td><i>src-port</i></td> <td>Source port hash.</td> </tr> <tr> <td><i>dst-port</i></td> <td>Destination port hash.</td> </tr> </tbody> </table>	Option	Description	<i>src-ip</i>	Source IP hash.	<i>dst-ip</i>	Destination IP hash.	<i>src-port</i>	Source port hash.	<i>dst-port</i>	Destination port hash.			
Option	Description													
<i>src-ip</i>	Source IP hash.													
<i>dst-ip</i>	Destination IP hash.													
<i>src-port</i>	Source port hash.													
<i>dst-port</i>	Destination port hash.													
priority	Service priority.	integer	Minimum value: 0 Maximum value: 255	0										
protocol	Service protocol.	integer	Minimum value: 0 Maximum value: 255	0										

Parameter	Description	Type	Size	Default								
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255	0								
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-	cisco-implementation								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wccp-v2</i></td> <td>WCCP-v2 bucket format.</td> </tr> <tr> <td><i>cisco-implementation</i></td> <td>Cisco bucket format.</td> </tr> </tbody> </table>	Option	Description	<i>wccp-v2</i>	WCCP-v2 bucket format.	<i>cisco-implementation</i>	Cisco bucket format.					
Option	Description											
<i>wccp-v2</i>	WCCP-v2 bucket format.											
<i>cisco-implementation</i>	Cisco bucket format.											
return-method	Method used to decline a redirected packet and return it to the FortiGate.	option	-	GRE								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>GRE</i></td> <td>GRE encapsulation.</td> </tr> <tr> <td><i>L2</i></td> <td>L2 rewrite.</td> </tr> <tr> <td><i>any</i></td> <td>GRE or L2.</td> </tr> </tbody> </table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.	<i>any</i>	GRE or L2.			
Option	Description											
<i>GRE</i>	GRE encapsulation.											
<i>L2</i>	L2 rewrite.											
<i>any</i>	GRE or L2.											
assignment-method	Hash key assignment preference.	option	-	HASH								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>HASH</i></td> <td>HASH assignment method.</td> </tr> <tr> <td><i>MASK</i></td> <td>MASK assignment method.</td> </tr> <tr> <td><i>any</i></td> <td>HASH or MASK.</td> </tr> </tbody> </table>	Option	Description	<i>HASH</i>	HASH assignment method.	<i>MASK</i>	MASK assignment method.	<i>any</i>	HASH or MASK.			
Option	Description											
<i>HASH</i>	HASH assignment method.											
<i>MASK</i>	MASK assignment method.											
<i>any</i>	HASH or MASK.											
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified	0.0.23.65								
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified	0.0.0.0								

## config system nat64

Configure NAT64.

```

config system nat64
  Description: Configure NAT64.
  set status [enable|disable]
  set nat64-prefix {ipv6-prefix}
  set secondary-prefix-status [enable|disable]
  config secondary-prefix

```

```

Description: Secondary NAT64 prefix.
edit <name>
    set nat64-prefix {ipv6-prefix}
next
end
set always-synthesize-aaaa-record [enable|disable]
set generate-ipv6-fragment-header [enable|disable]
set nat46-force-ipv4-packet-forwarding [enable|disable]
end

```

## config system nat64

Parameter	Description	Type	Size	Default						
status	Enable/disable NAT64 .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NAT64.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NAT64.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NAT64.	<i>disable</i>	Disable NAT64.			
Option	Description									
<i>enable</i>	Enable NAT64.									
<i>disable</i>	Disable NAT64.									
nat64-prefix	NAT64 prefix must be ::/96 .	ipv6-prefix	Not Specified	64:ff9b::/96						
secondary-prefix-status	Enable/disable secondary NAT64 prefix.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable secondary NAT64.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable secondary NAT64.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable secondary NAT64.	<i>disable</i>	Disable secondary NAT64.			
Option	Description									
<i>enable</i>	Enable secondary NAT64.									
<i>disable</i>	Disable secondary NAT64.									
always-synthesize-aaaa-record	Enable/disable AAAA record synthesis .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AAAA record synthesis.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AAAA record synthesis.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AAAA record synthesis.	<i>disable</i>	Disable AAAA record synthesis.			
Option	Description									
<i>enable</i>	Enable AAAA record synthesis.									
<i>disable</i>	Disable AAAA record synthesis.									
generate-ipv6-fragment-header	Enable/disable IPv6 fragment header generation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPv6 fragment header generation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPv6 fragment header generation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPv6 fragment header generation.	<i>disable</i>	Disable IPv6 fragment header generation.			
Option	Description									
<i>enable</i>	Enable IPv6 fragment header generation.									
<i>disable</i>	Disable IPv6 fragment header generation.									

Parameter	Description	Type	Size	Default
nat46-force-ipv4-packet-forwarding	Enable/disable mandatory IPv4 packet forwarding in nat46.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.		
	<i>disable</i>	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.		

### config secondary-prefix

Parameter	Description	Type	Size	Default
nat64-prefix	NAT64 prefix.	ipv6-prefix	Not Specified	::/0

## config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
  Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server
  for this VDOM.
  edit <name>
    set status [enable|disable]
    set radius-server-vdom {string}
  next
end
```

### config system vdom-radius-server

Parameter	Description	Type	Size	Default
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the RSSO RADIUS server for this VDOM.		
	<i>disable</i>	Disable the RSSO RADIUS server for this VDOM.		
radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31	

---

## config system startup-error-log

Display startup config error on console.

```
config system startup-error-log
  Description: Display startup config error on console.
end
```

## config system source-ip status

Show configured service source-IP.

```
config system source-ip status
  Description: Show configured service source-IP.
end
```

## config system auto-update status

Status of automatic updates.

```
config system auto-update status
  Description: Status of automatic updates.
end
```

## config system auto-update versions

Update object versions.

```
config system auto-update versions
  Description: Update object versions.
end
```

## config system session-info list

List session.

```
config system session-info list
  Description: List session.
end
```

## config system session-info expectation

List expectation session.

```
config system session-info expectation
  Description: List expectation session.
end
```

---

## config system session-info full-stat

Fully stat session.

```
config system session-info full-stat
  Description: Fully stat session.
end
```

## config system session-info statistics

Session statistics.

```
config system session-info statistics
  Description: Session statistics.
end
```

## config system session-info ttl

TTL session.

```
config system session-info ttl
  Description: TTL session.
end
```

## config system session-helper-info list

List session helper.

```
config system session-helper-info list
  Description: List session helper.
end
```

## config system ip-conflict status

List interface names and IP addresses in conflict.

```
config system ip-conflict status
  Description: List interface names and IP addresses in conflict.
end
```

## config system ftm-push

Configure FortiToken Mobile push services.

```
config system ftm-push
  Description: Configure FortiToken Mobile push services.
  set server-port {integer}
  set server-cert {string}
  set server-ip {ipv4-address}
  set status [enable|disable]
end
```

## config system ftm-push

Parameter	Description	Type	Size	Default
server-port	Port to communicate with FortiToken Mobile push services server .	integer	Minimum value: 1 Maximum value: 65535	4433
server-cert	Name of the server certificate to be used for SSL .	string	Maximum length: 35	Fortinet_ Factory **
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable the use of FortiToken Mobile push services.	option	-	disable

Option	Description
<i>enable</i>	Enable FortiToken Mobile push services.
<i>disable</i>	Disable FortiToken Mobile push services.

\*\* Values may differ between models.

## config system geoip-override

Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.

```
config system geoip-override
  Description: Configure geographical location mapping for IP address(es) to override
  mappings from FortiGuard.
  edit <name>
    set description {string}
    set country-id {string}
    config ip-range
      Description: Table of IP ranges assigned to country.
      edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
      next
    end
    config ip6-range
      Description: Table of IPv6 ranges assigned to country.
      edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
      next
    end
  next
end
```



## config system geoiip-override

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
country-id	Two character Country ID code.	string	Maximum length: 2	

## config ip-range

Parameter	Description	Type	Size	Default
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
end-ip	Ending IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0

## config ip6-range

Parameter	Description	Type	Size	Default
start-ip	Starting IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
end-ip	Ending IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::

## config system fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
  Description: Configure FortiSandbox.
  set status [enable|disable]
  set server {string}
  set source-ip {string}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
  set enc-algorithm [default|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set email {string}
end
```

## config system fortisandbox

Parameter	Description	Type	Size	Default												
status	Enable/disable FortiSandbox.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiSandbox.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiSandbox.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiSandbox.	<i>disable</i>	Disable FortiSandbox.									
Option	Description															
<i>enable</i>	Enable FortiSandbox.															
<i>disable</i>	Disable FortiSandbox.															
server	Server address of the remote FortiSandbox.	string	Maximum length: 63													
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>SSL communication with high and medium encryption algorithms.</td> </tr> <tr> <td><i>high</i></td> <td>SSL communication with high encryption algorithms.</td> </tr> <tr> <td><i>low</i></td> <td>SSL communication with low encryption algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.							
Option	Description															
<i>default</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

Parameter	Description	Type	Size	Default
email	Notifier email address.	string	Maximum length: 63	

## config system vdom-exception

Global configuration objects that can be configured independently across different ha peers for all VDOMs or for the defined VDOM scope.

```
config system vdom-exception
  Description: Global configuration objects that can be configured independently across
              different ha peers for all VDOMs or for the defined VDOM scope.
  edit <id>
    set object [log.fortianalyzer.setting|log.fortianalyzer.override-setting|...]
    set scope [all|inclusive|...]
    set vdom <name1>, <name2>, ...
  next
end
```

## config system vdom-exception

Parameter	Description	Type	Size	Default
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>log.fortianalyzer.setting</i>	log.fortianalyzer.setting		
	<i>log.fortianalyzer.override-setting</i>	log.fortianalyzer.override-setting		
	<i>log.fortianalyzer2.setting</i>	log.fortianalyzer2.setting		
	<i>log.fortianalyzer2.override-setting</i>	log.fortianalyzer2.override-setting		
	<i>log.fortianalyzer3.setting</i>	log.fortianalyzer3.setting		
	<i>log.fortianalyzer3.override-setting</i>	log.fortianalyzer3.override-setting		
	<i>log.fortianalyzer-cloud.setting</i>	log.fortianalyzer-cloud.setting		
	<i>log.fortianalyzer-cloud.override-setting</i>	log.fortianalyzer-cloud.override-setting		
	<i>log.syslogd.setting</i>	log.syslogd.setting		

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>log.syslogd.override-setting</i></td> <td>log.syslogd.override-setting</td> </tr> <tr> <td><i>log.syslogd2.setting</i></td> <td>log.syslogd2.setting</td> </tr> <tr> <td><i>log.syslogd2.override-setting</i></td> <td>log.syslogd2.override-setting</td> </tr> <tr> <td><i>log.syslogd3.setting</i></td> <td>log.syslogd3.setting</td> </tr> <tr> <td><i>log.syslogd3.override-setting</i></td> <td>log.syslogd3.override-setting</td> </tr> <tr> <td><i>log.syslogd4.setting</i></td> <td>log.syslogd4.setting</td> </tr> <tr> <td><i>log.syslogd4.override-setting</i></td> <td>log.syslogd4.override-setting</td> </tr> <tr> <td><i>system.gre-tunnel</i></td> <td>system.gre-tunnel</td> </tr> <tr> <td><i>system.central-management</i></td> <td>system.central-management</td> </tr> <tr> <td><i>system.csf</i></td> <td>system.csf</td> </tr> <tr> <td><i>user.radius</i></td> <td>user.radius</td> </tr> </tbody> </table>	Option	Description	<i>log.syslogd.override-setting</i>	log.syslogd.override-setting	<i>log.syslogd2.setting</i>	log.syslogd2.setting	<i>log.syslogd2.override-setting</i>	log.syslogd2.override-setting	<i>log.syslogd3.setting</i>	log.syslogd3.setting	<i>log.syslogd3.override-setting</i>	log.syslogd3.override-setting	<i>log.syslogd4.setting</i>	log.syslogd4.setting	<i>log.syslogd4.override-setting</i>	log.syslogd4.override-setting	<i>system.gre-tunnel</i>	system.gre-tunnel	<i>system.central-management</i>	system.central-management	<i>system.csf</i>	system.csf	<i>user.radius</i>	user.radius			
Option	Description																											
<i>log.syslogd.override-setting</i>	log.syslogd.override-setting																											
<i>log.syslogd2.setting</i>	log.syslogd2.setting																											
<i>log.syslogd2.override-setting</i>	log.syslogd2.override-setting																											
<i>log.syslogd3.setting</i>	log.syslogd3.setting																											
<i>log.syslogd3.override-setting</i>	log.syslogd3.override-setting																											
<i>log.syslogd4.setting</i>	log.syslogd4.setting																											
<i>log.syslogd4.override-setting</i>	log.syslogd4.override-setting																											
<i>system.gre-tunnel</i>	system.gre-tunnel																											
<i>system.central-management</i>	system.central-management																											
<i>system.csf</i>	system.csf																											
<i>user.radius</i>	user.radius																											
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-	all																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>all</i></td> <td>Object configuration independent for all VDOMs.</td> </tr> <tr> <td><i>inclusive</i></td> <td>Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.</td> </tr> <tr> <td><i>exclusive</i></td> <td>Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.</td> </tr> </tbody> </table>	Option	Description	<i>all</i>	Object configuration independent for all VDOMs.	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.	<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.																			
Option	Description																											
<i>all</i>	Object configuration independent for all VDOMs.																											
<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.																											
<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.																											
vdom <name>	Names of the VDOMs. VDOM name.	string	Maximum length: 79																									

## config system csf

Add this FortiGate to a Security Fabric or set up a new Security Fabric on this FortiGate.

```
config system csf
  Description: Add this FortiGate to a Security Fabric or set up a new Security Fabric on
  this FortiGate.
  set status [enable|disable]
  set upstream-ip {ipv4-address}
  set upstream-port {integer}
  set group-name {string}
  set group-password {password}
  set accept-auth-by-cert [disable|enable]
```

```

set management-ip {string}
set management-port {integer}
set authorization-request-type [serial|certificate]
set certificate {string}
set fabric-workers {integer}
set configuration-sync [default|local]
set fabric-object-unification [default|local]
set saml-configuration-sync [default|local]
config trusted-list
  Description: Pre-authorized and blocked security fabric nodes.
  edit <name>
    set authorization-type [serial|certificate]
    set serial {string}
    set certificate {var-string}
    set action [accept|deny]
    set ha-members {string}
    set downstream-authorization [enable|disable]
  next
end
config fabric-device
  Description: Fabric device configuration.
  edit <name>
    set device-ip {ipv4-address}
    set https-port {integer}
    set access-token {varlen_password}
  next
end
end

```

## config system csf

Parameter	Description	Type	Size	Default
status	Enable/disable Security Fabric.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Security Fabric.		
	<i>disable</i>	Disable Security Fabric.		
upstream-ip	IP address of the FortiGate upstream from this FortiGate in the Security Fabric.	ipv4-address	Not Specified	0.0.0.0
upstream-port	The port number to use to communicate with the FortiGate upstream from this FortiGate in the Security Fabric .	integer	Minimum value: 1 Maximum value: 65535	8013
group-name	Security Fabric group name. All FortiGates in a Security Fabric must have the same group name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
group-password	Security Fabric group password. All FortiGates in a Security Fabric must have the same group password.	password	Not Specified							
accept-auth-by-cert	Accept connections with unknown certificates and ask admin for approval.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not accept SSL connections with unknown certificates.</td> </tr> <tr> <td><i>enable</i></td> <td>Accept SSL connections without automatic certificate verification.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not accept SSL connections with unknown certificates.	<i>enable</i>	Accept SSL connections without automatic certificate verification.			
Option	Description									
<i>disable</i>	Do not accept SSL connections with unknown certificates.									
<i>enable</i>	Accept SSL connections without automatic certificate verification.									
management-ip	Management IP address of this FortiGate. Used to log into this FortiGate from another FortiGate in the Security Fabric.	string	Maximum length: 255							
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 0 Maximum value: 65535	0						
authorization-request-type	Authorization request type.	option	-	serial						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>serial</i></td> <td>Request verification by serial number.</td> </tr> <tr> <td><i>certificate</i></td> <td>Request verification by certificate.</td> </tr> </tbody> </table>	Option	Description	<i>serial</i>	Request verification by serial number.	<i>certificate</i>	Request verification by certificate.			
Option	Description									
<i>serial</i>	Request verification by serial number.									
<i>certificate</i>	Request verification by certificate.									
certificate	Certificate.	string	Maximum length: 35							
fabric-workers	Number of worker processes for Security Fabric daemon.	integer	Minimum value: 1 Maximum value: 4	2						
configuration-sync	Configuration sync mode.	option	-	default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Synchronize configuration for FortiAnalyzer, FortiSandbox, and Central Management to root node.</td> </tr> <tr> <td><i>local</i></td> <td>Do not synchronize configuration with root node.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Synchronize configuration for FortiAnalyzer, FortiSandbox, and Central Management to root node.	<i>local</i>	Do not synchronize configuration with root node.			
Option	Description									
<i>default</i>	Synchronize configuration for FortiAnalyzer, FortiSandbox, and Central Management to root node.									
<i>local</i>	Do not synchronize configuration with root node.									
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Global CMDB objects will be synchronized in Security Fabric.</td> </tr> <tr> <td><i>local</i></td> <td>Global CMDB objects will not be synchronized to and from this device.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.	<i>local</i>	Global CMDB objects will not be synchronized to and from this device.			
Option	Description									
<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.									
<i>local</i>	Global CMDB objects will not be synchronized to and from this device.									
saml-configuration-sync	SAML setting configuration synchronization.	option	-	default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>SAML setting for fabric members is created by fabric root.</td> </tr> <tr> <td><i>local</i></td> <td>Do not apply SAML configuration generated by root.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	SAML setting for fabric members is created by fabric root.	<i>local</i>	Do not apply SAML configuration generated by root.			
Option	Description									
<i>default</i>	SAML setting for fabric members is created by fabric root.									
<i>local</i>	Do not apply SAML configuration generated by root.									

### config trusted-list

Parameter	Description	Type	Size	Default						
authorization-type	Authorization type.	option	-	serial						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>serial</i></td> <td>Verify downstream by serial number.</td> </tr> <tr> <td><i>certificate</i></td> <td>Verify downstream by certificate.</td> </tr> </tbody> </table>	Option	Description	<i>serial</i>	Verify downstream by serial number.	<i>certificate</i>	Verify downstream by certificate.			
Option	Description									
<i>serial</i>	Verify downstream by serial number.									
<i>certificate</i>	Verify downstream by certificate.									
serial	Serial.	string	Maximum length: 19							
certificate	Certificate.	var-string	Maximum length: 32767							
action	Security fabric authorization action.	option	-	accept						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Accept authorization request.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny authorization request.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Accept authorization request.	<i>deny</i>	Deny authorization request.			
Option	Description									
<i>accept</i>	Accept authorization request.									
<i>deny</i>	Deny authorization request.									
ha-members	HA members.	string	Maximum length: 19							
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable downstream authorization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable downstream authorization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable downstream authorization.	<i>disable</i>	Disable downstream authorization.			
Option	Description									
<i>enable</i>	Enable downstream authorization.									
<i>disable</i>	Disable downstream authorization.									

## config fabric-device

Parameter	Description	Type	Size	Default
device-ip	Device IP.	ipv4-address	Not Specified	0.0.0.0
https-port	HTTPS port for fabric device.	integer	Minimum value: 1 Maximum value: 65535	443
access-token	Device access token.	varlen_password	Not Specified	

## config system automation-trigger

Trigger for automation stitches.

```

config system automation-trigger
  Description: Trigger for automation stitches.
  edit <name>
    set trigger-type [event-based|scheduled]
    set event-type [ioc|event-log|...]
    set license-type [forticare-support|fortiguard-webfilter|...]
    set ioc-level [medium|high]
    set report-type [PostureReport|CoverageReport|...]
    set logid {integer}
    set trigger-frequency [hourly|daily|...]
    set trigger-weekday [sunday|monday|...]
    set trigger-day {integer}
    set trigger-hour {integer}
    set trigger-minute {integer}
  config fields
    Description: Customized trigger field settings.
    edit <id>
      set name {string}
      set value {var-string}
    next
  end
  set faz-event-name {var-string}
  set faz-event-severity {var-string}
  set faz-event-tags {var-string}
next
end

```



## config system automation-trigger

Parameter	Description	Type	Size	Default																										
trigger-type	Trigger type.	option	-	event-based																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>event-based</i></td> <td>Event based trigger.</td> </tr> <tr> <td><i>scheduled</i></td> <td>Scheduled trigger.</td> </tr> </tbody> </table>	Option	Description	<i>event-based</i>	Event based trigger.	<i>scheduled</i>	Scheduled trigger.																							
Option	Description																													
<i>event-based</i>	Event based trigger.																													
<i>scheduled</i>	Scheduled trigger.																													
event-type	Event type.	option	-	ioc																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ioc</i></td> <td>Indicator of compromise detected.</td> </tr> <tr> <td><i>event-log</i></td> <td>Use log ID as trigger.</td> </tr> <tr> <td><i>reboot</i></td> <td>Device reboot.</td> </tr> <tr> <td><i>low-memory</i></td> <td>Conserve mode due to low memory.</td> </tr> <tr> <td><i>high-cpu</i></td> <td>High CPU usage.</td> </tr> <tr> <td><i>license-near-expiry</i></td> <td>License near expiration date.</td> </tr> <tr> <td><i>ha-failover</i></td> <td>HA failover.</td> </tr> <tr> <td><i>config-change</i></td> <td>Configuration change.</td> </tr> <tr> <td><i>security-rating-summary</i></td> <td>Security rating summary.</td> </tr> <tr> <td><i>virus-ips-db-updated</i></td> <td>Virus and IPS database updated.</td> </tr> <tr> <td><i>faz-event</i></td> <td>FortiAnalyzer event.</td> </tr> <tr> <td><i>incoming-webhook</i></td> <td>Incoming webhook call.</td> </tr> </tbody> </table>	Option	Description	<i>ioc</i>	Indicator of compromise detected.	<i>event-log</i>	Use log ID as trigger.	<i>reboot</i>	Device reboot.	<i>low-memory</i>	Conserve mode due to low memory.	<i>high-cpu</i>	High CPU usage.	<i>license-near-expiry</i>	License near expiration date.	<i>ha-failover</i>	HA failover.	<i>config-change</i>	Configuration change.	<i>security-rating-summary</i>	Security rating summary.	<i>virus-ips-db-updated</i>	Virus and IPS database updated.	<i>faz-event</i>	FortiAnalyzer event.	<i>incoming-webhook</i>	Incoming webhook call.			
Option	Description																													
<i>ioc</i>	Indicator of compromise detected.																													
<i>event-log</i>	Use log ID as trigger.																													
<i>reboot</i>	Device reboot.																													
<i>low-memory</i>	Conserve mode due to low memory.																													
<i>high-cpu</i>	High CPU usage.																													
<i>license-near-expiry</i>	License near expiration date.																													
<i>ha-failover</i>	HA failover.																													
<i>config-change</i>	Configuration change.																													
<i>security-rating-summary</i>	Security rating summary.																													
<i>virus-ips-db-updated</i>	Virus and IPS database updated.																													
<i>faz-event</i>	FortiAnalyzer event.																													
<i>incoming-webhook</i>	Incoming webhook call.																													
license-type	License type.	option	-	forticare-support																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>forticare-support</i></td> <td>FortiCare support license.</td> </tr> <tr> <td><i>fortiguard-webfilter</i></td> <td>FortiGuard web filter license.</td> </tr> <tr> <td><i>fortiguard-antispam</i></td> <td>FortiGuard antispam license.</td> </tr> </tbody> </table>	Option	Description	<i>forticare-support</i>	FortiCare support license.	<i>fortiguard-webfilter</i>	FortiGuard web filter license.	<i>fortiguard-antispam</i>	FortiGuard antispam license.																					
Option	Description																													
<i>forticare-support</i>	FortiCare support license.																													
<i>fortiguard-webfilter</i>	FortiGuard web filter license.																													
<i>fortiguard-antispam</i>	FortiGuard antispam license.																													

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard-antivirus</i></td> <td>FortiGuard AntiVirus license.</td> </tr> <tr> <td><i>fortiguard-ips</i></td> <td>FortiGuard IPS license.</td> </tr> <tr> <td><i>fortiguard-management</i></td> <td>FortiGuard management service license.</td> </tr> <tr> <td><i>forticloud</i></td> <td>FortiCloud license.</td> </tr> <tr> <td><i>any</i></td> <td>Any license.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.	<i>fortiguard-ips</i>	FortiGuard IPS license.	<i>fortiguard-management</i>	FortiGuard management service license.	<i>forticloud</i>	FortiCloud license.	<i>any</i>	Any license.			
Option	Description															
<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.															
<i>fortiguard-ips</i>	FortiGuard IPS license.															
<i>fortiguard-management</i>	FortiGuard management service license.															
<i>forticloud</i>	FortiCloud license.															
<i>any</i>	Any license.															
ioc-level	IOC threat level.	option	-	high												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>medium</i></td> <td>IOC level medium and high.</td> </tr> <tr> <td><i>high</i></td> <td>IOC level high only.</td> </tr> </tbody> </table>	Option	Description	<i>medium</i>	IOC level medium and high.	<i>high</i>	IOC level high only.									
Option	Description															
<i>medium</i>	IOC level medium and high.															
<i>high</i>	IOC level high only.															
report-type	Security Rating report.	option	-	PostureReport												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>PostureReport</i></td> <td>Posture Report.</td> </tr> <tr> <td><i>CoverageReport</i></td> <td>Coverage Report.</td> </tr> <tr> <td><i>OptimizationReport</i></td> <td>Optimization Report</td> </tr> </tbody> </table>	Option	Description	<i>PostureReport</i>	Posture Report.	<i>CoverageReport</i>	Coverage Report.	<i>OptimizationReport</i>	Optimization Report							
Option	Description															
<i>PostureReport</i>	Posture Report.															
<i>CoverageReport</i>	Coverage Report.															
<i>OptimizationReport</i>	Optimization Report															
logid	Log ID to trigger event.	integer	Minimum value: 1 Maximum value: 65535	0												
trigger-frequency	Scheduled trigger frequency .	option	-	daily												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hourly</i></td> <td>Run hourly.</td> </tr> <tr> <td><i>daily</i></td> <td>Run daily.</td> </tr> <tr> <td><i>weekly</i></td> <td>Run weekly.</td> </tr> <tr> <td><i>monthly</i></td> <td>Run monthly.</td> </tr> </tbody> </table>	Option	Description	<i>hourly</i>	Run hourly.	<i>daily</i>	Run daily.	<i>weekly</i>	Run weekly.	<i>monthly</i>	Run monthly.					
Option	Description															
<i>hourly</i>	Run hourly.															
<i>daily</i>	Run daily.															
<i>weekly</i>	Run weekly.															
<i>monthly</i>	Run monthly.															
trigger-weekday	Day of week for trigger.	option	-													

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sunday</i></td> <td>Sunday.</td> </tr> <tr> <td><i>monday</i></td> <td>Monday.</td> </tr> <tr> <td><i>tuesday</i></td> <td>Tuesday.</td> </tr> <tr> <td><i>wednesday</i></td> <td>Wednesday.</td> </tr> <tr> <td><i>thursday</i></td> <td>Thursday.</td> </tr> <tr> <td><i>friday</i></td> <td>Friday.</td> </tr> <tr> <td><i>saturday</i></td> <td>Saturday.</td> </tr> </tbody> </table>	Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.			
Option	Description																			
<i>sunday</i>	Sunday.																			
<i>monday</i>	Monday.																			
<i>tuesday</i>	Tuesday.																			
<i>wednesday</i>	Wednesday.																			
<i>thursday</i>	Thursday.																			
<i>friday</i>	Friday.																			
<i>saturday</i>	Saturday.																			
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31	1																
trigger-hour	Hour of the day on which to trigger .	integer	Minimum value: 0 Maximum value: 23	0																
trigger-minute	Minute of the hour on which to trigger .	integer	Minimum value: 0 Maximum value: 59	0																
faz-event-name	FortiAnalyzer event handler name.	var-string	Maximum length: 255																	
faz-event-severity	FortiAnalyzer event severity.	var-string	Maximum length: 255																	
faz-event-tags	FortiAnalyzer event tags.	var-string	Maximum length: 255																	

### config fields

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

### config system automation-action

Action for automation stitches.

---

```
config system automation-action
  Description: Action for automation stitches.
  edit <name>
    set action-type [email|ios-notification|...]
    set tls-certificate {string}
    set email-to <name1>, <name2>, ...
    set email-from {var-string}
    set email-subject {var-string}
    set minimum-interval {integer}
    set delay {integer}
    set required [enable|disable]
    set aws-api-id {string}
    set aws-region {string}
    set aws-domain {string}
    set aws-api-stage {string}
    set aws-api-path {string}
    set aws-api-key {password}
    set azure-app {string}
    set azure-function {string}
    set azure-domain {string}
    set azure-function-authorization [anonymous|function|...]
    set azure-api-key {password}
    set gcp-function-region {string}
    set gcp-project {string}
    set gcp-function-domain {string}
    set gcp-function {string}
    set alicloud-account-id {string}
    set alicloud-region {string}
    set alicloud-function-domain {string}
    set alicloud-version {string}
    set alicloud-service {string}
    set alicloud-function {string}
    set alicloud-function-authorization [anonymous|function]
    set alicloud-access-key-id {string}
    set alicloud-access-key-secret {password}
    set message {string}
    set protocol [http|https]
    set method [post|put|...]
    set uri {var-string}
    set http-body {var-string}
    set port {integer}
    set headers <header1>, <header2>, ...
    set verify-host-cert [enable|disable]
    set script {var-string}
    set accprofile {string}
    set security-tag {string}
    set sdn-connector <name1>, <name2>, ...
  next
end
```

## config system automation-action

Parameter	Description	Type	Size	Default																																		
action-type	Action type.	option	-	alert																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>email</i></td> <td>Send notification email.</td> </tr> <tr> <td><i>ios-notification</i></td> <td>Send push notification to FortiExplorer iOS.</td> </tr> <tr> <td><i>alert</i></td> <td>Generate FortiOS dashboard alert.</td> </tr> <tr> <td><i>disable-ssid</i></td> <td>Disable interface.</td> </tr> <tr> <td><i>quarantine</i></td> <td>Quarantine host.</td> </tr> <tr> <td><i>quarantine-forticlient</i></td> <td>Quarantine FortiClient by EMS.</td> </tr> <tr> <td><i>quarantine-nsx</i></td> <td>Quarantine NSX instance.</td> </tr> <tr> <td><i>quarantine-fortinac</i></td> <td>Quarantine host by FortiNAC.</td> </tr> <tr> <td><i>ban-ip</i></td> <td>Ban IP address.</td> </tr> <tr> <td><i>aws-lambda</i></td> <td>Send log data to integrated AWS service.</td> </tr> <tr> <td><i>azure-function</i></td> <td>Send log data to an Azure function.</td> </tr> <tr> <td><i>google-cloud-function</i></td> <td>Send log data to a Google Cloud function.</td> </tr> <tr> <td><i>alicloud-function</i></td> <td>Send log data to an AliCloud function.</td> </tr> <tr> <td><i>webhook</i></td> <td>Send an HTTP request.</td> </tr> <tr> <td><i>cli-script</i></td> <td>Run CLI script.</td> </tr> <tr> <td><i>slack-notification</i></td> <td>Send a notification message to a Slack incoming webhook.</td> </tr> </tbody> </table>	Option	Description	<i>email</i>	Send notification email.	<i>ios-notification</i>	Send push notification to FortiExplorer iOS.	<i>alert</i>	Generate FortiOS dashboard alert.	<i>disable-ssid</i>	Disable interface.	<i>quarantine</i>	Quarantine host.	<i>quarantine-forticlient</i>	Quarantine FortiClient by EMS.	<i>quarantine-nsx</i>	Quarantine NSX instance.	<i>quarantine-fortinac</i>	Quarantine host by FortiNAC.	<i>ban-ip</i>	Ban IP address.	<i>aws-lambda</i>	Send log data to integrated AWS service.	<i>azure-function</i>	Send log data to an Azure function.	<i>google-cloud-function</i>	Send log data to a Google Cloud function.	<i>alicloud-function</i>	Send log data to an AliCloud function.	<i>webhook</i>	Send an HTTP request.	<i>cli-script</i>	Run CLI script.	<i>slack-notification</i>	Send a notification message to a Slack incoming webhook.			
Option	Description																																					
<i>email</i>	Send notification email.																																					
<i>ios-notification</i>	Send push notification to FortiExplorer iOS.																																					
<i>alert</i>	Generate FortiOS dashboard alert.																																					
<i>disable-ssid</i>	Disable interface.																																					
<i>quarantine</i>	Quarantine host.																																					
<i>quarantine-forticlient</i>	Quarantine FortiClient by EMS.																																					
<i>quarantine-nsx</i>	Quarantine NSX instance.																																					
<i>quarantine-fortinac</i>	Quarantine host by FortiNAC.																																					
<i>ban-ip</i>	Ban IP address.																																					
<i>aws-lambda</i>	Send log data to integrated AWS service.																																					
<i>azure-function</i>	Send log data to an Azure function.																																					
<i>google-cloud-function</i>	Send log data to a Google Cloud function.																																					
<i>alicloud-function</i>	Send log data to an AliCloud function.																																					
<i>webhook</i>	Send an HTTP request.																																					
<i>cli-script</i>	Run CLI script.																																					
<i>slack-notification</i>	Send a notification message to a Slack incoming webhook.																																					
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35																																			
email-to <name>	Email addresses. Email address.	string	Maximum length: 255																																			
email-from	Email sender name.	var-string	Maximum length: 127																																			
email-subject	Email subject.	var-string	Maximum length: 511																																			

Parameter	Description	Type	Size	Default
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	0
required	Required in action chain.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Required in action chain.		
	<i>disable</i>	Not required in action chain.		
aws-api-id	AWS API Gateway ID.	string	Maximum length: 35	
aws-region	AWS region.	string	Maximum length: 35	
aws-domain	AWS domain.	string	Maximum length: 63	amazonaws.com
aws-api-stage	AWS API Gateway deployment stage name.	string	Maximum length: 63	
aws-api-path	AWS API Gateway path.	string	Maximum length: 63	
aws-api-key	AWS API Gateway API key.	password	Not Specified	
azure-app	Azure function application name.	string	Maximum length: 63	
azure-function	Azure function name.	string	Maximum length: 63	
azure-domain	Azure function domain.	string	Maximum length: 63	azurewebsites.net
azure-function-authorization	Azure function authorization level.	option	-	anonymous
	<b>Option</b>	<b>Description</b>		
	<i>anonymous</i>	Anonymous authorization level (No authorization required).		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>function</i></td> <td>Function authorization level (Function or Host Key required).</td> </tr> <tr> <td><i>admin</i></td> <td>Admin authorization level (Master Host Key required).</td> </tr> </tbody> </table>	Option	Description	<i>function</i>	Function authorization level (Function or Host Key required).	<i>admin</i>	Admin authorization level (Master Host Key required).			
Option	Description									
<i>function</i>	Function authorization level (Function or Host Key required).									
<i>admin</i>	Admin authorization level (Master Host Key required).									
azure-api-key	Azure function API key.	password	Not Specified							
gcp-function-region	Google Cloud function region.	string	Maximum length: 63							
gcp-project	Google Cloud Platform project name.	string	Maximum length: 63							
gcp-function-domain	Google Cloud function domain.	string	Maximum length: 63	cloudfunctions.net						
gcp-function	Google Cloud function name.	string	Maximum length: 63							
alicloud-account-id	AliCloud account ID.	string	Maximum length: 63							
alicloud-region	AliCloud region.	string	Maximum length: 63							
alicloud-function-domain	AliCloud function domain.	string	Maximum length: 63	fc.aliyuncs.com						
alicloud-version	AliCloud version.	string	Maximum length: 63							
alicloud-service	AliCloud service name.	string	Maximum length: 128							
alicloud-function	AliCloud function name.	string	Maximum length: 128							
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>anonymous</i></td> <td>Anonymous authorization (No authorization required).</td> </tr> <tr> <td><i>function</i></td> <td>Function authorization (Authorization required).</td> </tr> </tbody> </table>	Option	Description	<i>anonymous</i>	Anonymous authorization (No authorization required).	<i>function</i>	Function authorization (Authorization required).			
Option	Description									
<i>anonymous</i>	Anonymous authorization (No authorization required).									
<i>function</i>	Function authorization (Authorization required).									
alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default												
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified													
message	Message content.	string	Maximum length: 1023	%%log%%												
protocol	Request protocol.	option	-	http												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>HTTP.</td> </tr> <tr> <td><i>https</i></td> <td>HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.									
Option	Description															
<i>http</i>	HTTP.															
<i>https</i>	HTTPS.															
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-	post												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>post</i></td> <td>POST.</td> </tr> <tr> <td><i>put</i></td> <td>PUT.</td> </tr> <tr> <td><i>get</i></td> <td>GET.</td> </tr> <tr> <td><i>patch</i></td> <td>PATCH.</td> </tr> <tr> <td><i>delete</i></td> <td>DELETE.</td> </tr> </tbody> </table>	Option	Description	<i>post</i>	POST.	<i>put</i>	PUT.	<i>get</i>	GET.	<i>patch</i>	PATCH.	<i>delete</i>	DELETE.			
Option	Description															
<i>post</i>	POST.															
<i>put</i>	PUT.															
<i>get</i>	GET.															
<i>patch</i>	PATCH.															
<i>delete</i>	DELETE.															
uri	Request API URI.	var-string	Maximum length: 1023													
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 1023													
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0												
headers <header>	Request headers. Request header.	string	Maximum length: 255													
verify-host-cert	Enable/disable verification of the remote host certificate.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of the remote host certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of the remote host certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of the remote host certificate.	<i>disable</i>	Disable verification of the remote host certificate.									
Option	Description															
<i>enable</i>	Enable verification of the remote host certificate.															
<i>disable</i>	Disable verification of the remote host certificate.															



Parameter	Description	Type	Size	Default
script	CLI script.	var-string	Maximum length: 1023	
accprofile	Access profile for CLI script action to access FortiGate features.	string	Maximum length: 35	
security-tag	NSX security tag.	string	Maximum length: 255	
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79	

## config system automation-destination

Automation destinations.

```
config system automation-destination
  Description: Automation destinations.
  edit <name>
    set type [fortigate|ha-cluster]
    set destination <name1>, <name2>, ...
    set ha-group-id {integer}
  next
end
```

## config system automation-destination

Parameter	Description	Type	Size	Default						
type	Destination type.	option	-	fortigate						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortigate</i></td> <td>FortiGate set as destination.</td> </tr> <tr> <td><i>ha-cluster</i></td> <td>HA cluster set as destination.</td> </tr> </tbody> </table>	Option	Description	<i>fortigate</i>	FortiGate set as destination.	<i>ha-cluster</i>	HA cluster set as destination.			
Option	Description									
<i>fortigate</i>	FortiGate set as destination.									
<i>ha-cluster</i>	HA cluster set as destination.									
destination <name>	Destinations. Destination.	string	Maximum length: 31							
ha-group-id	Cluster group ID set for this destination .	integer	Minimum value: 0 Maximum value: 255	0						

## config system automation-stitch

Automation stitches.

```
config system automation-stitch
```

```

Description: Automation stitches.
edit <name>
    set status [enable|disable]
    set trigger {string}
    set action <name1>, <name2>, ...
    set destination <name1>, <name2>, ...
next
end

```

## config system automation-stitch

Parameter	Description	Type	Size	Default						
status	Enable/disable this stitch.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable stitch.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable stitch.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable stitch.	<i>disable</i>	Disable stitch.			
Option	Description									
<i>enable</i>	Enable stitch.									
<i>disable</i>	Disable stitch.									
trigger	Trigger name.	string	Maximum length: 35							
action <name>	Action names. Action name.	string	Maximum length: 79							
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79							

## config system nd-proxy

Configure IPv6 neighbor discovery proxy (RFC4389).

```

config system nd-proxy
    Description: Configure IPv6 neighbor discovery proxy (RFC4389).
    set status [enable|disable]
    set member <interface-name1>, <interface-name2>, ...
end

```

## config system nd-proxy

Parameter	Description	Type	Size	Default						
status	Enable/disable neighbor discovery proxy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable neighbor discovery proxy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable neighbor discovery proxy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable neighbor discovery proxy.	<i>disable</i>	Disable neighbor discovery proxy.			
Option	Description									
<i>enable</i>	Enable neighbor discovery proxy.									
<i>disable</i>	Disable neighbor discovery proxy.									

Parameter	Description	Type	Size	Default
member <interface-name>	Interfaces using the neighbor discovery proxy. Interface name.	string	Maximum length: 79	

## config system saml

Global settings for SAML authentication.

```

config system saml
  Description: Global settings for SAML authentication.
  set status [enable|disable]
  set role [identity-provider|service-provider]
  set default-login-page [normal|sso]
  set default-profile {string}
  set cert {string}
  set portal-url {string}
  set entity-id {string}
  set single-sign-on-url {string}
  set single-logout-url {string}
  set idp-entity-id {string}
  set idp-single-sign-on-url {string}
  set idp-single-logout-url {string}
  set idp-cert {string}
  set server-address {string}
  set tolerance {integer}
  set life {integer}
config service-providers
  Description: Authorized service providers.
  edit <name>
    set prefix {string}
    set sp-cert {string}
    set sp-entity-id {string}
    set sp-single-sign-on-url {string}
    set sp-single-logout-url {string}
    set sp-portal-url {string}
    set idp-entity-id {string}
    set idp-single-sign-on-url {string}
    set idp-single-logout-url {string}
  config assertion-attributes
    Description: Customized SAML attributes to send along with assertion.
    edit <name>
      set type [username|email|...]
    next
  end
next
end
end
end

```

## config system saml

Parameter	Description	Type	Size	Default						
status	Enable/disable SAML authentication .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SAML authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SAML authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SAML authentication.	<i>disable</i>	Disable SAML authentication.			
Option	Description									
<i>enable</i>	Enable SAML authentication.									
<i>disable</i>	Disable SAML authentication.									
role	SAML role.	option	-	service-provider						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>identity-provider</i></td> <td>Identity Provider.</td> </tr> <tr> <td><i>service-provider</i></td> <td>Service Provider.</td> </tr> </tbody> </table>	Option	Description	<i>identity-provider</i>	Identity Provider.	<i>service-provider</i>	Service Provider.			
Option	Description									
<i>identity-provider</i>	Identity Provider.									
<i>service-provider</i>	Service Provider.									
default-login-page	Choose default login page.	option	-	normal						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>normal</i></td> <td>Use local login page as default.</td> </tr> <tr> <td><i>sso</i></td> <td>Use IdP's Single Sign-On page as default.</td> </tr> </tbody> </table>	Option	Description	<i>normal</i>	Use local login page as default.	<i>sso</i>	Use IdP's Single Sign-On page as default.			
Option	Description									
<i>normal</i>	Use local login page as default.									
<i>sso</i>	Use IdP's Single Sign-On page as default.									
default-profile	Default profile for new SSO admin.	string	Maximum length: 35							
cert	Certificate to sign SAML messages.	string	Maximum length: 35							
portal-url	SP portal URL.	string	Maximum length: 255							
entity-id	SP entity ID.	string	Maximum length: 255							
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255							
single-logout-url	SP single logout URL.	string	Maximum length: 255							
idp-entity-id	IDP entity ID.	string	Maximum length: 255							
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255							
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default
idp-cert	IDP certificate name.	string	Maximum length: 35	
server-address	Server address.	string	Maximum length: 63	
tolerance	Tolerance to the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	5
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	30

### config service-providers

Parameter	Description	Type	Size	Default
prefix	Prefix.	string	Maximum length: 35	
sp-cert	SP certificate name.	string	Maximum length: 35	
sp-entity-id	SP entity ID.	string	Maximum length: 255	
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255	
sp-portal-url	SP portal URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	

## config assertion-attributes

Parameter	Description	Type	Size	Default								
type	Type.	option	-	username								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>username</i></td><td>User Name.</td></tr><tr><td><i>email</i></td><td>Email Address.</td></tr><tr><td><i>profile-name</i></td><td>Profile Name.</td></tr></tbody></table>	Option	Description	<i>username</i>	User Name.	<i>email</i>	Email Address.	<i>profile-name</i>	Profile Name.			
Option	Description											
<i>username</i>	User Name.											
<i>email</i>	Email Address.											
<i>profile-name</i>	Profile Name.											

## config system vne-tunnel

Configure virtual network enabler tunnel.

```
config system vne-tunnel
  Description: Configure virtual network enabler tunnel.
  set status [enable|disable]
  set interface {string}
  set ssl-certificate {string}
  set bmr-hostname {password}
  set auto-asic-offload [enable|disable]
  set ipv4-address {ipv4-classnet-host}
  set br {ipv6-address}
  set update-url {string}
  set mode [map-e|fixed-ip]
end
```

## config system vne-tunnel

Parameter	Description	Type	Size	Default						
status	Enable/disable VNE tunnel.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable VNE tunnel.</td></tr><tr><td><i>disable</i></td><td>Disable VNE tunnel.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable VNE tunnel.	<i>disable</i>	Disable VNE tunnel.			
Option	Description									
<i>enable</i>	Enable VNE tunnel.									
<i>disable</i>	Disable VNE tunnel.									
interface	Interface name.	string	Maximum length: 15							
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
bmr-hostname	BMR hostname.	password	Not Specified							

Parameter	Description	Type	Size	Default						
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auto ASIC offloading.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable ASIC offloading.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.			
Option	Description									
<i>enable</i>	Enable auto ASIC offloading.									
<i>disable</i>	Disable ASIC offloading.									
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0						
br	Border relay IPv6 address.	ipv6-address	Not Specified	::						
update-url	URL of provisioning server.	string	Maximum length: 511							
mode	VNE tunnel mode.	option	-	map-e						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>map-e</i></td> <td>Map-e mode.</td> </tr> <tr> <td><i>fixed-ip</i></td> <td>Fixed-ip mode.</td> </tr> </tbody> </table>	Option	Description	<i>map-e</i>	Map-e mode.	<i>fixed-ip</i>	Fixed-ip mode.			
Option	Description									
<i>map-e</i>	Map-e mode.									
<i>fixed-ip</i>	Fixed-ip mode.									

\* This parameter may not exist in some models.

## test

This section includes syntax for the following commands:

- [config test openstackd on page 1141](#)
- [config test dhcprelay on page 1129](#)
- [config test quarantined on page 1133](#)
- [config test azd on page 1139](#)
- [config test iotd on page 1126](#)
- [config test zebos\\_launcher on page 1137](#)
- [config test ipldbd on page 1127](#)
- [config test dhcp6r on page 1135](#)
- [config test ipsmonitor on page 1126](#)
- [config test ovrd on page 1125](#)
- [config test hataalk on page 1123](#)
- [config test forticron on page 1132](#)
- [config test snmpd on page 1127](#)
- [config test imap on page 1122](#)
- [config test wad on page 1130](#)
- [config test lnkmttd on page 1134](#)
- [config test radiusd on page 1131](#)
- [config test fas on page 1141](#)
- [config test dhcp6c on page 1133](#)
- [config test ipmc\\_sensord on page 1134](#)
- [config test fnbamd on page 1136](#)
- [config test smtp on page 1121](#)
- [config test urlfilter on page 1125](#)
- [config test dnscd on page 1127](#)
- [config test ipseengine on page 1126](#)
- [config test sessionsync on page 1124](#)
- [config test uploadd on page 1133](#)
- [config test hasync on page 1123](#)
- [config test sdnd on page 1142](#)
- [config test ocid on page 1140](#)
- [config test ipsufd on page 1131](#)
- [config test fsvrd on page 1138](#)
- [config test updated on page 1135](#)
- [config test sdncd on page 1139](#)
- [config test bfd on page 1141](#)
- [config test dnsproxy on page 1128](#)
- [config test gcpd on page 1139](#)
- [config test init on page 1129](#)
- [config test nntp on page 1122](#)



- [config test forticldd on page 1124](#)
- [config test harelay on page 1123](#)
- [config test acd on page 1128](#)
- [config test sepmd on page 1142](#)
- [config test fsd on page 1131](#)
- [config test mrd on page 1136](#)
- [config test radius-das on page 1137](#)
- [config test dsd on page 1134](#)
- [config test fcnacd on page 1138](#)
- [config test ftpd on page 1121](#)
- [config test wf\\_monitor on page 1125](#)
- [config test kubed on page 1140](#)
- [config test lted on page 1132](#)
- [config test vned on page 1143](#)
- [config test l2tpcd on page 1129](#)
- [config test sflowd on page 1128](#)
- [config test csfd on page 1137](#)
- [config test wccpd on page 1130](#)
- [config test pptpcd on page 1130](#)
- [config test ipamd on page 1142](#)
- [config test radvd on page 1138](#)
- [config test awsd on page 1135](#)
- [config test miglogd on page 1124](#)
- [config test autod on page 1140](#)
- [config test pop3 on page 1122](#)
- [config test netxd on page 1136](#)

## config test smtp

SMTP proxy.

```
config test smtp
  Description: SMTP proxy.
  set <Integer> {string}
end
```

### config test smtp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test ftpd

FTP proxy.

```
config test ftpd
  Description: FTP proxy.
  set <Integer> {string}
end
```

### config test ftpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test pop3

POP3 proxy.

```
config test pop3
  Description: POP3 proxy.
  set <Integer> {string}
end
```

### config test pop3

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test imap

IMAP proxy.

```
config test imap
  Description: IMAP proxy.
  set <Integer> {string}
end
```

### config test imap

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test nntp

NNTP proxy.

```
config test nntp
  Description: NNTP proxy.
  set <Integer> {string}
end
```

### config test nntp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test harelay

HA relay daemon.

```
config test harelay
  Description: HA relay daemon.
  set <Integer> {string}
end
```

### config test harelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test hasync

HA sync daemon.

```
config test hasync
  Description: HA sync daemon.
  set <Integer> {string}
end
```

### config test hasync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test hatalk

HA talk daemon.

```
config test hataalk
  Description: HA talk daemon.
  set <Integer> {string}
end
```

## config test hataalk

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test sessionsync

session sync daemon.

```
config test sessionsync
  Description: session sync daemon.
  set <Integer> {string}
end
```

## config test sessionsync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test forticldd

FortiCloud daemon.

```
config test forticldd
  Description: FortiCloud daemon.
  set <Integer> {string}
end
```

## config test forticldd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test miglogd

Miglog logging daemon.

```
config test miglogd
  Description: Miglog logging daemon.
  set <Integer> {string}
end
```

### config test miglogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test urlfilter

URL filter daemon.

```
config test urlfilter
  Description: URL filter daemon.
  set <Integer> {string}
end
```

### config test urlfilter

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test wf\_monitor

WF monitor.

```
config test wf_monitor
  Description: WF monitor.
  set <Integer> {string}
end
```

### config test wf\_monitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test ovrd

Override daemon.

```
config test ovrld
  Description: Override daemon.
  set <Integer> {string}
end
```

### config test ovrld

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test iotd

IoT device info daemon.

```
config test iotd
  Description: IoT device info daemon.
  set <Integer> {string}
end
```

### config test iotd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test ipsmonitor

ips monitor

```
config test ipsmonitor
  Description: ips monitor
  set <Integer> {string}
end
```

### config test ipsmonitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test ipsengine

ips sensor

```
config test ipseengine
  Description: ips sensor
  set <Integer> {string}
end
```

### config test ipseengine

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test ipldbd

IP load balancing daemon.

```
config test ipldbd
  Description: IP load balancing daemon.
  set <Integer> {string}
end
```

### config test ipldbd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test ddnsd

DDNS client daemon.

```
config test ddnsd
  Description: DDNS client daemon.
  set <Integer> {string}
end
```

### config test ddnsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test snmpd

SNMP daemon.

```
config test snmpd
  Description: SNMP daemon.
  set <Integer> {string}
end
```

### config test snmpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test acd

Aggregate Controller.

```
config test acd
  Description: Aggregate Controller.
  set <Integer> {string}
end
```

### config test acd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test dnsproxy

DNS proxy.

```
config test dnsproxy
  Description: DNS proxy.
  set <Integer> {string}
end
```

### config test dnsproxy

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test sflowd

sFlow daemon.



```
config test sflowd
  Description: sFlow daemon.
  set <Integer> {string}
end
```

### config test sflowd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test init

init process.

```
config test init
  Description: init process.
  set <Integer> {string}
end
```

### config test init

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test l2tpcd

L2TP client daemon.

```
config test l2tpcd
  Description: L2TP client daemon.
  set <Integer> {string}
end
```

### config test l2tpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test dhcprelay

DHCP relay daemon.

```
config test dhcprelay
  Description: DHCP relay daemon.
  set <Integer> {string}
end
```

### config test dhcprelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test pptpcd

PPTP client.

```
config test pptpcd
  Description: PPTP client.
  set <Integer> {string}
end
```

### config test pptpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test wccpd

WCCP daemon.

```
config test wccpd
  Description: WCCP daemon.
  set <Integer> {string}
end
```

### config test wccpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test wad

WAD related processes.

```
config test wad
  Description: WAD related processes.
  set <Integer> {string}
end
```

### config test wad

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test radiusd

RADIUS daemon.

```
config test radiusd
  Description: RADIUS daemon.
  set <Integer> {string}
end
```

### config test radiusd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test fsd

FortiExplorer daemon.

```
config test fsd
  Description: FortiExplorer daemon.
  set <Integer> {string}
end
```

### config test fsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

### config test ipsufd

IPS urlfilter daemon.

```
config test ipsufd
  Description: IPS urlfilter daemon.
  set <Integer> {string}
end
```

## config test ipsufd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test lted



This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64.

USB LTE daemon.

```
config test lted
  Description: USB LTE daemon.
  set <Integer> {string}
end
```

## config test lted

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test forticron

Forticron daemon.

```
config test forticron
  Description: Forticron daemon.
  set <Integer> {string}
end
```

## config test forticron

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

---

## config test uploadd

Upload daemon.

```
config test uploadd
  Description: Upload daemon.
  set <Integer> {string}
end
```

## config test uploadd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test quarantined

Quarantine daemon.

```
config test quarantined
  Description: Quarantine daemon.
  set <Integer> {string}
end
```

## config test quarantined

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test dhcp6c

DHCP6 client daemon.

```
config test dhcp6c
  Description: DHCP6 client daemon.
  set <Integer> {string}
end
```

## config test dhcp6c

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

---

## config test dsd

DLP Statistics daemon.

```
config test dsd
  Description: DLP Statistics daemon.
  set <Integer> {string}
end
```

## config test dsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test ipmc\_sensord



This command is available for reference model(s) FortiGate 80E-POE, FortiGate 501E, FortiGate 3000D. It is not available for FortiWiFi 61E, FortiGate VM64.

---

Ipmc sensor daemon.

```
config test ipmc_sensord
  Description: Ipmc sensor daemon.
  set <Integer> {string}
end
```

## config test ipmc\_sensord

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test lnkmttd

Link monitor daemon.

```
config test lnkmttd
  Description: Link monitor daemon.
  set <Integer> {string}
end
```

## config test InkmtD

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test dhcp6r

DHCP6 relay daemon.

```
config test dhcp6r
  Description: DHCP6 relay daemon.
  set <Integer> {string}
end
```

## config test dhcp6r

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test updated

Update daemon.

```
config test updated
  Description: Update daemon.
  set <Integer> {string}
end
```

## config test updated

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test awsd

Amazon Web Services (AWS) daemon.

```
config test awsd
  Description: Amazon Web Services (AWS) daemon.
  set <Integer> {string}
end
```

## config test awsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test netxd

VMWare NetX service manager daemon.

```
config test netxd
  Description: VMWare NetX service manager daemon.
  set <Integer> {string}
end
```

## config test netxd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test fnbamd

Fortigate non-blocking auth daemon.

```
config test fnbamd
  Description: Fortigate non-blocking auth daemon.
  set <Integer> {string}
end
```

## config test fnbamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test mrd

Mobile router daemon.

```
config test mrd
  Description: Mobile router daemon.
  set <Integer> {string}
end
```



## config test mrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test zebos\_launcher

ZEBOS Launcher daemon

```
config test zebos_launcher
  Description: ZEBOS Launcher daemon
  set <Integer> {string}
end
```

## config test zebos\_launcher

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test radius-das

Radius-das daemon.

```
config test radius-das
  Description: Radius-das daemon.
  set <Integer> {string}
end
```

## config test radius-das

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test csfd

Security Fabric daemon.

```
config test csfd
  Description: Security Fabric daemon.
  set <Integer> {string}
end
```

## config test csfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test fsvrd

FortiService daemon.

```
config test fsvrd
  Description: FortiService daemon.
  set <Integer> {string}
end
```

## config test fsvrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test radvd

radvd daemon.

```
config test radvd
  Description: radvd daemon.
  set <Integer> {string}
end
```

## config test radvd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test fcnacd

FortiClient NAC daemon.

```
config test fcnacd
  Description: FortiClient NAC daemon.
  set <Integer> {string}
end
```

## config test fcnacd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test sdncd

SDN Connector daemon.

```
config test sdncd
  Description: SDN Connector daemon.
  set <Integer> {string}
end
```

## config test sdncd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test azd

Microsoft Azure daemon.

```
config test azd
  Description: Microsoft Azure daemon.
  set <Integer> {string}
end
```

## config test azd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test gcpd

Google Cloud Platform (GCP) daemon.

```
config test gcpd
  Description: Google Cloud Platform (GCP) daemon.
  set <Integer> {string}
end
```

## config test gcpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test ocid

Oracle Cloud Infrastructure.

```
config test ocid
  Description: Oracle Cloud Infrastructure.
  set <Integer> {string}
end
```

## config test ocid

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test kubed

Kubernetes daemon.

```
config test kubed
  Description: Kubernetes daemon.
  set <Integer> {string}
end
```

## config test kubed

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test autod

Automation daemon.

```
config test autod
  Description: Automation daemon.
  set <Integer> {string}
end
```

## config test autod

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test bfd

BFD daemon.

```
config test bfd
  Description: BFD daemon.
  set <Integer> {string}
end
```

## config test bfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test openstackd

OpenStack SDN connector daemon.

```
config test openstackd
  Description: OpenStack SDN connector daemon.
  set <Integer> {string}
end
```

## config test openstackd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test fas

FortiToken Cloud daemon.

```
config test fas
  Description: FortiToken Cloud daemon.
  set <Integer> {string}
end
```

## config test fas

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test sepmd

Symantec Endpoint Protection Manager daemon.

```
config test sepmd
  Description: Symantec Endpoint Protection Manager daemon.
  set <Integer> {string}
end
```

## config test sepmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test ipamd

IP Address Management daemon.

```
config test ipamd
  Description: IP Address Management daemon.
  set <Integer> {string}
end
```

## config test ipamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test sdnd

SDN connector daemon.

```
config test sdnd
  Description: SDN connector daemon.
  set <Integer> {string}
end
```

---

## config test sdnd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## config test vned

Virtual network enabler daemon.

```
config test vned
  Description: Virtual network enabler daemon.
  set <Integer> {string}
end
```

## config test vned

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

## user

This section includes syntax for the following commands:

- [config user pop3 on page 1166](#)
- [config user peer on page 1183](#)
- [config user fortitoken on page 1174](#)
- [config user nac-policy on page 1192](#)
- [config user fso-polling on page 1172](#)
- [config user quarantine on page 1185](#)
- [config user password-policy on page 1175](#)
- [config user ldap on page 1159](#)
- [config user fso on page 1168](#)
- [config user tacacs+ on page 1155](#)
- [config user group on page 1186](#)
- [config user peergrp on page 1185](#)
- [config user security-exempt-list on page 1191](#)
- [config user exchange on page 1157](#)
- [config user setting on page 1179](#)
- [config user radius on page 1144](#)
- [config user adgrp on page 1172](#)
- [config user local on page 1176](#)
- [config user domain-controller on page 1165](#)
- [config user krb-keytab on page 1165](#)
- [config user saml on page 1167](#)

## config user radius

Configure RADIUS server entries.

```
config user radius
  Description: Configure RADIUS server entries.
  edit <name>
    set server {string}
    set secret {password}
    set secondary-server {string}
    set secondary-secret {password}
    set tertiary-server {string}
    set tertiary-secret {password}
    set timeout {integer}
    set all-usergroup [disable|enable]
    set use-management-vdom [enable|disable]
    set nas-ip {ipv4-address}
    set acct-interim-interval {integer}
    set radius-coa [enable|disable]
    set radius-port {integer}
    set h3c-compatibility [enable|disable]
```



```

set auth-type [auto|ms_chap_v2|...]
set source-ip {string}
set username-case-sensitive [enable|disable]
set group-override-attr-type [filter-Id|class]
set class <name1>, <name2>, ...
set password-renewal [enable|disable]
set password-encoding [auto|ISO-8859-1]
set acct-all-servers [enable|disable]
set switch-controller-acct-fast-framedip-detect {integer}
set interface-select-method [auto|sdwan|...]
set interface {string}
set switch-controller-service-type {option1}, {option2}, ...
set rso [enable|disable]
set rso-radius-server-port {integer}
set rso-radius-response [enable|disable]
set rso-validate-request-secret [enable|disable]
set rso-secret {password}
set rso-endpoint-attribute [User-Name|NAS-IP-Address|...]
set rso-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute-key {string}
set sso-attribute-value-override [enable|disable]
set rso-context-timeout {integer}
set rso-log-period {integer}
set rso-log-flags {option1}, {option2}, ...
set rso-flush-ip-session [enable|disable]
set rso-ep-one-ip-only [enable|disable]
config accounting-server
  Description: Additional accounting servers.
  edit <id>
    set status [enable|disable]
    set server {string}
    set secret {password}
    set port {integer}
    set source-ip {string}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
  next
end
next
end

```

## config user radius

Parameter	Description	Type	Size	Default
server	Primary RADIUS server CN domain name or IP address.	string	Maximum length: 63	
secret	Pre-shared secret key used to access the primary RADIUS server.	password	Not Specified	
secondary-server	{<name_str ip_str> secondary RADIUS CN domain name or IP.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
secondary-secret	Secret key to access the secondary server.	password	Not Specified							
tertiary-server	{<name_str  ip_str>} tertiary RADIUS CN domain name or IP.	string	Maximum length: 63							
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified							
timeout	Time in seconds between re-sending authentication requests.	integer	Minimum value: 1 Maximum value: 300	5						
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not automatically include this server in a user group.</td> </tr> <tr> <td><i>enable</i></td> <td>Include this RADIUS server in every user group.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not automatically include this server in a user group.	<i>enable</i>	Include this RADIUS server in every user group.			
Option	Description									
<i>disable</i>	Do not automatically include this server in a user group.									
<i>enable</i>	Include this RADIUS server in every user group.									
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send requests using the management VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Send requests using the current VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send requests using the management VDOM.	<i>disable</i>	Send requests using the current VDOM.			
Option	Description									
<i>enable</i>	Send requests using the management VDOM.									
<i>disable</i>	Send requests using the current VDOM.									
nas-ip	IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.	ipv4-address	Not Specified	0.0.0.0						
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 60 Maximum value: 86400	0						
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable RADIUS CoA.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable RADIUS CoA.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable RADIUS CoA.	<i>disable</i>	Disable RADIUS CoA.			
Option	Description									
<i>enable</i>	Enable RADIUS CoA.									
<i>disable</i>	Disable RADIUS CoA.									

Parameter	Description	Type	Size	Default												
radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535	0												
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable H3C compatibility.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable H3C compatibility.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable H3C compatibility.	<i>disable</i>	Disable H3C compatibility.									
Option	Description															
<i>enable</i>	Enable H3C compatibility.															
<i>disable</i>	Disable H3C compatibility.															
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Use PAP, MSCHAP_v2, and CHAP (in that order).</td> </tr> <tr> <td><i>ms_chap_v2</i></td> <td>Microsoft Challenge Handshake Authentication Protocol version 2.</td> </tr> <tr> <td><i>ms_chap</i></td> <td>Microsoft Challenge Handshake Authentication Protocol.</td> </tr> <tr> <td><i>chap</i></td> <td>Challenge Handshake Authentication Protocol.</td> </tr> <tr> <td><i>pap</i></td> <td>Password Authentication Protocol.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Use PAP, MSCHAP_v2, and CHAP (in that order).	<i>ms_chap_v2</i>	Microsoft Challenge Handshake Authentication Protocol version 2.	<i>ms_chap</i>	Microsoft Challenge Handshake Authentication Protocol.	<i>chap</i>	Challenge Handshake Authentication Protocol.	<i>pap</i>	Password Authentication Protocol.			
Option	Description															
<i>auto</i>	Use PAP, MSCHAP_v2, and CHAP (in that order).															
<i>ms_chap_v2</i>	Microsoft Challenge Handshake Authentication Protocol version 2.															
<i>ms_chap</i>	Microsoft Challenge Handshake Authentication Protocol.															
<i>chap</i>	Challenge Handshake Authentication Protocol.															
<i>pap</i>	Password Authentication Protocol.															
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63													
username-case-sensitive	Enable/disable case sensitive user names.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable username case-sensitive.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable username case-sensitive.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable username case-sensitive.	<i>disable</i>	Disable username case-sensitive.									
Option	Description															
<i>enable</i>	Enable username case-sensitive.															
<i>disable</i>	Disable username case-sensitive.															
group-override-attr-type	RADIUS attribute type to override user group information.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>filter-ld</i></td> <td>Filter-ld</td> </tr> <tr> <td><i>class</i></td> <td>Class</td> </tr> </tbody> </table>	Option	Description	<i>filter-ld</i>	Filter-ld	<i>class</i>	Class									
Option	Description															
<i>filter-ld</i>	Filter-ld															
<i>class</i>	Class															
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79													

Parameter	Description	Type	Size	Default								
password-renewal	Enable/disable password renewal.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable password renewal.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable password renewal.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable password renewal.	<i>disable</i>	Disable password renewal.					
Option	Description											
<i>enable</i>	Enable password renewal.											
<i>disable</i>	Disable password renewal.											
password-encoding	Password encoding.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Use original password encoding.</td> </tr> <tr> <td><i>ISO-8859-1</i></td> <td>Use ISO-8859-1 password encoding.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Use original password encoding.	<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.					
Option	Description											
<i>auto</i>	Use original password encoding.											
<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.											
acct-all-servers	Enable/disable sending of accounting messages to all configured servers .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send accounting messages to all configured servers.</td> </tr> <tr> <td><i>disable</i></td> <td>Send accounting message only to servers that are confirmed to be reachable.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send accounting messages to all configured servers.	<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.					
Option	Description											
<i>enable</i>	Send accounting messages to all configured servers.											
<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.											
switch-controller-acct-fast-framedip-detect	Switch controller accounting message Framed-IP detection from DHCP snooping .	integer	Minimum value: 2 Maximum value: 600	2								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
switch-controller-service-type	RADIUS service type.	option	-									

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>login</i></td> <td>User should be connected to a host.</td> </tr> <tr> <td><i>framed</i></td> <td>User use Framed Protocol.</td> </tr> <tr> <td><i>callback-login</i></td> <td>User disconnected and called back.</td> </tr> <tr> <td><i>callback-framed</i></td> <td>User disconnected and called back, then a Framed Protocol.</td> </tr> <tr> <td><i>outbound</i></td> <td>User granted access to outgoing devices.</td> </tr> <tr> <td><i>administrative</i></td> <td>User granted access to the administrative unsigned interface.</td> </tr> <tr> <td><i>nas-prompt</i></td> <td>User provided a command prompt on the NAS.</td> </tr> <tr> <td><i>authenticate-only</i></td> <td>Authentication requested, and no auth info needs to be returned.</td> </tr> <tr> <td><i>callback-nas-prompt</i></td> <td>User disconnected and called back, then provided a command prompt.</td> </tr> <tr> <td><i>call-check</i></td> <td>Used by the NAS in an Access-Request packet, Access-Accept to answer the call.</td> </tr> <tr> <td><i>callback-administrative</i></td> <td>User disconnected and called back, granted access to the admin unsigned interface.</td> </tr> </tbody> </table>	Option	Description	<i>login</i>	User should be connected to a host.	<i>framed</i>	User use Framed Protocol.	<i>callback-login</i>	User disconnected and called back.	<i>callback-framed</i>	User disconnected and called back, then a Framed Protocol.	<i>outbound</i>	User granted access to outgoing devices.	<i>administrative</i>	User granted access to the administrative unsigned interface.	<i>nas-prompt</i>	User provided a command prompt on the NAS.	<i>authenticate-only</i>	Authentication requested, and no auth info needs to be returned.	<i>callback-nas-prompt</i>	User disconnected and called back, then provided a command prompt.	<i>call-check</i>	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.	<i>callback-administrative</i>	User disconnected and called back, granted access to the admin unsigned interface.			
Option	Description																											
<i>login</i>	User should be connected to a host.																											
<i>framed</i>	User use Framed Protocol.																											
<i>callback-login</i>	User disconnected and called back.																											
<i>callback-framed</i>	User disconnected and called back, then a Framed Protocol.																											
<i>outbound</i>	User granted access to outgoing devices.																											
<i>administrative</i>	User granted access to the administrative unsigned interface.																											
<i>nas-prompt</i>	User provided a command prompt on the NAS.																											
<i>authenticate-only</i>	Authentication requested, and no auth info needs to be returned.																											
<i>callback-nas-prompt</i>	User disconnected and called back, then provided a command prompt.																											
<i>call-check</i>	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.																											
<i>callback-administrative</i>	User disconnected and called back, granted access to the admin unsigned interface.																											
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable RADIUS based single sign on feature.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable RADIUS based single sign on feature.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable RADIUS based single sign on feature.	<i>disable</i>	Disable RADIUS based single sign on feature.																					
Option	Description																											
<i>enable</i>	Enable RADIUS based single sign on feature.																											
<i>disable</i>	Disable RADIUS based single sign on feature.																											
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 0 Maximum value: 65535	1813																								
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending RADIUS response packets.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending RADIUS response packets.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending RADIUS response packets.	<i>disable</i>	Disable sending RADIUS response packets.																					
Option	Description																											
<i>enable</i>	Enable sending RADIUS response packets.																											
<i>disable</i>	Disable sending RADIUS response packets.																											
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-	disable																								

Parameter	Description	Type	Size	Default																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable validating RADIUS request shared secret.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable validating RADIUS request shared secret.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable validating RADIUS request shared secret.	<i>disable</i>	Disable validating RADIUS request shared secret.																																			
Option	Description																																									
<i>enable</i>	Enable validating RADIUS request shared secret.																																									
<i>disable</i>	Disable validating RADIUS request shared secret.																																									
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified																																							
rsso-endpoint-attribute	RADIUS attributes used to extract the user endpoint identifier from the RADIUS Start record.	option	-	Calling-Station-Id																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>User-Name</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Netmask</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Filter-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-IP-Host</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Reply-Message</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Number</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-Route</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IPX-Network</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Class</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Called-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Calling-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-Identifier</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Proxy-State</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Service</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Node</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.			
Option	Description																																									
<i>User-Name</i>	Use this attribute.																																									
<i>NAS-IP-Address</i>	Use this attribute.																																									
<i>Framed-IP-Address</i>	Use this attribute.																																									
<i>Framed-IP-Netmask</i>	Use this attribute.																																									
<i>Filter-Id</i>	Use this attribute.																																									
<i>Login-IP-Host</i>	Use this attribute.																																									
<i>Reply-Message</i>	Use this attribute.																																									
<i>Callback-Number</i>	Use this attribute.																																									
<i>Callback-Id</i>	Use this attribute.																																									
<i>Framed-Route</i>	Use this attribute.																																									
<i>Framed-IPX-Network</i>	Use this attribute.																																									
<i>Class</i>	Use this attribute.																																									
<i>Called-Station-Id</i>	Use this attribute.																																									
<i>Calling-Station-Id</i>	Use this attribute.																																									
<i>NAS-Identifier</i>	Use this attribute.																																									
<i>Proxy-State</i>	Use this attribute.																																									
<i>Login-LAT-Service</i>	Use this attribute.																																									
<i>Login-LAT-Node</i>	Use this attribute.																																									

Parameter	Description	Type	Size	Default																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Login-LAT-Group</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-AppleTalk-Zone</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Session-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Multi-Session-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.																											
Option	Description																																					
<i>Login-LAT-Group</i>	Use this attribute.																																					
<i>Framed-AppleTalk-Zone</i>	Use this attribute.																																					
<i>Acct-Session-Id</i>	Use this attribute.																																					
<i>Acct-Multi-Session-Id</i>	Use this attribute.																																					
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-																																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>User-Name</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Netmask</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Filter-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-IP-Host</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Reply-Message</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Number</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-Route</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IPX-Network</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Class</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Called-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Calling-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-Identifier</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Proxy-State</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.			
Option	Description																																					
<i>User-Name</i>	Use this attribute.																																					
<i>NAS-IP-Address</i>	Use this attribute.																																					
<i>Framed-IP-Address</i>	Use this attribute.																																					
<i>Framed-IP-Netmask</i>	Use this attribute.																																					
<i>Filter-Id</i>	Use this attribute.																																					
<i>Login-IP-Host</i>	Use this attribute.																																					
<i>Reply-Message</i>	Use this attribute.																																					
<i>Callback-Number</i>	Use this attribute.																																					
<i>Callback-Id</i>	Use this attribute.																																					
<i>Framed-Route</i>	Use this attribute.																																					
<i>Framed-IPX-Network</i>	Use this attribute.																																					
<i>Class</i>	Use this attribute.																																					
<i>Called-Station-Id</i>	Use this attribute.																																					
<i>Calling-Station-Id</i>	Use this attribute.																																					
<i>NAS-Identifier</i>	Use this attribute.																																					
<i>Proxy-State</i>	Use this attribute.																																					

Parameter	Description	Type	Size	Default																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Login-LAT-Service</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Node</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Group</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-AppleTalk-Zone</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Session-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Multi-Session-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.																	
Option	Description																															
<i>Login-LAT-Service</i>	Use this attribute.																															
<i>Login-LAT-Node</i>	Use this attribute.																															
<i>Login-LAT-Group</i>	Use this attribute.																															
<i>Framed-AppleTalk-Zone</i>	Use this attribute.																															
<i>Acct-Session-Id</i>	Use this attribute.																															
<i>Acct-Multi-Session-Id</i>	Use this attribute.																															
sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-	Class																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>User-Name</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Netmask</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Filter-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-IP-Host</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Reply-Message</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Number</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-Route</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IPX-Network</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Class</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Called-Station-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.			
Option	Description																															
<i>User-Name</i>	Use this attribute.																															
<i>NAS-IP-Address</i>	Use this attribute.																															
<i>Framed-IP-Address</i>	Use this attribute.																															
<i>Framed-IP-Netmask</i>	Use this attribute.																															
<i>Filter-Id</i>	Use this attribute.																															
<i>Login-IP-Host</i>	Use this attribute.																															
<i>Reply-Message</i>	Use this attribute.																															
<i>Callback-Number</i>	Use this attribute.																															
<i>Callback-Id</i>	Use this attribute.																															
<i>Framed-Route</i>	Use this attribute.																															
<i>Framed-IPX-Network</i>	Use this attribute.																															
<i>Class</i>	Use this attribute.																															
<i>Called-Station-Id</i>	Use this attribute.																															



Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Calling-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-Identifier</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Proxy-State</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Service</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Node</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Group</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-AppleTalk-Zone</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Session-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Multi-Session-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.			
Option	Description																							
<i>Calling-Station-Id</i>	Use this attribute.																							
<i>NAS-Identifier</i>	Use this attribute.																							
<i>Proxy-State</i>	Use this attribute.																							
<i>Login-LAT-Service</i>	Use this attribute.																							
<i>Login-LAT-Node</i>	Use this attribute.																							
<i>Login-LAT-Group</i>	Use this attribute.																							
<i>Framed-AppleTalk-Zone</i>	Use this attribute.																							
<i>Acct-Session-Id</i>	Use this attribute.																							
<i>Acct-Multi-Session-Id</i>	Use this attribute.																							
sso-attribute-key	Key prefix for SSO group value in the SSO attribute.	string	Maximum length: 35																					
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable override old attribute value with new value for the same endpoint.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable override old attribute value with new value for the same endpoint.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable override old attribute value with new value for the same endpoint.	<i>disable</i>	Disable override old attribute value with new value for the same endpoint.																	
Option	Description																							
<i>enable</i>	Enable override old attribute value with new value for the same endpoint.																							
<i>disable</i>	Disable override old attribute value with new value for the same endpoint.																							
rsso-context-timeout	Time in seconds before the logged out user is removed from the "user context list" of logged on users.	integer	Minimum value: 0 Maximum value: 4294967295	28800																				
rsso-log-period	Time interval in seconds that group event log messages will be generated for dynamic profile events.	integer	Minimum value: 0 Maximum value: 4294967295	0																				

Parameter	Description	Type	Size	Default																
rsso-log-flags	Events to log.	option	-	protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>protocol-error</i></td> <td>Enable this log type.</td> </tr> <tr> <td><i>profile-missing</i></td> <td>Enable this log type.</td> </tr> <tr> <td><i>accounting-stop-missed</i></td> <td>Enable this log type.</td> </tr> <tr> <td><i>accounting-event</i></td> <td>Enable this log type.</td> </tr> <tr> <td><i>endpoint-block</i></td> <td>Enable this log type.</td> </tr> <tr> <td><i>radiusd-other</i></td> <td>Enable this log type.</td> </tr> <tr> <td><i>none</i></td> <td>Disable all logging.</td> </tr> </tbody> </table>	Option	Description	<i>protocol-error</i>	Enable this log type.	<i>profile-missing</i>	Enable this log type.	<i>accounting-stop-missed</i>	Enable this log type.	<i>accounting-event</i>	Enable this log type.	<i>endpoint-block</i>	Enable this log type.	<i>radiusd-other</i>	Enable this log type.	<i>none</i>	Disable all logging.			
Option	Description																			
<i>protocol-error</i>	Enable this log type.																			
<i>profile-missing</i>	Enable this log type.																			
<i>accounting-stop-missed</i>	Enable this log type.																			
<i>accounting-event</i>	Enable this log type.																			
<i>endpoint-block</i>	Enable this log type.																			
<i>radiusd-other</i>	Enable this log type.																			
<i>none</i>	Disable all logging.																			
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable flush user IP sessions on RADIUS accounting stop.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable flush user IP sessions on RADIUS accounting stop.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.	<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.													
Option	Description																			
<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.																			
<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.																			
rsso-ep-one-ip-only	Enable/disable the replacement of old IP addresses with new ones for the same endpoint on RADIUS accounting Start messages.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.	<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.													
Option	Description																			
<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																			
<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																			

## config accounting-server

Parameter	Description	Type	Size	Default								
status	Status.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.					
Option	Description											
<i>enable</i>	Log to remote syslog server.											
<i>disable</i>	Do not log to remote syslog server.											
server	{<name_str ip_str>} Server CN domain name or IP.	string	Maximum length: 63									
secret	Secret key.	password	Not Specified									
port	RADIUS accounting port number.	integer	Minimum value: 0 Maximum value: 65535	0								
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></tbody></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config user tacacs+

Configure TACACS+ server entries.

```
config user tacacs+
  Description: Configure TACACS+ server entries.
  edit <name>
    set server {string}
    set secondary-server {string}
    set tertiary-server {string}
    set port {integer}
    set key {password}
    set secondary-key {password}
    set tertiary-key {password}
    set authen-type [mschap|chap|...]
```

```

set authorization [enable|disable]
set source-ip {string}
set interface-select-method [auto|sdwan|...]
set interface {string}
next
end

```

## config user tacacs+

Parameter	Description	Type	Size	Default												
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535	49												
key	Key to access the primary server.	password	Not Specified													
secondary-key	Key to access the secondary server.	password	Not Specified													
tertiary-key	Key to access the tertiary server.	password	Not Specified													
authen-type	Allowed authentication protocols/methods.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mschap</i></td> <td>MSCHAP.</td> </tr> <tr> <td><i>chap</i></td> <td>CHAP.</td> </tr> <tr> <td><i>pap</i></td> <td>PAP.</td> </tr> <tr> <td><i>ascii</i></td> <td>ASCII.</td> </tr> <tr> <td><i>auto</i></td> <td>Use PAP, MSCHAP, and CHAP (in that order).</td> </tr> </tbody> </table>	Option	Description	<i>mschap</i>	MSCHAP.	<i>chap</i>	CHAP.	<i>pap</i>	PAP.	<i>ascii</i>	ASCII.	<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).			
Option	Description															
<i>mschap</i>	MSCHAP.															
<i>chap</i>	CHAP.															
<i>pap</i>	PAP.															
<i>ascii</i>	ASCII.															
<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).															
authorization	Enable/disable TACACS+ authorization.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TACACS+ authorization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TACACS+ authorization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TACACS+ authorization.	<i>disable</i>	Disable TACACS+ authorization.									
Option	Description															
<i>enable</i>	Enable TACACS+ authorization.															
<i>disable</i>	Disable TACACS+ authorization.															

Parameter	Description	Type	Size	Default								
source-ip	source IP for communications to TACACS+ server.	string	Maximum length: 63									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config user exchange

Configure MS Exchange server entries.

```

config user exchange
  Description: Configure MS Exchange server entries.
  edit <name>
    set server-name {string}
    set domain-name {string}
    set username {string}
    set password {password}
    set ip {ipv4-address-any}
    set connect-protocol [rpc-over-tcp|rpc-over-http|...]
    set auth-type [spnego|ntlm|...]
    set auth-level [connect|call|...]
    set http-auth-type [basic|ntlm]
    set ssl-min-proto-version [default|SSLv3|...]
    set auto-discover-kdc [enable|disable]
    set kdc-ip <ipv41>, <ipv42>, ...
  next
end

```

## config user exchange

Parameter	Description	Type	Size	Default
server-name	MS Exchange server hostname.	string	Maximum length: 63	
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79	
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default												
password	Password for the specified username.	password	Not Specified													
ip	Server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0												
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-	rpc-over-https												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rpc-over-tcp</i></td> <td>Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.</td> </tr> <tr> <td><i>rpc-over-http</i></td> <td>Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td> </tr> <tr> <td><i>rpc-over-https</i></td> <td>Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td> </tr> </tbody> </table>	Option	Description	<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.	<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.	<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.							
Option	Description															
<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.															
<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.															
<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.															
auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>spnego</i></td> <td>Negotiate authentication.</td> </tr> <tr> <td><i>ntlm</i></td> <td>NTLM authentication.</td> </tr> <tr> <td><i>kerberos</i></td> <td>Kerberos authentication.</td> </tr> </tbody> </table>	Option	Description	<i>spnego</i>	Negotiate authentication.	<i>ntlm</i>	NTLM authentication.	<i>kerberos</i>	Kerberos authentication.							
Option	Description															
<i>spnego</i>	Negotiate authentication.															
<i>ntlm</i>	NTLM authentication.															
<i>kerberos</i>	Kerberos authentication.															
auth-level	Authentication security level used for the RPC protocol layer.	option	-	privacy												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>connect</i></td> <td>RPC authentication level 'connect'.</td> </tr> <tr> <td><i>call</i></td> <td>RPC authentication level 'call'.</td> </tr> <tr> <td><i>packet</i></td> <td>RPC authentication level 'packet'.</td> </tr> <tr> <td><i>integrity</i></td> <td>RPC authentication level 'integrity'.</td> </tr> <tr> <td><i>privacy</i></td> <td>RPC authentication level 'privacy'.</td> </tr> </tbody> </table>	Option	Description	<i>connect</i>	RPC authentication level 'connect'.	<i>call</i>	RPC authentication level 'call'.	<i>packet</i>	RPC authentication level 'packet'.	<i>integrity</i>	RPC authentication level 'integrity'.	<i>privacy</i>	RPC authentication level 'privacy'.			
Option	Description															
<i>connect</i>	RPC authentication level 'connect'.															
<i>call</i>	RPC authentication level 'call'.															
<i>packet</i>	RPC authentication level 'packet'.															
<i>integrity</i>	RPC authentication level 'integrity'.															
<i>privacy</i>	RPC authentication level 'privacy'.															
http-auth-type	Authentication security type used for the HTTP transport.	option	-	ntlm												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>basic</i></td> <td>Basic HTTP authentication.</td> </tr> </tbody> </table>	Option	Description	<i>basic</i>	Basic HTTP authentication.											
Option	Description															
<i>basic</i>	Basic HTTP authentication.															

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ntlm</i></td> <td>NTLM HTTP authentication.</td> </tr> </tbody> </table>	Option	Description	<i>ntlm</i>	NTLM HTTP authentication.											
Option	Description															
<i>ntlm</i>	NTLM HTTP authentication.															
ssl-min-protocol-version	Minimum SSL/TLS protocol version for HTTPS transport .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
auto-discover-kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic discovery of KDC IP addresses.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic discovery of KDC IP addresses.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic discovery of KDC IP addresses.	<i>disable</i>	Disable automatic discovery of KDC IP addresses.									
Option	Description															
<i>enable</i>	Enable automatic discovery of KDC IP addresses.															
<i>disable</i>	Disable automatic discovery of KDC IP addresses.															
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79													

## config user ldap

Configure LDAP server entries.

```

config user ldap
  Description: Configure LDAP server entries.
  edit <name>
    set server {string}
    set secondary-server {string}
    set tertiary-server {string}
    set server-identity-check [enable|disable]
    set source-ip {ipv4-address}
    set cnid {string}
    set dn {string}
    set type [simple|anonymous|...]
    set two-factor [disable|fortitoken-cloud]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set username {string}
    set password {password}
    set group-member-check [user-attr|group-object|...]
    set group-search-base {string}
    set group-object-filter {string}
  
```

```

set group-filter {string}
set secure [disable|starttls|...]
set ssl-min-proto-version [default|SSLv3|...]
set ca-cert {string}
set port {integer}
set password-expiry-warning [enable|disable]
set password-renewal [enable|disable]
set member-attr {string}
set account-key-processing [same|strip]
set account-key-filter {string}
set search-type {option1}, {option2}, ...
set obtain-user-info [enable|disable]
set user-info-exchange-server {string}
set interface-select-method [auto|sdwan|...]
set interface {string}
next
end

```

## config user ldap

Parameter	Description	Type	Size	Default
server	LDAP server CN domain name or IP.	string	Maximum length: 63	
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63	
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63	
server-identity-check	Enable/disable LDAP server identity check (verify server domain name/IP address against the server certificate).	option	-	enable
		<b>Option</b>	<b>Description</b>	
		<i>enable</i>	Enable server identity check.	
		<i>disable</i>	Disable server identity check.	





Parameter	Description	Type	Size	Default
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>email</i>	Email notification for activation code.		
	<i>sms</i>	SMS notification for activation code.		
username	Username (full DN) for initial binding.	string	Maximum length: 511	
password	Password for initial binding.	password	Not Specified	
group-member-check	Group member checking methods.	option	-	user-attr
	<b>Option</b>	<b>Description</b>		
	<i>user-attr</i>	User attribute checking.		
	<i>group-object</i>	Group object checking.		
	<i>posix-group-object</i>	POSIX group object checking.		
group-search-base	Search base used for group searching.	string	Maximum length: 511	
group-object-filter	Filter used for group searching.	string	Maximum length: 2047	(&(objectcategory=group)(member=*))
group-filter	Filter used for group matching.	string	Maximum length: 2047	
secure	Port to be used for authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	No SSL.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>starttls</i></td> <td>Use StartTLS.</td> </tr> <tr> <td><i>ldaps</i></td> <td>Use LDAPS.</td> </tr> </tbody> </table>	Option	Description	<i>starttls</i>	Use StartTLS.	<i>ldaps</i>	Use LDAPS.									
Option	Description															
<i>starttls</i>	Use StartTLS.															
<i>ldaps</i>	Use LDAPS.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
ca-cert	CA certificate name.	string	Maximum length: 79													
port	Port to be used for communication with the LDAP server .	integer	Minimum value: 1 Maximum value: 65535	389												
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable password expiry warnings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable password expiry warnings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable password expiry warnings.	<i>disable</i>	Disable password expiry warnings.									
Option	Description															
<i>enable</i>	Enable password expiry warnings.															
<i>disable</i>	Disable password expiry warnings.															
password-renewal	Enable/disable online password renewal.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable online password renewal.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable online password renewal.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable online password renewal.	<i>disable</i>	Disable online password renewal.									
Option	Description															
<i>enable</i>	Enable online password renewal.															
<i>disable</i>	Disable online password renewal.															

Parameter	Description	Type	Size	Default
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-	same
	<b>Option</b>	<b>Description</b>		
	<i>same</i>	Same as UPN.		
	<i>strip</i>	Strip domain string from UPN.		
account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047	(&(userPrincipalName=%s)!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
search-type	Search type.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.		
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable obtaining of user information.		
	<i>disable</i>	Disable obtaining of user information.		
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config user krb-keytab

Configure Kerberos keytab entries.

```
config user krb-keytab
  Description: Configure Kerberos keytab entries.
  edit <name>
    set pac-data [enable|disable]
    set principal {string}
    set ldap-server <name1>, <name2>, ...
    set keytab {string}
  next
end
```

## config user krb-keytab

Parameter	Description	Type	Size	Default						
pac-data	Enable/disable parsing PAC data in the ticket.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable parsing PAC data in the ticket.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable parsing PAC data in the ticket.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable parsing PAC data in the ticket.	<i>disable</i>	Disable parsing PAC data in the ticket.			
Option	Description									
<i>enable</i>	Enable parsing PAC data in the ticket.									
<i>disable</i>	Disable parsing PAC data in the ticket.									
principal	Kerberos service principal, e.g. HTTP/fgt.example.com@EXAMPLE.COM.	string	Maximum length: 511							
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79							
keytab	base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191							

## config user domain-controller

Configure domain controller entries.

```

config user domain-controller
  Description: Configure domain controller entries.
  edit <name>
    set ip-address {ipv4-address}
    set port {integer}
    config extra-server
      Description: extra servers.
      edit <id>
        set ip-address {ipv4-address}
        set port {integer}
      next
    end
    set domain-name {string}
    set ldap-server <name1>, <name2>, ...
  next
end

```

### config user domain-controller

Parameter	Description	Type	Size	Default
ip-address	Domain controller IP address.	ipv4-address	Not Specified	0.0.0.0
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535	445
domain-name	Domain DNS name.	string	Maximum length: 255	
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79	

### config extra-server

Parameter	Description	Type	Size	Default
ip-address	Domain controller IP address.	ipv4-address	Not Specified	0.0.0.0
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535	445

### config user pop3

POP3 server entry configuration.

```

config user pop3
  Description: POP3 server entry configuration.
  edit <name>
    set server {string}
    set port {integer}
    set secure [none|starttls|...]
    set ssl-min-proto-version [default|SSLv3|...]
  next
end

```

## config user pop3

Parameter	Description	Type	Size	Default												
server	{<name_str ip_str>} server domain name or IP.	string	Maximum length: 63													
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535	0												
secure	SSL connection.	option	-	starttls												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None.</td> </tr> <tr> <td><i>starttls</i></td> <td>Use StartTLS.</td> </tr> <tr> <td><i>pop3s</i></td> <td>Use POP3 over SSL.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>starttls</i>	Use StartTLS.	<i>pop3s</i>	Use POP3 over SSL.							
Option	Description															
<i>none</i>	None.															
<i>starttls</i>	Use StartTLS.															
<i>pop3s</i>	Use POP3 over SSL.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

## config user saml

SAML server entry configuration.

```

config user saml
  Description: SAML server entry configuration.
  edit <name>

```

```

set cert {string}
set entity-id {string}
set single-sign-on-url {string}
set single-logout-url {string}
set idp-entity-id {string}
set idp-single-sign-on-url {string}
set idp-single-logout-url {string}
set idp-cert {string}
set user-name {string}
set group-name {string}
next
end

```

## config user saml

Parameter	Description	Type	Size	Default
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
entity-id	SP entity ID.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
single-logout-url	SP single logout URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255	
idp-cert	IDP Certificate name.	string	Maximum length: 35	
user-name	User name in assertion statement.	string	Maximum length: 255	
group-name	Group name in assertion statement.	string	Maximum length: 255	

## config user fssso

Configure Fortinet Single Sign On (FSSO) agents.

```

config user fssso
  Description: Configure Fortinet Single Sign On (FSSO) agents.
  edit <name>
    set type [default|fortinac]

```



```

set server {string}
set port {integer}
set password {password}
set server2 {string}
set port2 {integer}
set password2 {password}
set server3 {string}
set port3 {integer}
set password3 {password}
set server4 {string}
set port4 {integer}
set password4 {password}
set server5 {string}
set port5 {integer}
set password5 {password}
set logon-timeout {integer}
set ldap-server {string}
set group-poll-interval {integer}
set ldap-poll [enable|disable]
set ldap-poll-interval {integer}
set ldap-poll-filter {string}
set user-info-server {string}
set ssl [enable|disable]
set ssl-trusted-cert {string}
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set interface-select-method [auto|sdwan|...]
set interface {string}
next
end

```

## config user fssso

Parameter	Description	Type	Size	Default						
type	Server type.	option	-	default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>All other unspecified types of servers.</td> </tr> <tr> <td><i>fortinac</i></td> <td>FortiNAC server.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	All other unspecified types of servers.	<i>fortinac</i>	FortiNAC server.			
Option	Description									
<i>default</i>	All other unspecified types of servers.									
<i>fortinac</i>	FortiNAC server.									
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63							
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000						
password	Password of the first FSSO collector agent.	password	Not Specified							

Parameter	Description	Type	Size	Default
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63	
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password2	Password of the second FSSO collector agent.	password	Not Specified	
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63	
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password3	Password of the third FSSO collector agent.	password	Not Specified	
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63	
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password4	Password of the fourth FSSO collector agent.	password	Not Specified	
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63	
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password5	Password of the fifth FSSO collector agent.	password	Not Specified	
logon-timeout	Interval in minutes to keep logons after FSSO server down.	integer	Minimum value: 1 Maximum value: 2880	5

Parameter	Description	Type	Size	Default
ldap-server	LDAP server to get group information.	string	Maximum length: 35	
group-poll-interval	Interval in minutes within to fetch groups from FSSO server, or unset to disable.	integer	Minimum value: 1 Maximum value: 2880	0
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic fetching of groups from LDAP server.		
	<i>disable</i>	Disable automatic fetching of groups from LDAP server.		
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047	(objectCategory=group)
user-info-server	LDAP server to get user information.	string	Maximum length: 35	
ssl	Enable/disable use of SSL.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of SSL.		
	<i>disable</i>	Disable use of SSL.		
ssl-trusted-cert	Trusted server certificate or CA certificate.	string	Maximum length: 79	
source-ip	Source IP for communications to FSSO agent.	ipv4-address	Not Specified	0.0.0.0
source-ip6	IPv6 source for communications to FSSO agent.	ipv6-address	Not Specified	::
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description									
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

## config user adgrp

Configure FSSO groups.

```
config user adgrp
  Description: Configure FSSO groups.
  edit <name>
    set server-name {string}
    set connector-source {string}
    set id {integer}
  next
end
```

## config user adgrp

Parameter	Description	Type	Size	Default
server-name	FSSO agent name.	string	Maximum length: 35	
connector-source	FSSO connector source.	string	Maximum length: 35	
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config user fssso-polling

Configure FSSO active directory servers for polling mode.

```
config user fssso-polling
  Description: Configure FSSO active directory servers for polling mode.
  edit <id>
    set status [enable|disable]
    set server {string}
    set default-domain {string}
    set port {integer}
    set user {string}
```

```

set password {password}
set ldap-server {string}
set logon-history {integer}
set polling-frequency {integer}
config adgrp
  Description: LDAP Group Info.
  edit <name>
  next
end
set smbvl [enable|disable]
set smb-ntlmv1-auth [enable|disable]
next
end

```

## config user fssso-polling

Parameter	Description	Type	Size	Default						
status	Enable/disable polling for the status of this Active Directory server.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63							
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35							
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535	0						
user	User name required to log into this Active Directory server.	string	Maximum length: 35							
password	Password required to log into this Active Directory server	password	Not Specified							
ldap-server	LDAP server name used in LDAP connection strings.	string	Maximum length: 35							
logon-history	Number of hours of logon history to keep, 0 means keep all history.	integer	Minimum value: 0 Maximum value: 48	8						

Parameter	Description	Type	Size	Default						
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30	10						
smbv1	Enable/disable support of SMBv1 for Samba.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support of SMBv1 for Samba.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support of SMBv1 for Samba.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support of SMBv1 for Samba.	<i>disable</i>	Disable support of SMBv1 for Samba.			
Option	Description									
<i>enable</i>	Enable support of SMBv1 for Samba.									
<i>disable</i>	Disable support of SMBv1 for Samba.									
smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support of NTLMv1 for Samba authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support of NTLMv1 for Samba authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support of NTLMv1 for Samba authentication.	<i>disable</i>	Disable support of NTLMv1 for Samba authentication.			
Option	Description									
<i>enable</i>	Enable support of NTLMv1 for Samba authentication.									
<i>disable</i>	Disable support of NTLMv1 for Samba authentication.									

## config user fortitoken

Configure FortiToken.

```

config user fortitoken
  Description: Configure FortiToken.
  edit <serial-number>
    set status [active|lock]
    set comments {var-string}
    set license {string}
    set activation-code {string}
    set activation-expire {integer}
    set reg-id {string}
    set os-ver {string}
  next
end

```

## config user fortitoken

Parameter	Description	Type	Size	Default						
status	Status	option	-	active						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>active</i></td> <td>Activate FortiToken.</td> </tr> <tr> <td><i>lock</i></td> <td>Lock FortiToken.</td> </tr> </tbody> </table>	Option	Description	<i>active</i>	Activate FortiToken.	<i>lock</i>	Lock FortiToken.			
Option	Description									
<i>active</i>	Activate FortiToken.									
<i>lock</i>	Lock FortiToken.									

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
license	Mobile token license.	string	Maximum length: 31	
activation-code	Mobile token user activation-code.	string	Maximum length: 32	
activation-expire	Mobile token user activation-code expire time.	integer	Minimum value: 0 Maximum value: 4294967295	0
reg-id	Device Reg ID.	string	Maximum length: 256	
os-ver	Device Mobile Version.	string	Maximum length: 15	

## config user password-policy

Configure user password policy.

```
config user password-policy
  Description: Configure user password policy.
  edit <name>
    set expire-days {integer}
    set warn-days {integer}
    set expired-password-renewal [enable|disable]
  next
end
```

## config user password-policy

Parameter	Description	Type	Size	Default
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180
warn-days	Time in days before a password expiration warning message is displayed to the user upon login.	integer	Minimum value: 0 Maximum value: 30	15

Parameter	Description	Type	Size	Default
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable renewal of a password that already is expired.		
	<i>disable</i>	Disable renewal of a password that already is expired.		

## config user local

Configure local users.

```

config user local
  Description: Configure local users.
  edit <name>
    set id {integer}
    set status [enable|disable]
    set type [password|radius|...]
    set passwd {password}
    set ldap-server {string}
    set radius-server {string}
    set tacacs+-server {string}
    set two-factor [disable|fortitoken|...]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set fortitoken {string}
    set email-to {string}
    set sms-server [fortiguard|custom]
    set sms-custom-server {string}
    set sms-phone {string}
    set passwd-policy {string}
    set passwd-time {user}
    set authtimeout {integer}
    set workstation {string}
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set ppk-secret {password-3}
    set ppk-identity {string}
    set username-sensitivity [disable|enable]
  next
end

```



## config user local

Parameter	Description	Type	Size	Default												
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
status	Enable/disable allowing the local user to authenticate with the FortiGate unit.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable user.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable user.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable user.	<i>disable</i>	Disable user.									
Option	Description															
<i>enable</i>	Enable user.															
<i>disable</i>	Disable user.															
type	Authentication method.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>password</i></td> <td>Password authentication.</td> </tr> <tr> <td><i>radius</i></td> <td>RADIUS server authentication.</td> </tr> <tr> <td><i>tacacs+</i></td> <td>TACACS+ server authentication.</td> </tr> <tr> <td><i>ldap</i></td> <td>LDAP server authentication.</td> </tr> </tbody> </table>	Option	Description	<i>password</i>	Password authentication.	<i>radius</i>	RADIUS server authentication.	<i>tacacs+</i>	TACACS+ server authentication.	<i>ldap</i>	LDAP server authentication.					
Option	Description															
<i>password</i>	Password authentication.															
<i>radius</i>	RADIUS server authentication.															
<i>tacacs+</i>	TACACS+ server authentication.															
<i>ldap</i>	LDAP server authentication.															
passwd	User's password.	password	Not Specified													
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35													
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35													
tacacs+-server	Name of TACACS+ server with which the user must authenticate.	string	Maximum length: 35													
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>disable</td> </tr> <tr> <td><i>fortitoken</i></td> <td>FortiToken</td> </tr> <tr> <td><i>fortitoken-cloud</i></td> <td>FortiToken Cloud Service.</td> </tr> <tr> <td><i>email</i></td> <td>Email authentication code.</td> </tr> <tr> <td><i>sms</i></td> <td>SMS authentication code.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	disable	<i>fortitoken</i>	FortiToken	<i>fortitoken-cloud</i>	FortiToken Cloud Service.	<i>email</i>	Email authentication code.	<i>sms</i>	SMS authentication code.			
Option	Description															
<i>disable</i>	disable															
<i>fortitoken</i>	FortiToken															
<i>fortitoken-cloud</i>	FortiToken Cloud Service.															
<i>email</i>	Email authentication code.															
<i>sms</i>	SMS authentication code.															

Parameter	Description	Type	Size	Default								
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortitoken</i></td> <td>FortiToken authentication.</td> </tr> <tr> <td><i>email</i></td> <td>Email one time password.</td> </tr> <tr> <td><i>sms</i></td> <td>SMS one time password.</td> </tr> </tbody> </table>	Option	Description	<i>fortitoken</i>	FortiToken authentication.	<i>email</i>	Email one time password.	<i>sms</i>	SMS one time password.			
Option	Description											
<i>fortitoken</i>	FortiToken authentication.											
<i>email</i>	Email one time password.											
<i>sms</i>	SMS one time password.											
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>email</i></td> <td>Email notification for activation code.</td> </tr> <tr> <td><i>sms</i></td> <td>SMS notification for activation code.</td> </tr> </tbody> </table>	Option	Description	<i>email</i>	Email notification for activation code.	<i>sms</i>	SMS notification for activation code.					
Option	Description											
<i>email</i>	Email notification for activation code.											
<i>sms</i>	SMS notification for activation code.											
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16									
email-to	Two-factor recipient's email address.	string	Maximum length: 63									
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard</i></td> <td>Send SMS by FortiGuard.</td> </tr> <tr> <td><i>custom</i></td> <td>Send SMS by custom server.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.					
Option	Description											
<i>fortiguard</i>	Send SMS by FortiGuard.											
<i>custom</i>	Send SMS by custom server.											
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35									
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15									
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35									
passwd-time	Time of the last password update.	user	Not Specified									
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440	0								

Parameter	Description	Type	Size	Default						
workstation	Name of the remote user workstation, if you want to limit the user to authenticate only from a particular workstation.	string	Maximum length: 35							
auth-concurrent-override	Enable/disable overriding the policy-auth-concurrent under config system global.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auth-concurrent-override.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable auth-concurrent-override.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auth-concurrent-override.	<i>disable</i>	Disable auth-concurrent-override.			
Option	Description									
<i>enable</i>	Enable auth-concurrent-override.									
<i>disable</i>	Disable auth-concurrent-override.									
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100	0						
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35							
username-sensitivity	Enable/disable case and accent sensitivity when performing username matching (accents are stripped and case is ignored when disabled).	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Ignore case and accents. Username at prompt not required to match case or accents.</td> </tr> <tr> <td><i>enable</i></td> <td>Do not ignore case and accents. Username at prompt must be an exact match.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Ignore case and accents. Username at prompt not required to match case or accents.	<i>enable</i>	Do not ignore case and accents. Username at prompt must be an exact match.			
Option	Description									
<i>disable</i>	Ignore case and accents. Username at prompt not required to match case or accents.									
<i>enable</i>	Do not ignore case and accents. Username at prompt must be an exact match.									

## config user setting

Configure user authentication setting.

```

config user setting
  Description: Configure user authentication setting.
  set auth-type {option1}, {option2}, ...
  set auth-cert {string}
  set auth-ca-cert {string}
  set auth-secure-http [enable|disable]
  set auth-http-basic [enable|disable]
  set auth-ssl-allow-renegotiation [enable|disable]
  set auth-src-mac [enable|disable]
  set auth-on-demand [always|implicitly]
  set auth-timeout {integer}
  set auth-timeout-type [idle-timeout|hard-timeout|...]
  set auth-portal-timeout {integer}

```

```

set radius-ses-timeout-act [hard-timeout|ignore-timeout]
set auth-blackout-time {integer}
set auth-invalid-max {integer}
set auth-lockout-threshold {integer}
set auth-lockout-duration {integer}
set per-policy-disclaimer [enable|disable]
config auth-ports
    Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
    TELNET.
    edit <id>
        set type [http|https|...]
        set port {integer}
    next
end
set auth-ssl-min-proto-version [default|SSLv3|...]
end

```

## config user setting

Parameter	Description	Type	Size	Default										
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http</i></td> <td>Allow HTTP authentication.</td> </tr> <tr> <td><i>https</i></td> <td>Allow HTTPS authentication.</td> </tr> <tr> <td><i>ftp</i></td> <td>Allow FTP authentication.</td> </tr> <tr> <td><i>telnet</i></td> <td>Allow TELNET authentication.</td> </tr> </tbody> </table>	Option	Description	<i>http</i>	Allow HTTP authentication.	<i>https</i>	Allow HTTPS authentication.	<i>ftp</i>	Allow FTP authentication.	<i>telnet</i>	Allow TELNET authentication.			
Option	Description													
<i>http</i>	Allow HTTP authentication.													
<i>https</i>	Allow HTTPS authentication.													
<i>ftp</i>	Allow FTP authentication.													
<i>telnet</i>	Allow TELNET authentication.													
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35											
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35											
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-	disable										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow SSL re-negotiation.</td> </tr> <tr> <td><i>disable</i></td> <td>Forbid SSL re-negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow SSL re-negotiation.	<i>disable</i>	Forbid SSL re-negotiation.					
Option	Description											
<i>enable</i>	Allow SSL re-negotiation.											
<i>disable</i>	Forbid SSL re-negotiation.											
auth-src-mac	Enable/disable source MAC for user identity.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable source MAC for user identity.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable source MAC for user identity.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable source MAC for user identity.	<i>disable</i>	Disable source MAC for user identity.					
Option	Description											
<i>enable</i>	Enable source MAC for user identity.											
<i>disable</i>	Disable source MAC for user identity.											
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-	implicitly								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>always</i></td> <td>Always trigger firewall authentication on demand.</td> </tr> <tr> <td><i>implicitly</i></td> <td>Implicitly trigger firewall authentication on demand.</td> </tr> </tbody> </table>	Option	Description	<i>always</i>	Always trigger firewall authentication on demand.	<i>implicitly</i>	Implicitly trigger firewall authentication on demand.					
Option	Description											
<i>always</i>	Always trigger firewall authentication on demand.											
<i>implicitly</i>	Implicitly trigger firewall authentication on demand.											
auth-timeout	Time in minutes before the firewall user authentication timeout requires the user to re-authenticate.	integer	Minimum value: 1 Maximum value: 1440	5								
auth-timeout-type	Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.	option	-	idle-timeout								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>idle-timeout</i></td> <td>Idle timeout.</td> </tr> <tr> <td><i>hard-timeout</i></td> <td>Hard timeout.</td> </tr> <tr> <td><i>new-session</i></td> <td>New session timeout.</td> </tr> </tbody> </table>	Option	Description	<i>idle-timeout</i>	Idle timeout.	<i>hard-timeout</i>	Hard timeout.	<i>new-session</i>	New session timeout.			
Option	Description											
<i>idle-timeout</i>	Idle timeout.											
<i>hard-timeout</i>	Hard timeout.											
<i>new-session</i>	New session timeout.											
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate .	integer	Minimum value: 1 Maximum value: 30	3								

Parameter	Description	Type	Size	Default												
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hard-timeout</i></td> <td>Use session timeout from RADIUS as hard-timeout.</td> </tr> <tr> <td><i>ignore-timeout</i></td> <td>Ignore session timeout from RADIUS.</td> </tr> </tbody> </table>	Option	Description	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.									
Option	Description															
<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.															
<i>ignore-timeout</i>	Ignore session timeout from RADIUS.															
auth-blackout-time	Time in seconds an IP address is denied access after failing to authenticate five times within one minute.	integer	Minimum value: 0 Maximum value: 3600	0												
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100	5												
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10	3												
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295	0												
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable per policy disclaimer.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable per policy disclaimer.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable per policy disclaimer.	<i>disable</i>	Disable per policy disclaimer.									
Option	Description															
<i>enable</i>	Enable per policy disclaimer.															
<i>disable</i>	Disable per policy disclaimer.															
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

## config auth-ports

Parameter	Description	Type	Size	Default										
type	Service type.	option	-	http										
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>http</i></td><td>HTTP service.</td></tr><tr><td><i>https</i></td><td>HTTPS service.</td></tr><tr><td><i>ftp</i></td><td>FTP service.</td></tr><tr><td><i>telnet</i></td><td>TELNET service.</td></tr></tbody></table>	Option	Description	<i>http</i>	HTTP service.	<i>https</i>	HTTPS service.	<i>ftp</i>	FTP service.	<i>telnet</i>	TELNET service.			
Option	Description													
<i>http</i>	HTTP service.													
<i>https</i>	HTTPS service.													
<i>ftp</i>	FTP service.													
<i>telnet</i>	TELNET service.													
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024										

## config user peer

Configure peer users.

```
config user peer
  Description: Configure peer users.
  edit <name>
    set mandatory-ca-verify [enable|disable]
    set ca {string}
    set subject {string}
    set cn {string}
    set cn-type [string|email|...]
    set ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set ldap-mode [password|principal-name]
    set ocsf-override-server {string}
    set two-factor [enable|disable]
    set passwd {password}
  next
end
```

## config user peer

Parameter	Description	Type	Size	Default
mandatory-ca-verify	Determine what happens to the peer if the CA certificate is not installed. Disable to automatically consider the peer certificate as valid.	option	-	enable

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
ca	Name of the CA certificate.	string	Maximum length: 127													
subject	Peer certificate name constraints.	string	Maximum length: 255													
cn	Peer certificate common name.	string	Maximum length: 255													
cn-type	Peer certificate common name type.	option	-	string												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>string</i></td> <td>Normal string.</td> </tr> <tr> <td><i>email</i></td> <td>Email address.</td> </tr> <tr> <td><i>FQDN</i></td> <td>Fully Qualified Domain Name.</td> </tr> <tr> <td><i>ipv4</i></td> <td>IPv4 address.</td> </tr> <tr> <td><i>ipv6</i></td> <td>IPv6 address.</td> </tr> </tbody> </table>	Option	Description	<i>string</i>	Normal string.	<i>email</i>	Email address.	<i>FQDN</i>	Fully Qualified Domain Name.	<i>ipv4</i>	IPv4 address.	<i>ipv6</i>	IPv6 address.			
Option	Description															
<i>string</i>	Normal string.															
<i>email</i>	Email address.															
<i>FQDN</i>	Fully Qualified Domain Name.															
<i>ipv4</i>	IPv4 address.															
<i>ipv6</i>	IPv6 address.															
ldap-server	Name of an LDAP server defined under the user ldap command. Performs client access rights check.	string	Maximum length: 35													
ldap-username	Username for LDAP server bind.	string	Maximum length: 35													
ldap-password	Password for LDAP server bind.	password	Not Specified													
ldap-mode	Mode for LDAP peer authentication.	option	-	password												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>password</i></td> <td>Username/password.</td> </tr> <tr> <td><i>principal-name</i></td> <td>Principal name.</td> </tr> </tbody> </table>	Option	Description	<i>password</i>	Username/password.	<i>principal-name</i>	Principal name.									
Option	Description															
<i>password</i>	Username/password.															
<i>principal-name</i>	Principal name.															
ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35													
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-	disable												



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable 2-factor authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 2-factor authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable 2-factor authentication.	<i>disable</i>	Disable 2-factor authentication.			
Option	Description									
<i>enable</i>	Enable 2-factor authentication.									
<i>disable</i>	Disable 2-factor authentication.									
passwd	Peer's password used for two-factor authentication.	password	Not Specified							

## config user peergrp

Configure peer groups.

```
config user peergrp
  Description: Configure peer groups.
  edit <name>
    set member <name1>, <name2>, ...
  next
end
```

## config user peergrp

Parameter	Description	Type	Size	Default
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	

## config user quarantine

Configure quarantine support.

```
config user quarantine
  Description: Configure quarantine support.
  set quarantine [enable|disable]
  set traffic-policy {string}
  set firewall-groups {string}
  config targets
    Description: Quarantine entry to hold multiple MACs.
    edit <entry>
      set description {string}
      config macs
        Description: Quarantine MACs.
        edit <mac>
          set description {string}
          set drop [disable|enable]
          set parent {string}
        next
      end
    next
  end
end
```

end

## config user quarantine

Parameter	Description	Type	Size	Default						
quarantine	Enable/disable quarantine.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable quarantine.</td></tr><tr><td><i>disable</i></td><td>Disable quarantine.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable quarantine.	<i>disable</i>	Disable quarantine.			
Option	Description									
<i>enable</i>	Enable quarantine.									
<i>disable</i>	Disable quarantine.									
traffic-policy	Traffic policy for quarantined MACs.	string	Maximum length: 63							
firewall-groups	Firewall address group which includes all quarantine MAC address.	string	Maximum length: 79							

## config targets

Parameter	Description	Type	Size	Default
description	Description for the quarantine entry.	string	Maximum length: 63	

## config macs

Parameter	Description	Type	Size	Default						
description	Description for the quarantine MAC.	string	Maximum length: 63							
drop	Enable/Disable dropping of quarantined device traffic	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Sends quarantined device traffic to FortiGate.</td></tr><tr><td><i>enable</i></td><td>Blocks quarantined device traffic to FortiGate.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Sends quarantined device traffic to FortiGate.	<i>enable</i>	Blocks quarantined device traffic to FortiGate.			
Option	Description									
<i>disable</i>	Sends quarantined device traffic to FortiGate.									
<i>enable</i>	Blocks quarantined device traffic to FortiGate.									
parent	Parent entry name.	string	Maximum length: 63							

## config user group

Configure user groups.

```
config user group
  Description: Configure user groups.
  edit <name>
    set id {integer}
```

```

set group-type [firewall|fsso-service|...]
set authtimeout {integer}
set auth-concurrent-override [enable|disable]
set auth-concurrent-value {integer}
set http-digest-realm {string}
set sso-attribute-value {string}
set member <name1>, <name2>, ...
config match
  Description: Group matches.
  edit <id>
    set server-name {string}
    set group-name {string}
  next
end
set user-id [email|auto-generate|...]
set password [auto-generate|specify|...]
set user-name [disable|enable]
set sponsor [optional|mandatory|...]
set company [optional|mandatory|...]
set email [disable|enable]
set mobile-phone [disable|enable]
set sms-server [fortiguard|custom]
set sms-custom-server {string}
set expire-type [immediately|first-successful-login]
set expire {integer}
set max-accounts {integer}
set multiple-guest-add [disable|enable]
config guest
  Description: Guest User.
  edit <id>
    set user-id {string}
    set name {string}
    set password {password}
    set mobile-phone {string}
    set sponsor {string}
    set company {string}
    set email {string}
    set expiration {user}
    set comment {var-string}
  next
end
next
end

```

## config user group

Parameter	Description	Type	Size	Default
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default										
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-	firewall										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>firewall</i></td> <td>Firewall.</td> </tr> <tr> <td><i>fss-service</i></td> <td>Fortinet Single Sign-On Service.</td> </tr> <tr> <td><i>rsso</i></td> <td>RADIUS based Single Sign-On Service.</td> </tr> <tr> <td><i>guest</i></td> <td>Guest.</td> </tr> </tbody> </table>	Option	Description	<i>firewall</i>	Firewall.	<i>fss-service</i>	Fortinet Single Sign-On Service.	<i>rsso</i>	RADIUS based Single Sign-On Service.	<i>guest</i>	Guest.			
Option	Description													
<i>firewall</i>	Firewall.													
<i>fss-service</i>	Fortinet Single Sign-On Service.													
<i>rsso</i>	RADIUS based Single Sign-On Service.													
<i>guest</i>	Guest.													
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 Maximum value: 43200	0										
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable auth-concurrent-override.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable auth-concurrent-override.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable auth-concurrent-override.	<i>disable</i>	Disable auth-concurrent-override.							
Option	Description													
<i>enable</i>	Enable auth-concurrent-override.													
<i>disable</i>	Disable auth-concurrent-override.													
auth-concurrent-value	Maximum number of concurrent authenticated connections per user .	integer	Minimum value: 0 Maximum value: 100	0										
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35											
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511											
member <name>	Names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Group member name.	string	Maximum length: 511											
user-id	Guest user ID type.	option	-	email										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>email</i></td> <td>Email address.</td> </tr> <tr> <td><i>auto-generate</i></td> <td>Automatically generate.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify.</td> </tr> </tbody> </table>	Option	Description	<i>email</i>	Email address.	<i>auto-generate</i>	Automatically generate.	<i>specify</i>	Specify.					
Option	Description													
<i>email</i>	Email address.													
<i>auto-generate</i>	Automatically generate.													
<i>specify</i>	Specify.													

Parameter	Description	Type	Size	Default								
password	Guest user password type.	option	-	auto-generate								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto-generate</i></td> <td>Automatically generate.</td> </tr> <tr> <td><i>specify</i></td> <td>Specify.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> </tbody> </table>	Option	Description	<i>auto-generate</i>	Automatically generate.	<i>specify</i>	Specify.	<i>disable</i>	Disable.			
Option	Description											
<i>auto-generate</i>	Automatically generate.											
<i>specify</i>	Specify.											
<i>disable</i>	Disable.											
user-name	Enable/disable the guest user name entry.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.					
Option	Description											
<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.											
sponsor	Set the action for the sponsor guest user field.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>optional</i></td> <td>Optional.</td> </tr> <tr> <td><i>mandatory</i></td> <td>Mandatory.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> </tbody> </table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
Option	Description											
<i>optional</i>	Optional.											
<i>mandatory</i>	Mandatory.											
<i>disabled</i>	Disabled.											
company	Set the action for the company guest user field.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>optional</i></td> <td>Optional.</td> </tr> <tr> <td><i>mandatory</i></td> <td>Mandatory.</td> </tr> <tr> <td><i>disabled</i></td> <td>Disabled.</td> </tr> </tbody> </table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
Option	Description											
<i>optional</i>	Optional.											
<i>mandatory</i>	Mandatory.											
<i>disabled</i>	Disabled.											
email	Enable/disable the guest user email address field.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.					
Option	Description											
<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.											
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.					
Option	Description											
<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.											

Parameter	Description	Type	Size	Default						
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fortiguard</i></td> <td>Send SMS by FortiGuard.</td> </tr> <tr> <td><i>custom</i></td> <td>Send SMS by custom server.</td> </tr> </tbody> </table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.			
Option	Description									
<i>fortiguard</i>	Send SMS by FortiGuard.									
<i>custom</i>	Send SMS by custom server.									
sms-custom-server	SMS server.	string	Maximum length: 35							
expire-type	Determine when the expiration countdown begins.	option	-	immediately						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>immediately</i></td> <td>Immediately.</td> </tr> <tr> <td><i>first-successful-login</i></td> <td>First successful login.</td> </tr> </tbody> </table>	Option	Description	<i>immediately</i>	Immediately.	<i>first-successful-login</i>	First successful login.			
Option	Description									
<i>immediately</i>	Immediately.									
<i>first-successful-login</i>	First successful login.									
expire	Time in seconds before guest user accounts expire.	integer	Minimum value: 1 Maximum value: 31536000	14400						
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 500 **	0						
multiple-guest-add	Enable/disable addition of multiple guests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.			
Option	Description									
<i>disable</i>	Enable setting.									
<i>enable</i>	Disable setting.									

\*\* Values may differ between models.

### config match

Parameter	Description	Type	Size	Default
server-name	Name of remote auth server.	string	Maximum length: 35	
group-name	Name of matching user or group on remote authentication server.	string	Maximum length: 511	

## config guest

Parameter	Description	Type	Size	Default
user-id	Guest ID.	string	Maximum length: 64	
name	Guest name.	string	Maximum length: 64	
password	Guest password.	password	Not Specified	
mobile-phone	Mobile phone.	string	Maximum length: 35	
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35	
company	Set the action for the company guest user field.	string	Maximum length: 35	
email	Email.	string	Maximum length: 64	
expiration	Expire time.	user	Not Specified	
comment	Comment.	var-string	Maximum length: 255	

## config user security-exempt-list

Configure security exemption list.

```
config user security-exempt-list
  Description: Configure security exemption list.
  edit <name>
    set description {string}
    config rule
      Description: Configure rules for exempting users from captive portal authentication.
      edit <id>
        set srcaddr <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set service <name1>, <name2>, ...
      next
    end
  next
end
```

## config user security-exempt-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	

## config rule

Parameter	Description	Type	Size	Default
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79	
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79	
service <name>	Destination services. Service name.	string	Maximum length: 79	

## config user nac-policy

Configure NAC policy matching pattern to identify matching NAC devices.

```
config user nac-policy
  Description: Configure NAC policy matching pattern to identify matching NAC devices.
  edit <name>
    set description {string}
    set category [device|firewall-user|...]
    set status [enable|disable]
    set mac {string}
    set hw-vendor {string}
    set type {string}
    set family {string}
    set os {string}
    set hw-version {string}
    set sw-version {string}
    set host {string}
    set user {string}
    set src {string}
    set user-group {string}
    set ems-tag {string}
    set switch-fortilink {string}
    set switch-scope <switch-id1>, <switch-id2>, ...
    set switch-auto-auth [global|disable|...]
    set switch-port-policy {string}
    set switch-mac-policy {string}
  next
end
```



## config user nac-policy

Parameter	Description	Type	Size	Default								
description	Description for the NAC policy matching pattern.	string	Maximum length: 63									
category	Category of NAC policy.	option	-	device								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>device</i></td> <td>Device category.</td> </tr> <tr> <td><i>firewall-user</i></td> <td>Firewall user category.</td> </tr> <tr> <td><i>ems-tag</i></td> <td>EMS Tag category.</td> </tr> </tbody> </table>	Option	Description	<i>device</i>	Device category.	<i>firewall-user</i>	Firewall user category.	<i>ems-tag</i>	EMS Tag category.			
Option	Description											
<i>device</i>	Device category.											
<i>firewall-user</i>	Firewall user category.											
<i>ems-tag</i>	EMS Tag category.											
status	Enable/disable NAC policy.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NAC policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NAC policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NAC policy.	<i>disable</i>	Disable NAC policy.					
Option	Description											
<i>enable</i>	Enable NAC policy.											
<i>disable</i>	Disable NAC policy.											
mac	NAC policy matching MAC address.	string	Maximum length: 17									
hw-vendor	NAC policy matching hardware vendor.	string	Maximum length: 15									
type	NAC policy matching type.	string	Maximum length: 15									
family	NAC policy matching family.	string	Maximum length: 31									
os	NAC policy matching operating system.	string	Maximum length: 31									
hw-version	NAC policy matching hardware version.	string	Maximum length: 15									
sw-version	NAC policy matching software version.	string	Maximum length: 15									
host	NAC policy matching host.	string	Maximum length: 64									
user	NAC policy matching user.	string	Maximum length: 64									
src	NAC policy matching source.	string	Maximum length: 15									
user-group	NAC policy matching user group.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default								
ems-tag	NAC policy matching EMS tag.	string	Maximum length: 79									
switch-fortilink	FortiLink interface for which this NAC policy belongs to.	string	Maximum length: 15									
switch-scope <switch-id>	List of managed FortiSwitches on which NAC policy can be applied. Managed FortiSwitch name from available options.	string	Maximum length: 79									
switch-auto-auth	NAC device auto authorization when discovered and nac-policy matched.	option	-	global								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Follows global auto-auth configuration under nac-settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NAC device auto authorization.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable NAC device auto authorization.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Follows global auto-auth configuration under nac-settings.	<i>disable</i>	Disable NAC device auto authorization.	<i>enable</i>	Enable NAC device auto authorization.			
Option	Description											
<i>global</i>	Follows global auto-auth configuration under nac-settings.											
<i>disable</i>	Disable NAC device auto authorization.											
<i>enable</i>	Enable NAC device auto authorization.											
switch-port-policy	switch-port-policy to be applied on the matched NAC policy.	string	Maximum length: 63									
switch-mac-policy	switch-mac-policy to be applied on the matched NAC policy.	string	Maximum length: 63									

## voip

This section includes syntax for the following commands:

- [config voip profile on page 1195](#)

### config voip profile

Configure VoIP profiles.

```
config voip profile
  Description: Configure VoIP profiles.
  edit <name>
    set comment {var-string}
  config sip
    Description: SIP.
    set status [disable|enable]
    set rtp [disable|enable]
    set nat-port-range {user}
    set open-register-pinhole [disable|enable]
    set open-contact-pinhole [disable|enable]
    set strict-register [disable|enable]
    set register-rate {integer}
    set invite-rate {integer}
    set max-dialogs {integer}
    set max-line-length {integer}
    set block-long-lines [disable|enable]
    set block-unknown [disable|enable]
    set call-keepalive {integer}
    set block-ack [disable|enable]
    set block-bye [disable|enable]
    set block-cancel [disable|enable]
    set block-info [disable|enable]
    set block-invite [disable|enable]
    set block-message [disable|enable]
    set block-notify [disable|enable]
    set block-options [disable|enable]
    set block-prack [disable|enable]
    set block-publish [disable|enable]
    set block-refer [disable|enable]
    set block-register [disable|enable]
    set block-subscribe [disable|enable]
    set block-update [disable|enable]
    set register-contact-trace [disable|enable]
    set open-via-pinhole [disable|enable]
    set open-record-route-pinhole [disable|enable]
    set rfc2543-branch [disable|enable]
    set log-violations [disable|enable]
    set log-call-summary [disable|enable]
    set nat-trace [disable|enable]
    set subscribe-rate {integer}
    set message-rate {integer}
```

---

```
set notify-rate {integer}
set refer-rate {integer}
set update-rate {integer}
set options-rate {integer}
set ack-rate {integer}
set prack-rate {integer}
set info-rate {integer}
set publish-rate {integer}
set bye-rate {integer}
set cancel-rate {integer}
set preserve-override [disable|enable]
set no-sdp-fixup [disable|enable]
set contact-fixup [disable|enable]
set max-idle-dialogs {integer}
set block-geo-red-options [disable|enable]
set hosted-nat-traversal [disable|enable]
set hnt-restrict-source-ip [disable|enable]
set max-body-length {integer}
set unknown-header [discard|pass|...]
set malformed-request-line [discard|pass|...]
set malformed-header-via [discard|pass|...]
set malformed-header-from [discard|pass|...]
set malformed-header-to [discard|pass|...]
set malformed-header-call-id [discard|pass|...]
set malformed-header-cseq [discard|pass|...]
set malformed-header-rack [discard|pass|...]
set malformed-header-rseq [discard|pass|...]
set malformed-header-contact [discard|pass|...]
set malformed-header-record-route [discard|pass|...]
set malformed-header-route [discard|pass|...]
set malformed-header-expires [discard|pass|...]
set malformed-header-content-type [discard|pass|...]
set malformed-header-content-length [discard|pass|...]
set malformed-header-max-forwards [discard|pass|...]
set malformed-header-allow [discard|pass|...]
set malformed-header-p-asserted-identity [discard|pass|...]
set malformed-header-sdp-v [discard|pass|...]
set malformed-header-sdp-o [discard|pass|...]
set malformed-header-sdp-s [discard|pass|...]
set malformed-header-sdp-i [discard|pass|...]
set malformed-header-sdp-c [discard|pass|...]
set malformed-header-sdp-b [discard|pass|...]
set malformed-header-sdp-z [discard|pass|...]
set malformed-header-sdp-k [discard|pass|...]
set malformed-header-sdp-a [discard|pass|...]
set malformed-header-sdp-t [discard|pass|...]
set malformed-header-sdp-r [discard|pass|...]
set malformed-header-sdp-m [discard|pass|...]
set provisional-invite-expiry-time {integer}
set ips-rtp [disable|enable]
set ssl-mode [off|full]
set ssl-send-empty-frags [enable|disable]
set ssl-client-renegotiation [allow|deny|...]
set ssl-algorithm [high|medium|...]
set ssl-pfs [require|deny|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-max-version [ssl-3.0|tls-1.0|...]
```

```

        set ssl-client-certificate {string}
        set ssl-server-certificate {string}
        set ssl-auth-client {string}
        set ssl-auth-server {string}
    end
    config sccp
        Description: SCCP.
        set status [disable|enable]
        set block-mcast [disable|enable]
        set verify-header [disable|enable]
        set log-call-summary [disable|enable]
        set log-violations [disable|enable]
        set max-calls {integer}
    end
end
next
end

```

## config voip profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	

## config sip

Parameter	Description	Type	Size	Default						
status	Enable/disable SIP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
rtp	Enable/disable create pinholes for RTP traffic to traverse firewall.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
nat-port-range	RTP NAT port range.	user	Not Specified	5117-65533						
open-register-pinhole	Enable/disable open pinhole for REGISTER Contact port.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
open-contact-pinhole	Enable/disable open pinhole for non-REGISTER Contact port.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
strict-register	Enable/disable only allow the registrar to connect.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
register-rate	REGISTER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
invite-rate	INVITE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-dialogs	Maximum number of concurrent calls/dialogs (per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-line-length	Maximum SIP header line length .	integer	Minimum value: 78 Maximum value: 4096	998						
block-long-lines	Enable/disable block requests with headers exceeding max-line-length.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-unknown	Block unrecognized SIP requests .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
call-keepalive	Continue tracking calls with no RTP for this many minutes.	integer	Minimum value: 0 Maximum value: 10080	0						
block-ack	Enable/disable block ACK requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-bye	Enable/disable block BYE requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-cancel	Enable/disable block CANCEL requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-info	Enable/disable block INFO requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-invite	Enable/disable block INVITE requests.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-message	Enable/disable block MESSAGE requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-notify	Enable/disable block NOTIFY requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-options	Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-prack	Enable/disable block prack requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-publish	Enable/disable block PUBLISH requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-refer	Enable/disable block REFER requests.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-register	Enable/disable block REGISTER requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-subscribe	Enable/disable block SUBSCRIBE requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-update	Enable/disable block UPDATE requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
register-contact-trace	Enable/disable trace original IP/port within the contact header of REGISTER requests.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
open-via-pinhole	Enable/disable open pinhole for Via port.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
open-record-route-pinhole	Enable/disable open pinhole for Record-Route port.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
rfc2543-branch	Enable/disable support via branch compliant with RFC 2543.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
log-violations	Enable/disable logging of SIP violations.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
log-call-summary	Enable/disable logging of SIP call summary.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
nat-trace	Enable/disable preservation of original IP in SDP i line.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
subscribe-rate	SUBSCRIBE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
message-rate	MESSAGE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default
notify-rate	NOTIFY request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
refer-rate	REFER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
update-rate	UPDATE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
options-rate	OPTIONS request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
ack-rate	ACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
prack-rate	PRACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
info-rate	INFO request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
publish-rate	PUBLISH request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
bye-rate	BYE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
cancel-rate	CANCEL request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
preserve-override	Override i line to preserve original IPS .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
no-sdp-fixup	Enable/disable no SDP fix-up.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
contact-fixup	Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
max-idle-dialogs	Maximum number established but idle dialogs to retain (per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						
block-geo-red-options	Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									

Parameter	Description	Type	Size	Default								
hosted-nat-traversal	Hosted NAT Traversal (HNT).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
hnt-restrict-source-ip	Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
max-body-length	Maximum SIP message body length (0 meaning no limit).	integer	Minimum value: 0 Maximum value: 4294967295	0								
unknown-header	Action for unknown SIP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-request-line	Action for malformed request line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-via	Action for malformed VIA header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.							
Option	Description											
<i>discard</i>	Discard malformed messages.											

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.					
Option	Description											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-from	Action for malformed From header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-to	Action for malformed To header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-call-id	Action for malformed Call-ID header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-cseq	Action for malformed CSeq header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-rack	Action for malformed RACK header.	option	-	pass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-rseq	Action for malformed RSeq header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-contact	Action for malformed Contact header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-record-route	Action for malformed Record-Route header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-route	Action for malformed Route header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-expires	Action for malformed Expires header.	option	-	pass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-content-type	Action for malformed Content-Type header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-content-length	Action for malformed Content-Length header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-max-forwards	Action for malformed Max-Forwards header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-allow	Action for malformed Allow header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											



Parameter	Description	Type	Size	Default								
malformed-header-p-asserted-identity	Action for malformed P-Asserted-Identity header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-v	Action for malformed SDP v line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-o	Action for malformed SDP o line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-s	Action for malformed SDP s line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-i	Action for malformed SDP i line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.					
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>respond</i>	Respond with error code.							
Option	Description											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-c	Action for malformed SDP c line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-b	Action for malformed SDP b line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-z	Action for malformed SDP z line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-k	Action for malformed SDP k line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-a	Action for malformed SDP a line.	option	-	pass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-t	Action for malformed SDP t line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-r	Action for malformed SDP r line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-sdp-m	Action for malformed SDP m line.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discard</i></td> <td>Discard malformed messages.</td> </tr> <tr> <td><i>pass</i></td> <td>Bypass malformed messages.</td> </tr> <tr> <td><i>respond</i></td> <td>Respond with error code.</td> </tr> </tbody> </table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
provisional-invite-expiry-time	Expiry time for provisional INVITE .	integer	Minimum value: 10 Maximum value: 3600	210								
ips-rtp	Enable/disable allow IPS on RTP.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
ssl-mode	SSL/TLS mode for encryption & decryption of traffic.	option	-	off								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>off</i></td> <td>No SSL.</td> </tr> <tr> <td><i>full</i></td> <td>Client to FortiGate and FortiGate to Server SSL.</td> </tr> </tbody> </table>	Option	Description	<i>off</i>	No SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.					
Option	Description											
<i>off</i>	No SSL.											
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.											
ssl-send-empty-frags	Send empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Send empty fragments.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not send empty fragments.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.					
Option	Description											
<i>enable</i>	Send empty fragments.											
<i>disable</i>	Do not send empty fragments.											
ssl-client-renegotiation	Allow/block client renegotiation by server.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow a SSL client to renegotiate.</td> </tr> <tr> <td><i>deny</i></td> <td>Abort any SSL connection that attempts to renegotiate.</td> </tr> <tr> <td><i>secure</i></td> <td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.			
Option	Description											
<i>allow</i>	Allow a SSL client to renegotiate.											
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.											
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.											
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High encryption. Allow only AES and ChaCha.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
Option	Description											
<i>high</i>	High encryption. Allow only AES and ChaCha.											
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											
ssl-pfs	SSL Perfect Forward Secrecy.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>require</i></td> <td>PFS mandatory.</td> </tr> <tr> <td><i>deny</i></td> <td>PFS rejected.</td> </tr> <tr> <td><i>allow</i></td> <td>PFS allowed.</td> </tr> </tbody> </table>	Option	Description	<i>require</i>	PFS mandatory.	<i>deny</i>	PFS rejected.	<i>allow</i>	PFS allowed.			
Option	Description											
<i>require</i>	PFS mandatory.											
<i>deny</i>	PFS rejected.											
<i>allow</i>	PFS allowed.											
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.							
Option	Description											
<i>ssl-3.0</i>	SSL 3.0.											

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.					
Option	Description															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.3												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ssl-3.0</i></td> <td>SSL 3.0.</td> </tr> <tr> <td><i>tls-1.0</i></td> <td>TLS 1.0.</td> </tr> <tr> <td><i>tls-1.1</i></td> <td>TLS 1.1.</td> </tr> <tr> <td><i>tls-1.2</i></td> <td>TLS 1.2.</td> </tr> <tr> <td><i>tls-1.3</i></td> <td>TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-client-certificate	Name of Certificate to offer to server if requested.	string	Maximum length: 35													
ssl-server-certificate	Name of Certificate return to the client in every SSL connection.	string	Maximum length: 35													
ssl-auth-client	Require a client certificate and authenticate it with the peer/peergrp.	string	Maximum length: 35													
ssl-auth-server	Authenticate the server's certificate with the peer/peergrp.	string	Maximum length: 35													

### config sccp

Parameter	Description	Type	Size	Default						
status	Enable/disable SCCP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
block-mcast	Enable/disable block multicast RTP connections.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
verify-header	Enable/disable verify SCCP header content.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
log-call-summary	Enable/disable log summary of SCCP calls.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
log-violations	Enable/disable logging of SCCP violations.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable status.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable status.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
max-calls	Maximum calls per minute per SCCP client (max 65535).	integer	Minimum value: 0 Maximum value: 65535	0						

## vpn

This section includes syntax for the following commands:

- [config vpn certificate local on page 1218](#)
- [config vpn ipsec tunnel details on page 1336](#)
- [config vpn ssl web realm on page 1226](#)
- [config vpn ipsec stats crypto on page 1336](#)
- [config vpn ipsec forticlient on page 1335](#)
- [config vpn ssl web host-check-software on page 1227](#)
- [config vpn pptp on page 1337](#)
- [config vpn certificate crl on page 1220](#)
- [config vpn ipsec phase2 on page 1289](#)
- [config vpn l2tp on page 1338](#)
- [config vpn ipsec manualkey on page 1298](#)
- [config vpn ipsec stats tunnel on page 1336](#)
- [config vpn ssl web user-bookmark on page 1251](#)
- [config vpn ipsec phase1 on page 1270](#)
- [config vpn status ssl hw-acceleration-status on page 1343](#)
- [config vpn ssl monitor on page 1270](#)
- [config vpn ipsec concentrator on page 1300](#)
- [config vpn ssl settings on page 1257](#)
- [config vpn ipsec tunnel name on page 1337](#)
- [config vpn certificate ocsf-server on page 1222](#)
- [config vpn ocvpn on page 1339](#)
- [config vpn certificate remote on page 1217](#)
- [config vpn ipsec phase1-interface on page 1300](#)
- [config vpn status ssl list on page 1343](#)
- [config vpn ssl web portal on page 1229](#)
- [config vpn certificate setting on page 1223](#)
- [config vpn ike gateway on page 1343](#)
- [config vpn ipsec phase2-interface on page 1324](#)
- [config vpn status l2tp on page 1343](#)
- [config vpn ssl web user-group-bookmark on page 1246](#)
- [config vpn certificate ca on page 1215](#)
- [config vpn status pptp on page 1343](#)
- [config vpn ipsec tunnel summary on page 1336](#)
- [config vpn ipsec manualkey-interface on page 1333](#)

### config vpn certificate ca

CA certificate.

```

config vpn certificate ca
  Description: CA certificate.
  edit <name>
    set ca {user}
    set range [global|vdom]
    set source [factory|user|...]
    set ssl-inspection-trusted [enable|disable]
    set scep-url {string}
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set source-ip {ipv4-address}
  next
end

```

## config vpn certificate ca

Parameter	Description	Type	Size	Default								
ca	CA certificate as a PEM file.	user	Not Specified									
range	Either global or VDOM IP address range for the CA certificate.	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Global range.</td> </tr> <tr> <td><i>vdom</i></td> <td>VDOM IP address range.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	CA certificate source type.	option	-	user								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>factory</i></td> <td>Factory installed certificate.</td> </tr> <tr> <td><i>user</i></td> <td>User generated certificate.</td> </tr> <tr> <td><i>bundle</i></td> <td>Bundle file certificate.</td> </tr> </tbody> </table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Trusted CA for SSL inspection.</td> </tr> <tr> <td><i>disable</i></td> <td>Untrusted CA for SSL inspection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Trusted CA for SSL inspection.	<i>disable</i>	Untrusted CA for SSL inspection.					
Option	Description											
<i>enable</i>	Trusted CA for SSL inspection.											
<i>disable</i>	Untrusted CA for SSL inspection.											
scep-url	URL of the SCEP server.	string	Maximum length: 255									



Parameter	Description	Type	Size	Default
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated .	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0

## config vpn certificate remote

Remote certificate as a PEM file.

```
config vpn certificate remote
  Description: Remote certificate as a PEM file.
  edit <name>
    set remote {user}
    set range [global|vdom]
    set source [factory|user|...]
  next
end
```

## config vpn certificate remote

Parameter	Description	Type	Size	Default						
remote	Remote certificate.	user	Not Specified							
range	Either the global or VDOM IP address range for the remote certificate.	option	-	vdom						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Global range.</td> </tr> <tr> <td><i>vdom</i></td> <td>VDOM IP address range.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.			
Option	Description									
<i>global</i>	Global range.									
<i>vdom</i>	VDOM IP address range.									
source	Remote certificate source type.	option	-	user						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>factory</i></td> <td>Factory installed certificate.</td> </tr> </tbody> </table>	Option	Description	<i>factory</i>	Factory installed certificate.					
Option	Description									
<i>factory</i>	Factory installed certificate.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		

## config vpn certificate local

Local keys and certificates.

```

config vpn certificate local
  Description: Local keys and certificates.
  edit <name>
    set password {password}
    set comments {string}
    set private-key {user}
    set certificate {user}
    set csr {user}
    set state {user}
    set scep-url {string}
    set range [global|vdom]
    set source [factory|user|...]
    set auto-regenerate-days {integer}
    set auto-regenerate-days-warning {integer}
    set scep-password {password}
    set ca-identifier {string}
    set name-encoding [printable|utf8]
    set source-ip {ipv4-address}
    set ike-localid {string}
    set ike-localid-type [asn1dn|fqdn]
    set enroll-protocol [none|scep|...]
    set cmp-server {string}
    set cmp-path {string}
    set cmp-server-cert {string}
    set cmp-regeneration-method [keyupate|renewal]
  next
end

```

## config vpn certificate local

Parameter	Description	Type	Size	Default
password	Password as a PEM file.	password	Not Specified	
comments	Comment.	string	Maximum length: 511	
private-key	PEM format key, encrypted with a password.	user	Not Specified	
certificate	PEM format certificate.	user	Not Specified	

Parameter	Description	Type	Size	Default								
csr	Certificate Signing Request.	user	Not Specified									
state	Certificate Signing Request State.	user	Not Specified									
scep-url	SCEP server URL.	string	Maximum length: 255									
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Global range.</td> </tr> <tr> <td><i>vdom</i></td> <td>VDOM IP address range.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>factory</i></td> <td>Factory installed certificate.</td> </tr> <tr> <td><i>user</i></td> <td>User generated certificate.</td> </tr> <tr> <td><i>bundle</i></td> <td>Bundle file certificate.</td> </tr> </tbody> </table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified									
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255									
name-encoding	Name encoding method for auto-regeneration.	option	-	printable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>printable</i></td> <td>Printable encoding (default).</td> </tr> <tr> <td><i>utf8</i></td> <td>UTF-8 encoding.</td> </tr> </tbody> </table>	Option	Description	<i>printable</i>	Printable encoding (default).	<i>utf8</i>	UTF-8 encoding.					
Option	Description											
<i>printable</i>	Printable encoding (default).											
<i>utf8</i>	UTF-8 encoding.											

Parameter	Description	Type	Size	Default								
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0								
ike-localid	Local ID the FortiGate uses for authentication as a VPN client.	string	Maximum length: 63									
ike-localid-type	IKE local ID type.	option	-	asn1dn								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>asn1dn</i></td> <td>ASN.1 distinguished name.</td> </tr> <tr> <td><i>fqdn</i></td> <td>Fully qualified domain name.</td> </tr> </tbody> </table>	Option	Description	<i>asn1dn</i>	ASN.1 distinguished name.	<i>fqdn</i>	Fully qualified domain name.					
Option	Description											
<i>asn1dn</i>	ASN.1 distinguished name.											
<i>fqdn</i>	Fully qualified domain name.											
enroll-protocol	Certificate enrollment protocol.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>None (default).</td> </tr> <tr> <td><i>scep</i></td> <td>Simple Certificate Enrollment Protocol.</td> </tr> <tr> <td><i>cmpv2</i></td> <td>Certificate Management Protocol Version 2.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	None (default).	<i>scep</i>	Simple Certificate Enrollment Protocol.	<i>cmpv2</i>	Certificate Management Protocol Version 2.			
Option	Description											
<i>none</i>	None (default).											
<i>scep</i>	Simple Certificate Enrollment Protocol.											
<i>cmpv2</i>	Certificate Management Protocol Version 2.											
cmp-server	'ADDRESS:PORT' for CMP server.	string	Maximum length: 63									
cmp-path	Path location inside CMP server.	string	Maximum length: 255									
cmp-server-cert	CMP server certificate.	string	Maximum length: 79									
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>keyupate</i></td> <td>Key Update.</td> </tr> <tr> <td><i>renewal</i></td> <td>Renewal.</td> </tr> </tbody> </table>	Option	Description	<i>keyupate</i>	Key Update.	<i>renewal</i>	Renewal.					
Option	Description											
<i>keyupate</i>	Key Update.											
<i>renewal</i>	Renewal.											

## config vpn certificate crl

Certificate Revocation List as a PEM file.

```
config vpn certificate crl
  Description: Certificate Revocation List as a PEM file.
  edit <name>
    set crl {user}
    set range [global|vdom]
    set source [factory|user|...]
    set update-vdom {string}
    set ldap-server {string}
```

```

set ldap-username {string}
set ldap-password {password}
set http-url {string}
set scep-url {string}
set scep-cert {string}
set update-interval {integer}
set source-ip {ipv4-address}
next
end

```

## config vpn certificate crl

Parameter	Description	Type	Size	Default								
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
range	Either global or VDOM IP address range for the certificate.	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>global</i></td> <td>Global range.</td> </tr> <tr> <td><i>vdom</i></td> <td>VDOM IP address range.</td> </tr> </tbody> </table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>factory</i></td> <td>Factory installed certificate.</td> </tr> <tr> <td><i>user</i></td> <td>User generated certificate.</td> </tr> <tr> <td><i>bundle</i></td> <td>Bundle file certificate.</td> </tr> </tbody> </table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									
ldap-password	LDAP server user password.	password	Not Specified									
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255									
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								

Parameter	Description	Type	Size	Default
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0

## config vpn certificate ocsf-server

OCSP server configuration.

```
config vpn certificate ocsf-server
  Description: OCSP server configuration.
  edit <name>
    set url {string}
    set cert {string}
    set secondary-url {string}
    set secondary-cert {string}
    set unavail-action [revoke|ignore]
    set source-ip {ipv4-address}
  next
end
```

## config vpn certificate ocsf-server

Parameter	Description	Type	Size	Default						
url	OCSP server URL.	string	Maximum length: 127							
cert	OCSP server certificate.	string	Maximum length: 127							
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127							
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127							
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-	revoke						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>revoke</i></td> <td>Revoke certificate if server is unavailable.</td> </tr> <tr> <td><i>ignore</i></td> <td>Ignore OCSP check if server is unavailable.</td> </tr> </tbody> </table>				Option	Description	<i>revoke</i>	Revoke certificate if server is unavailable.	<i>ignore</i>	Ignore OCSP check if server is unavailable.
Option	Description									
<i>revoke</i>	Revoke certificate if server is unavailable.									
<i>ignore</i>	Ignore OCSP check if server is unavailable.									
source-ip	Source IP address for communications to the OCSP server.	ipv4-address	Not Specified	0.0.0.0						

## config vpn certificate setting

VPN certificate setting.

```
config vpn certificate setting
  Description: VPN certificate setting.
  set oosp-status [enable|disable]
  set oosp-option [certificate|server]
  set ssl-ocsp-source-ip {ipv4-address}
  set oosp-default-server {string}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
  set check-ca-cert [enable|disable]
  set check-ca-chain [enable|disable]
  set subject-match [substring|value]
  set cn-match [substring|value]
  set strict-crl-check [enable|disable]
  set strict-ocsp-check [enable|disable]
  set ssl-min-prot-version [default|SSLv3|...]
  set cmp-save-extra-certs [enable|disable]
  set cmp-key-usage-checking [enable|disable]
  set certname-rsa1024 {string}
  set certname-rsa2048 {string}
  set certname-rsa4096 {string}
  set certname-dsa1024 {string}
  set certname-dsa2048 {string}
  set certname-ecdsa256 {string}
  set certname-ecdsa384 {string}
  set certname-ecdsa521 {string}
  set certname-ed25519 {string}
  set certname-ed448 {string}
end
```

## config vpn certificate setting

Parameter	Description	Type	Size	Default						
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-	server						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>certificate</i></td><td>Use URL from certificate.</td></tr><tr><td><i>server</i></td><td>Use URL from configured OCSP server.</td></tr></tbody></table>	Option	Description	<i>certificate</i>	Use URL from certificate.	<i>server</i>	Use URL from configured OCSP server.			
Option	Description									
<i>certificate</i>	Use URL from certificate.									
<i>server</i>	Use URL from configured OCSP server.									

Parameter	Description	Type	Size	Default								
ssl-ocsp-source-ip	Source IP address to use to communicate with the OCSP server.	ipv4-address	Not Specified	0.0.0.0								
ocsp-default-server	Default OCSP server.	string	Maximum length: 35									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of the user certificate.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of the user certificate.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of the user certificate.	<i>disable</i>	Disable verification of the user certificate.					
Option	Description											
<i>enable</i>	Enable verification of the user certificate.											
<i>disable</i>	Disable verification of the user certificate.											
check-ca-chain	Enable/disable verification of the entire certificate chain and pass authentication only if the chain is complete and all of the CAs in the chain are trusted .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of the entire certificate chain.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of the entire certificate chain.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of the entire certificate chain.	<i>disable</i>	Disable verification of the entire certificate chain.					
Option	Description											
<i>enable</i>	Enable verification of the entire certificate chain.											
<i>disable</i>	Disable verification of the entire certificate chain.											
subject-match	When searching for a matching certificate, control how to find matches in the certificate subject name.	option	-	substring								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>substring</i></td> <td>Find a match if any string in the certificate subject name matches the name being searched for.</td> </tr> <tr> <td><i>value</i></td> <td>Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.</td> </tr> </tbody> </table>	Option	Description	<i>substring</i>	Find a match if any string in the certificate subject name matches the name being searched for.	<i>value</i>	Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.					
Option	Description											
<i>substring</i>	Find a match if any string in the certificate subject name matches the name being searched for.											
<i>value</i>	Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.											
cn-match	When searching for a matching certificate, control how to find matches in the cn attribute of the certificate subject name.	option	-	substring								



Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>substring</i></td> <td>Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.</td> </tr> <tr> <td><i>value</i></td> <td>Find a match if the cn attribute value string is an exact match with the name being searched for.</td> </tr> </tbody> </table>	Option	Description	<i>substring</i>	Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.	<i>value</i>	Find a match if the cn attribute value string is an exact match with the name being searched for.									
Option	Description															
<i>substring</i>	Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.															
<i>value</i>	Find a match if the cn attribute value string is an exact match with the name being searched for.															
strict-crl-check	Enable/disable strict mode CRL checking.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strict mode CRL checking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strict mode CRL checking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strict mode CRL checking.	<i>disable</i>	Disable strict mode CRL checking.									
Option	Description															
<i>enable</i>	Enable strict mode CRL checking.															
<i>disable</i>	Disable strict mode CRL checking.															
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strict mode OCSP checking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strict mode OCSP checking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strict mode OCSP checking.	<i>disable</i>	Disable strict mode OCSP checking.									
Option	Description															
<i>enable</i>	Enable strict mode OCSP checking.															
<i>disable</i>	Disable strict mode OCSP checking.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Follow system global setting.</td> </tr> <tr> <td><i>SSLv3</i></td> <td>SSLv3.</td> </tr> <tr> <td><i>TLSv1</i></td> <td>TLSv1.</td> </tr> <tr> <td><i>TLSv1-1</i></td> <td>TLSv1.1.</td> </tr> <tr> <td><i>TLSv1-2</i></td> <td>TLSv1.2.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode .	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable saving extra certificates in CMP mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable saving extra certificates in CMP mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable saving extra certificates in CMP mode.	<i>disable</i>	Disable saving extra certificates in CMP mode.									
Option	Description															
<i>enable</i>	Enable saving extra certificates in CMP mode.															
<i>disable</i>	Disable saving extra certificates in CMP mode.															
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode .	option	-	enable												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable server certificate key usage checking in CMP mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable server certificate key usage checking in CMP mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable server certificate key usage checking in CMP mode.	<i>disable</i>	Disable server certificate key usage checking in CMP mode.			
Option	Description									
<i>enable</i>	Enable server certificate key usage checking in CMP mode.									
<i>disable</i>	Disable server certificate key usage checking in CMP mode.									
certname-rsa1024	1024 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA1024						
certname-rsa2048	2048 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA2048						
certname-rsa4096	4096 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA4096						
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA1024						
certname-dsa2048	2048 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA2048						
certname-ecdsa256	256 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA256						
certname-ecdsa384	384 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA384						
certname-ecdsa521	521 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA521						
certname-ed25519	253 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED25519						
certname-ed448	456 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED448						

## config vpn ssl web realm

Realm.

```
config vpn ssl web realm
  Description: Realm.
  edit <url-path>
    set max-concurrent-user {integer}
```

```

set login-page {var-string}
set virtual-host {var-string}
set virtual-host-only [enable|disable]
set radius-server {string}
set nas-ip {ipv4-address}
set radius-port {integer}
next
end

```

## config vpn ssl web realm

Parameter	Description	Type	Size	Default						
max-concurrent-user	Maximum concurrent users .	integer	Minimum value: 0 Maximum value: 65535	0						
login-page	Replacement HTML for SSL-VPN login page.	var-string	Maximum length: 32768							
virtual-host	Virtual host name for realm.	var-string	Maximum length: 255							
virtual-host-only	Enable/disable enforcement of virtual host method for SSL-VPN client access.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
radius-server	RADIUS server associated with realm.	string	Maximum length: 35							
nas-ip	IP address used as a NAS-IP to communicate with the RADIUS server.	ipv4-address	Not Specified	0.0.0.0						
radius-port	RADIUS service port number .	integer	Minimum value: 0 Maximum value: 65535	0						

## config vpn ssl web host-check-software

SSL-VPN host check software.

```

config vpn ssl web host-check-software
  Description: SSL-VPN host check software.
  edit <name>

```

```

set os-type [windows|macos]
set type [av|fw]
set version {string}
set guid {user}
config check-item-list
  Description: Check item list.
  edit <id>
    set action [require|deny]
    set type [file|registry|...]
    set target {string}
    set version {string}
    set md5s <id1>, <id2>, ...
  next
end
next
end

```

## config vpn ssl web host-check-software

Parameter	Description	Type	Size	Default						
os-type	OS type.	option	-	windows						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>windows</i></td> <td>Microsoft Windows operating system.</td> </tr> <tr> <td><i>macos</i></td> <td>Apple MacOS operating system.</td> </tr> </tbody> </table>	Option	Description	<i>windows</i>	Microsoft Windows operating system.	<i>macos</i>	Apple MacOS operating system.			
Option	Description									
<i>windows</i>	Microsoft Windows operating system.									
<i>macos</i>	Apple MacOS operating system.									
type	Type.	option	-	av						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>av</i></td> <td>AntiVirus.</td> </tr> <tr> <td><i>fw</i></td> <td>Firewall.</td> </tr> </tbody> </table>	Option	Description	<i>av</i>	AntiVirus.	<i>fw</i>	Firewall.			
Option	Description									
<i>av</i>	AntiVirus.									
<i>fw</i>	Firewall.									
version	Version.	string	Maximum length: 35							
guid	Globally unique ID.	user	Not Specified							

## config check-item-list

Parameter	Description	Type	Size	Default						
action	Action.	option	-	require						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>require</i></td> <td>Require.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny.</td> </tr> </tbody> </table>	Option	Description	<i>require</i>	Require.	<i>deny</i>	Deny.			
Option	Description									
<i>require</i>	Require.									
<i>deny</i>	Deny.									

Parameter	Description	Type	Size	Default								
type	Type.	option	-	file								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>file</i></td> <td>File.</td> </tr> <tr> <td><i>registry</i></td> <td>Registry.</td> </tr> <tr> <td><i>process</i></td> <td>Process.</td> </tr> </tbody> </table>	Option	Description	<i>file</i>	File.	<i>registry</i>	Registry.	<i>process</i>	Process.			
Option	Description											
<i>file</i>	File.											
<i>registry</i>	Registry.											
<i>process</i>	Process.											
target	Target.	string	Maximum length: 255									
version	Version.	string	Maximum length: 35									
md5s <id>	MD5 checksum. Hex string of MD5 checksum.	string	Maximum length: 32									

## config vpn ssl web portal

### Portal.

```

config vpn ssl web portal
  Description: Portal.
  edit <name>
    set tunnel-mode [enable|disable]
    set ip-mode [range|user-group]
    set auto-connect [enable|disable]
    set keep-alive [enable|disable]
    set save-password [enable|disable]
    set ip-pools <name1>, <name2>, ...
    set exclusive-routing [enable|disable]
    set service-restriction [enable|disable]
    set split-tunneling [enable|disable]
    set split-tunneling-routing-negate [enable|disable]
    set split-tunneling-routing-address <name1>, <name2>, ...
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-suffix {var-string}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
    set ipv6-tunnel-mode [enable|disable]
    set ipv6-pools <name1>, <name2>, ...
    set ipv6-exclusive-routing [enable|disable]
    set ipv6-service-restriction [enable|disable]
    set ipv6-split-tunneling [enable|disable]
    set ipv6-split-tunneling-routing-negate [enable|disable]
    set ipv6-split-tunneling-routing-address <name1>, <name2>, ...
    set ipv6-dns-server1 {ipv6-address}
    set ipv6-dns-server2 {ipv6-address}
    set ipv6-wins-server1 {ipv6-address}
    set ipv6-wins-server2 {ipv6-address}
    set web-mode [enable|disable]
  
```

```

set display-bookmark [enable|disable]
set user-bookmark [enable|disable]
set allow-user-access {option1}, {option2}, ...
set user-group-bookmark [enable|disable]
config bookmark-group
  Description: Portal bookmark group.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set apptype [ftp|rdp|...]
        set url {var-string}
        set host {var-string}
        set folder {var-string}
        set domain {var-string}
        set additional-params {var-string}
        set description {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set security [rdp|nla|...]
        set send-preconnection-id [enable|disable]
        set preconnection-id {integer}
        set preconnection-blob {var-string}
        set load-balancing-info {var-string}
        set restricted-admin [enable|disable]
        set port {integer}
        set logon-user {var-string}
        set logon-password {password}
        set color-depth [32|16|...]
        set sso [disable|static|...]
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
        set sso-credential [sslvpn-login|alternative]
        set sso-username {var-string}
        set sso-password {password}
        set sso-credential-sent-once [enable|disable]
      next
    end
  next
end
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set heading {string}
set redir-url {var-string}
set theme [blue|green|...]
set custom-lang {string}
set smb-ntlmv1-auth [enable|disable]
set smbv1 [enable|disable]
set smb-min-version [smbv1|smbv2|...]
set smb-max-version [smbv1|smbv2|...]
set use-sdwan [enable|disable]
set clipboard [enable|disable]
set host-check [none|av|...]

```

```

set host-check-interval {integer}
set host-check-policy <name1>, <name2>, ...
set limit-user-logins [enable|disable]
set mac-addr-check [enable|disable]
set mac-addr-action [allow|deny]
config mac-addr-check-rule
  Description: Client MAC address check rule.
  edit <name>
    set mac-addr-mask {integer}
    set mac-addr-list <addr1>, <addr2>, ...
  next
end
set os-check [enable|disable]
config os-check-list
  Description: SSL-VPN OS checks.
  edit <name>
    set action [deny|allow|...]
    set tolerance {integer}
    set latest-patch-level {user}
  next
end
set forticlient-download [enable|disable]
set forticlient-download-method [direct|ssl-vpn]
set customize-forticlient-download-url [enable|disable]
set windows-forticlient-download-url {var-string}
set macos-forticlient-download-url {var-string}
set skip-check-for-unsupported-os [enable|disable]
set skip-check-for-browser [enable|disable]
set hide-sso-credential [enable|disable]
config split-dns
  Description: Split DNS for SSL-VPN.
  edit <id>
    set domains {var-string}
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set ipv6-dns-server1 {ipv6-address}
    set ipv6-dns-server2 {ipv6-address}
  next
end
next
end

```

## config vpn ssl web portal

Parameter	Description	Type	Size	Default						
tunnel-mode	Enable/disable IPv4 SSL-VPN tunnel mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
ip-mode	Method by which users of this SSL-VPN tunnel obtain IP addresses.	option	-	range						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>range</i></td> <td>Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.</td> </tr> <tr> <td><i>user-group</i></td> <td>Use IP the addresses associated with individual users or user groups (usually from external auth servers).</td> </tr> </tbody> </table>	Option	Description	<i>range</i>	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.	<i>user-group</i>	Use IP the addresses associated with individual users or user groups (usually from external auth servers).			
Option	Description									
<i>range</i>	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.									
<i>user-group</i>	Use IP the addresses associated with individual users or user groups (usually from external auth servers).									
auto-connect	Enable/disable automatic connect by client when system is up.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
keep-alive	Enable/disable automatic reconnect for FortiClient connections.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
save-password	Enable/disable FortiClient saving the user's password.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ip-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string	Maximum length: 79							
exclusive-routing	Enable/disable all traffic go through tunnel only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
service-restriction	Enable/disable tunnel service restriction.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
split-tunneling	Enable/disable IPv4 split tunneling.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
split-tunneling-routing-negate	Enable to negate split tunneling routing address.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
split-tunneling-routing-address <name>	IPv4 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79							
dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0						
dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0						
dns-suffix	DNS suffix.	var-string	Maximum length: 253							
wins-server1	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0						
wins-server2	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0						
ipv6-tunnel-mode	Enable/disable IPv6 SSL-VPN tunnel mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-pools <name>	IPv6 firewall source address objects reserved for SSL-VPN tunnel mode clients.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
	Address name.									
ipv6-exclusive-routing	Enable/disable all IPv6 traffic go through tunnel only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-service-restriction	Enable/disable IPv6 tunnel service restriction.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-split-tunneling	Enable/disable IPv6 split tunneling.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-split-tunneling-routing-negate	Enable to negate IPv6 split tunneling routing address.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-split-tunneling-routing-address <name>	IPv6 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79							
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::						

Parameter	Description	Type	Size	Default																				
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::																				
web-mode	Enable/disable SSL-VPN web mode.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
allow-user-access	Allow user access to SSL-VPN applications.	option	-	web ftp smb sftp telnet ssh vnc rdp ping																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>web</i></td> <td>HTTP/HTTPS access.</td> </tr> <tr> <td><i>ftp</i></td> <td>FTP access.</td> </tr> <tr> <td><i>smb</i></td> <td>SMB/CIFS access.</td> </tr> <tr> <td><i>sftp</i></td> <td>SFTP access.</td> </tr> <tr> <td><i>telnet</i></td> <td>TELNET access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>vnc</i></td> <td>VNC access.</td> </tr> <tr> <td><i>rdp</i></td> <td>RDP access.</td> </tr> <tr> <td><i>ping</i></td> <td>PING access.</td> </tr> </tbody> </table>	Option	Description	<i>web</i>	HTTP/HTTPS access.	<i>ftp</i>	FTP access.	<i>smb</i>	SMB/CIFS access.	<i>sftp</i>	SFTP access.	<i>telnet</i>	TELNET access.	<i>ssh</i>	SSH access.	<i>vnc</i>	VNC access.	<i>rdp</i>	RDP access.	<i>ping</i>	PING access.			
Option	Description																							
<i>web</i>	HTTP/HTTPS access.																							
<i>ftp</i>	FTP access.																							
<i>smb</i>	SMB/CIFS access.																							
<i>sftp</i>	SFTP access.																							
<i>telnet</i>	TELNET access.																							
<i>ssh</i>	SSH access.																							
<i>vnc</i>	VNC access.																							
<i>rdp</i>	RDP access.																							
<i>ping</i>	PING access.																							

Parameter	Description	Type	Size	Default												
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
display-connection-tools	Enable to display the web portal connection tools widget.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
display-history	Enable to display the web portal user login history widget.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
display-status	Enable to display the web portal status widget.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
heading	Web portal heading message.	string	Maximum length: 31	SSL-VPN Portal												
redir-url	Client login redirect URL.	var-string	Maximum length: 255													
theme	Web portal color scheme.	option	-	blue												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>blue</i></td> <td>Light blue theme.</td> </tr> <tr> <td><i>green</i></td> <td>Green theme.</td> </tr> <tr> <td><i>neutrino</i></td> <td>Neutrino theme.</td> </tr> <tr> <td><i>melongene</i></td> <td>Melongene theme (eggplant color).</td> </tr> <tr> <td><i>mariner</i></td> <td>Mariner theme (dark blue color).</td> </tr> </tbody> </table>	Option	Description	<i>blue</i>	Light blue theme.	<i>green</i>	Green theme.	<i>neutrino</i>	Neutrino theme.	<i>melongene</i>	Melongene theme (eggplant color).	<i>mariner</i>	Mariner theme (dark blue color).			
Option	Description															
<i>blue</i>	Light blue theme.															
<i>green</i>	Green theme.															
<i>neutrino</i>	Neutrino theme.															
<i>melongene</i>	Melongene theme (eggplant color).															
<i>mariner</i>	Mariner theme (dark blue color).															

Parameter	Description	Type	Size	Default								
custom-lang	Change the web portal display language. Overrides config system global set language. You can use config system custom-language and execute system custom-language to add custom language files.	string	Maximum length: 35									
smb-ntlmv1-auth	Enable support of NTLMv1 for Samba authentication.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
smbv1	smbv1	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>enable</td> </tr> <tr> <td><i>disable</i></td> <td>disable</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	enable	<i>disable</i>	disable					
Option	Description											
<i>enable</i>	enable											
<i>disable</i>	disable											
smb-min-version	SMB minimum client protocol version.	option	-	smbv2								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>smbv1</i></td> <td>SMB version 1.</td> </tr> <tr> <td><i>smbv2</i></td> <td>SMB version 2.</td> </tr> <tr> <td><i>smbv3</i></td> <td>SMB version 3.</td> </tr> </tbody> </table>	Option	Description	<i>smbv1</i>	SMB version 1.	<i>smbv2</i>	SMB version 2.	<i>smbv3</i>	SMB version 3.			
Option	Description											
<i>smbv1</i>	SMB version 1.											
<i>smbv2</i>	SMB version 2.											
<i>smbv3</i>	SMB version 3.											
smb-max-version	SMB maximum client protocol version.	option	-	smbv3								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>smbv1</i></td> <td>SMB version 1.</td> </tr> <tr> <td><i>smbv2</i></td> <td>SMB version 2.</td> </tr> <tr> <td><i>smbv3</i></td> <td>SMB version 3.</td> </tr> </tbody> </table>	Option	Description	<i>smbv1</i>	SMB version 1.	<i>smbv2</i>	SMB version 2.	<i>smbv3</i>	SMB version 3.			
Option	Description											
<i>smbv1</i>	SMB version 1.											
<i>smbv2</i>	SMB version 2.											
<i>smbv3</i>	SMB version 3.											
use-sdwan	Use SD-WAN rules to get output interface.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
clipboard	Enable to support RDP/VPC clipboard functionality.	option	-	enable								

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support of RDP/VNC clipboard.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support of RDP/VNC clipboard.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support of RDP/VNC clipboard.	<i>disable</i>	Disable support of RDP/VNC clipboard.									
Option	Description															
<i>enable</i>	Enable support of RDP/VNC clipboard.															
<i>disable</i>	Disable support of RDP/VNC clipboard.															
host-check	Type of host checking performed on endpoints.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No host checking.</td> </tr> <tr> <td><i>av</i></td> <td>AntiVirus software recognized by the Windows Security Center.</td> </tr> <tr> <td><i>fw</i></td> <td>Firewall software recognized by the Windows Security Center.</td> </tr> <tr> <td><i>av-fw</i></td> <td>AntiVirus and firewall software recognized by the Windows Security Center.</td> </tr> <tr> <td><i>custom</i></td> <td>Custom.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No host checking.	<i>av</i>	AntiVirus software recognized by the Windows Security Center.	<i>fw</i>	Firewall software recognized by the Windows Security Center.	<i>av-fw</i>	AntiVirus and firewall software recognized by the Windows Security Center.	<i>custom</i>	Custom.			
Option	Description															
<i>none</i>	No host checking.															
<i>av</i>	AntiVirus software recognized by the Windows Security Center.															
<i>fw</i>	Firewall software recognized by the Windows Security Center.															
<i>av-fw</i>	AntiVirus and firewall software recognized by the Windows Security Center.															
<i>custom</i>	Custom.															
host-check-interval	Periodic host check interval. Value of 0 means disabled and host checking only happens when the endpoint connects.	integer	Minimum value: 120 Maximum value: 259200	0												
host-check-policy <name>	One or more policies to require the endpoint to have specific security software. Host check software list name.	string	Maximum length: 79													
limit-user-logins	Enable to limit each user to one SSL-VPN session at a time.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
mac-addr-check	Enable/disable MAC address host checking.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
mac-addr-action	Client MAC address action.	option	-	allow												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow connection when client MAC address is matched.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny connection when client MAC address is matched.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow connection when client MAC address is matched.	<i>deny</i>	Deny connection when client MAC address is matched.			
Option	Description									
<i>allow</i>	Allow connection when client MAC address is matched.									
<i>deny</i>	Deny connection when client MAC address is matched.									
os-check	Enable to let the FortiGate decide action based on client OS.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
forticlient-download	Enable/disable download option for FortiClient.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
forticlient-download-method	FortiClient download method.	option	-	direct						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>direct</i></td> <td>Download via direct link.</td> </tr> <tr> <td><i>ssl-vpn</i></td> <td>Download via SSL-VPN.</td> </tr> </tbody> </table>	Option	Description	<i>direct</i>	Download via direct link.	<i>ssl-vpn</i>	Download via SSL-VPN.			
Option	Description									
<i>direct</i>	Download via direct link.									
<i>ssl-vpn</i>	Download via SSL-VPN.									
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023							
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023							

Parameter	Description	Type	Size	Default						
skip-check-for-unsupported-os	Enable to skip host check if client OS does not support it.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
skip-check-for-browser	Enable to skip host check for browser support.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
hide-sso-credential	Enable to prevent SSO credential being sent to client.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

### config bookmarks

Parameter	Description	Type	Size	Default																		
apptype	Application type.	option	-	web																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>rdp</i></td> <td>RDP.</td> </tr> <tr> <td><i>sftp</i></td> <td>SFTP.</td> </tr> <tr> <td><i>smb</i></td> <td>SMB/CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> <tr> <td><i>telnet</i></td> <td>Telnet.</td> </tr> <tr> <td><i>vnc</i></td> <td>VNC.</td> </tr> <tr> <td><i>web</i></td> <td>HTTP/HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP.	<i>rdp</i>	RDP.	<i>sftp</i>	SFTP.	<i>smb</i>	SMB/CIFS.	<i>ssh</i>	SSH.	<i>telnet</i>	Telnet.	<i>vnc</i>	VNC.	<i>web</i>	HTTP/HTTPS.			
Option	Description																					
<i>ftp</i>	FTP.																					
<i>rdp</i>	RDP.																					
<i>sftp</i>	SFTP.																					
<i>smb</i>	SMB/CIFS.																					
<i>ssh</i>	SSH.																					
<i>telnet</i>	Telnet.																					
<i>vnc</i>	VNC.																					
<i>web</i>	HTTP/HTTPS.																					
url	URL parameter.	var-string	Maximum length: 128																			



Parameter	Description	Type	Size	Default
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us

Option	Description
<i>ar-101</i>	Arabic (101).
<i>ar-102</i>	Arabic (102).
<i>ar-102-azerty</i>	Arabic (102) AZERTY.
<i>can-mul</i>	Canadian Multilingual Standard.
<i>cz</i>	Czech.
<i>cz-qwerty</i>	Czech (QWERTY).
<i>cz-pr</i>	Czech Programmers.
<i>da</i>	Danish.
<i>nl</i>	Dutch.
<i>de</i>	German.
<i>de-ch</i>	German, Switzerland.
<i>de-ibm</i>	German (IBM).
<i>en-uk</i>	English, United Kingdom.
<i>en-uk-ext</i>	English, United Kingdom Extended.
<i>en-us</i>	English, United States.
<i>en-us-dvorak</i>	English, United States-Dvorak.
<i>es</i>	Spanish.
<i>es-var</i>	Spanish Variation.
<i>fi</i>	Finish.

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgian.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ko</i>	Korean.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lav-std</i>	Latvian (Standard).		
	<i>lav-leg</i>	Latvian (Legacy).		
	<i>mk</i>	Macedonian (FYROM).		
	<i>mk-std</i>	Macedonia (FYROM) - Standard.		
	<i>no</i>	Norwegian.		
	<i>no-sami</i>	Norwegian with Sami.		
	<i>pol-214</i>	Polish (214).		
	<i>pol-pr</i>	Polish (Programmers).		
	<i>pt</i>	Portuguese.		
	<i>pt-br</i>	Portuguese (Brazilian ABNT).		
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).		
	<i>ru</i>	Russian.		
	<i>ru-mne</i>	Russian - Mnemonic.		
	<i>ru-t</i>	Russian (Typewriter).		

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sl</i></td> <td>Slovenian.</td> </tr> <tr> <td><i>sv</i></td> <td>Swedish.</td> </tr> <tr> <td><i>sv-sami</i></td> <td>Swedish with Sami.</td> </tr> <tr> <td><i>tuk</i></td> <td>Turkmen.</td> </tr> <tr> <td><i>tur-f</i></td> <td>Turkish F.</td> </tr> <tr> <td><i>tur-q</i></td> <td>Turkish Q.</td> </tr> <tr> <td><i>zh-sym-sg-us</i></td> <td>Chinese (Simplified, Singapore) - US keyboard.</td> </tr> <tr> <td><i>zh-sym-us</i></td> <td>Chinese (Simplified) - US Keyboard.</td> </tr> <tr> <td><i>zh-tr-hk</i></td> <td>Chinese (Traditional, Hong Kong S.A.R.).</td> </tr> <tr> <td><i>zh-tr-mo</i></td> <td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td> </tr> <tr> <td><i>zh-tr-us</i></td> <td>Chinese (Traditional) - US keyboard.</td> </tr> </tbody> </table>	Option	Description	<i>sl</i>	Slovenian.	<i>sv</i>	Swedish.	<i>sv-sami</i>	Swedish with Sami.	<i>tuk</i>	Turkmen.	<i>tur-f</i>	Turkish F.	<i>tur-q</i>	Turkish Q.	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
Option	Description																											
<i>sl</i>	Slovenian.																											
<i>sv</i>	Swedish.																											
<i>sv-sami</i>	Swedish with Sami.																											
<i>tuk</i>	Turkmen.																											
<i>tur-f</i>	Turkish F.																											
<i>tur-q</i>	Turkish Q.																											
<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.																											
<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.																											
<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).																											
<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.																											
<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.																											
security	Security mode for RDP connection.	option	-	any																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rdp</i></td> <td>Standard RDP encryption.</td> </tr> <tr> <td><i>nla</i></td> <td>Network Level Authentication.</td> </tr> <tr> <td><i>tls</i></td> <td>TLS encryption.</td> </tr> <tr> <td><i>any</i></td> <td>Allow the server to choose the type of security.</td> </tr> </tbody> </table>	Option	Description	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.	<i>any</i>	Allow the server to choose the type of security.																	
Option	Description																											
<i>rdp</i>	Standard RDP encryption.																											
<i>nla</i>	Network Level Authentication.																											
<i>tls</i>	TLS encryption.																											
<i>any</i>	Allow the server to choose the type of security.																											
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of preconnection ID.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of preconnection ID.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.																					
Option	Description																											
<i>enable</i>	Enable sending of preconnection ID.																											
<i>disable</i>	Disable sending of preconnection ID.																											
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0																								
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511																									

Parameter	Description	Type	Size	Default								
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511									
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable restricted admin mode for RDP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable restricted admin mode for RDP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.					
Option	Description											
<i>enable</i>	Enable restricted admin mode for RDP.											
<i>disable</i>	Disable restricted admin mode for RDP.											
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0								
logon-user	Logon user.	var-string	Maximum length: 35									
logon-password	Logon password.	password	Not Specified									
color-depth	Color depth per pixel.	option	-	16								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>32</td> <td>32bits per pixel.</td> </tr> <tr> <td>16</td> <td>16bits per pixel.</td> </tr> <tr> <td>8</td> <td>8bits per pixel.</td> </tr> </tbody> </table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.			
Option	Description											
32	32bits per pixel.											
16	16bits per pixel.											
8	8bits per pixel.											
sso	Single Sign-On.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SSO.</td> </tr> <tr> <td><i>static</i></td> <td>Static SSO.</td> </tr> <tr> <td><i>auto</i></td> <td>Auto SSO.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.			
Option	Description											
<i>disable</i>	Disable SSO.											
<i>static</i>	Static SSO.											
<i>auto</i>	Auto SSO.											
sso-credential	Single sign-on credentials.	option	-	sslvpn-login								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sslvpn-login</i></td> <td>SSL-VPN login.</td> </tr> <tr> <td><i>alternative</i></td> <td>Alternative.</td> </tr> </tbody> </table>	Option	Description	<i>sslvpn-login</i>	SSL-VPN login.	<i>alternative</i>	Alternative.					
Option	Description											
<i>sslvpn-login</i>	SSL-VPN login.											
<i>alternative</i>	Alternative.											
sso-username	SSO user name.	var-string	Maximum length: 35									
sso-password	SSO password.	password	Not Specified									

Parameter	Description	Type	Size	Default						
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Single sign-on credentials are only sent once to remote server.</td> </tr> <tr> <td><i>disable</i></td> <td>Single sign-on credentials are sent to remote server for every HTTP request.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.			
Option	Description									
<i>enable</i>	Single sign-on credentials are only sent once to remote server.									
<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.									

### config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

### config mac-addr-check-rule

Parameter	Description	Type	Size	Default
mac-addr-mask	Client MAC address mask.	integer	Minimum value: 1 Maximum value: 48	48
mac-addr-list <addr>	Client MAC address list. Client MAC address.	mac-address	Not Specified	

### config os-check-list

Parameter	Description	Type	Size	Default								
action	OS check options.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>deny</i></td> <td>Deny all OS versions.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow any OS version.</td> </tr> <tr> <td><i>check-up-to-date</i></td> <td>Verify OS is up-to-date.</td> </tr> </tbody> </table>	Option	Description	<i>deny</i>	Deny all OS versions.	<i>allow</i>	Allow any OS version.	<i>check-up-to-date</i>	Verify OS is up-to-date.			
Option	Description											
<i>deny</i>	Deny all OS versions.											
<i>allow</i>	Allow any OS version.											
<i>check-up-to-date</i>	Verify OS is up-to-date.											
tolerance	OS patch level tolerance.	integer	Minimum value: 0 Maximum value: 65535	0								
latest-patch-level	Latest OS patch level.	user	Not Specified	0								

## config split-dns

Parameter	Description	Type	Size	Default
domains	Split DNS domains used for SSL-VPN clients separated by comma(,).	var-string	Maximum length: 1024	
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::

## config vpn ssl web user-group-bookmark

Configure SSL-VPN user group bookmark.

```
config vpn ssl web user-group-bookmark
  Description: Configure SSL-VPN user group bookmark.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set apptype [ftp|rdp|...]
        set url {var-string}
        set host {var-string}
        set folder {var-string}
        set domain {var-string}
        set additional-params {var-string}
        set description {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set security [rdp|nla|...]
        set send-preconnection-id [enable|disable]
        set preconnection-id {integer}
        set preconnection-blob {var-string}
        set load-balancing-info {var-string}
        set restricted-admin [enable|disable]
        set port {integer}
        set logon-user {var-string}
        set logon-password {password}
        set color-depth [32|16|...]
        set sso [disable|static|...]
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
        set sso-credential [sslvpn-login|alternative]
        set sso-username {var-string}
```

```

        set sso-password {password}
        set sso-credential-sent-once [enable|disable]
    next
end
next
end

```

## config bookmarks

Parameter	Description	Type	Size	Default																		
apptype	Application type.	option	-	web																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>rdp</i></td> <td>RDP.</td> </tr> <tr> <td><i>sftp</i></td> <td>SFTP.</td> </tr> <tr> <td><i>smb</i></td> <td>SMB/CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> <tr> <td><i>telnet</i></td> <td>Telnet.</td> </tr> <tr> <td><i>vnc</i></td> <td>VNC.</td> </tr> <tr> <td><i>web</i></td> <td>HTTP/HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP.	<i>rdp</i>	RDP.	<i>sftp</i>	SFTP.	<i>smb</i>	SMB/CIFS.	<i>ssh</i>	SSH.	<i>telnet</i>	Telnet.	<i>vnc</i>	VNC.	<i>web</i>	HTTP/HTTPS.			
Option	Description																					
<i>ftp</i>	FTP.																					
<i>rdp</i>	RDP.																					
<i>sftp</i>	SFTP.																					
<i>smb</i>	SMB/CIFS.																					
<i>ssh</i>	SSH.																					
<i>telnet</i>	Telnet.																					
<i>vnc</i>	VNC.																					
<i>web</i>	HTTP/HTTPS.																					
url	URL parameter.	var-string	Maximum length: 128																			
host	Host name/IP parameter.	var-string	Maximum length: 128																			
folder	Network shared file folder parameter.	var-string	Maximum length: 128																			
domain	Login domain.	var-string	Maximum length: 128																			
additional-params	Additional parameters.	var-string	Maximum length: 128																			
description	Description.	var-string	Maximum length: 128																			
keyboard-layout	Keyboard layout.	option	-	en-us																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ar-101</i></td> <td>Arabic (101).</td> </tr> <tr> <td><i>ar-102</i></td> <td>Arabic (102).</td> </tr> </tbody> </table>	Option	Description	<i>ar-101</i>	Arabic (101).	<i>ar-102</i>	Arabic (102).															
Option	Description																					
<i>ar-101</i>	Arabic (101).																					
<i>ar-102</i>	Arabic (102).																					

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ar-102-azerty</i>	Arabic (102) AZERTY.		
	<i>can-mul</i>	Canadian Multilingual Standard.		
	<i>cz</i>	Czech.		
	<i>cz-qwerty</i>	Czech (QWERTY).		
	<i>cz-pr</i>	Czech Programmers.		
	<i>da</i>	Danish.		
	<i>nl</i>	Dutch.		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgian.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ko</i>	Korean.		



Parameter	Description	Type	Size	Default																																																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>lt</i></td> <td>Lithuanian.</td> </tr> <tr> <td><i>lt-ibm</i></td> <td>Lithuanian IBM.</td> </tr> <tr> <td><i>lt-std</i></td> <td>Lithuanian Standard.</td> </tr> <tr> <td><i>lav-std</i></td> <td>Latvian (Standard).</td> </tr> <tr> <td><i>lav-leg</i></td> <td>Latvian (Legacy).</td> </tr> <tr> <td><i>mk</i></td> <td>Macedonian (FYROM).</td> </tr> <tr> <td><i>mk-std</i></td> <td>Macedonia (FYROM) - Standard.</td> </tr> <tr> <td><i>no</i></td> <td>Norwegian.</td> </tr> <tr> <td><i>no-sami</i></td> <td>Norwegian with Sami.</td> </tr> <tr> <td><i>pol-214</i></td> <td>Polish (214).</td> </tr> <tr> <td><i>pol-pr</i></td> <td>Polish (Programmers).</td> </tr> <tr> <td><i>pt</i></td> <td>Portuguese.</td> </tr> <tr> <td><i>pt-br</i></td> <td>Portuguese (Brazilian ABNT).</td> </tr> <tr> <td><i>pt-br-abnt2</i></td> <td>Portuguese (Brazilian ABNT2).</td> </tr> <tr> <td><i>ru</i></td> <td>Russian.</td> </tr> <tr> <td><i>ru-mne</i></td> <td>Russian - Mnemonic.</td> </tr> <tr> <td><i>ru-t</i></td> <td>Russian (Typewriter).</td> </tr> <tr> <td><i>sl</i></td> <td>Slovenian.</td> </tr> <tr> <td><i>sv</i></td> <td>Swedish.</td> </tr> <tr> <td><i>sv-sami</i></td> <td>Swedish with Sami.</td> </tr> <tr> <td><i>tuk</i></td> <td>Turkmen.</td> </tr> <tr> <td><i>tur-f</i></td> <td>Turkish F.</td> </tr> <tr> <td><i>tur-q</i></td> <td>Turkish Q.</td> </tr> <tr> <td><i>zh-sym-sg-us</i></td> <td>Chinese (Simplified, Singapore) - US keyboard.</td> </tr> <tr> <td><i>zh-sym-us</i></td> <td>Chinese (Simplified) - US Keyboard.</td> </tr> <tr> <td><i>zh-tr-hk</i></td> <td>Chinese (Traditional, Hong Kong S.A.R.).</td> </tr> <tr> <td><i>zh-tr-mo</i></td> <td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td> </tr> <tr> <td><i>zh-tr-us</i></td> <td>Chinese (Traditional) - US keyboard.</td> </tr> </tbody> </table>	Option	Description	<i>lt</i>	Lithuanian.	<i>lt-ibm</i>	Lithuanian IBM.	<i>lt-std</i>	Lithuanian Standard.	<i>lav-std</i>	Latvian (Standard).	<i>lav-leg</i>	Latvian (Legacy).	<i>mk</i>	Macedonian (FYROM).	<i>mk-std</i>	Macedonia (FYROM) - Standard.	<i>no</i>	Norwegian.	<i>no-sami</i>	Norwegian with Sami.	<i>pol-214</i>	Polish (214).	<i>pol-pr</i>	Polish (Programmers).	<i>pt</i>	Portuguese.	<i>pt-br</i>	Portuguese (Brazilian ABNT).	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>ru</i>	Russian.	<i>ru-mne</i>	Russian - Mnemonic.	<i>ru-t</i>	Russian (Typewriter).	<i>sl</i>	Slovenian.	<i>sv</i>	Swedish.	<i>sv-sami</i>	Swedish with Sami.	<i>tuk</i>	Turkmen.	<i>tur-f</i>	Turkish F.	<i>tur-q</i>	Turkish Q.	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
Option	Description																																																													
<i>lt</i>	Lithuanian.																																																													
<i>lt-ibm</i>	Lithuanian IBM.																																																													
<i>lt-std</i>	Lithuanian Standard.																																																													
<i>lav-std</i>	Latvian (Standard).																																																													
<i>lav-leg</i>	Latvian (Legacy).																																																													
<i>mk</i>	Macedonian (FYROM).																																																													
<i>mk-std</i>	Macedonia (FYROM) - Standard.																																																													
<i>no</i>	Norwegian.																																																													
<i>no-sami</i>	Norwegian with Sami.																																																													
<i>pol-214</i>	Polish (214).																																																													
<i>pol-pr</i>	Polish (Programmers).																																																													
<i>pt</i>	Portuguese.																																																													
<i>pt-br</i>	Portuguese (Brazilian ABNT).																																																													
<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																																																													
<i>ru</i>	Russian.																																																													
<i>ru-mne</i>	Russian - Mnemonic.																																																													
<i>ru-t</i>	Russian (Typewriter).																																																													
<i>sl</i>	Slovenian.																																																													
<i>sv</i>	Swedish.																																																													
<i>sv-sami</i>	Swedish with Sami.																																																													
<i>tuk</i>	Turkmen.																																																													
<i>tur-f</i>	Turkish F.																																																													
<i>tur-q</i>	Turkish Q.																																																													
<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.																																																													
<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.																																																													
<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).																																																													
<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.																																																													
<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.																																																													
<i>security</i>	Security mode for RDP connection.	option	-	any																																																										

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rdp</i></td> <td>Standard RDP encryption.</td> </tr> <tr> <td><i>nla</i></td> <td>Network Level Authentication.</td> </tr> <tr> <td><i>tls</i></td> <td>TLS encryption.</td> </tr> <tr> <td><i>any</i></td> <td>Allow the server to choose the type of security.</td> </tr> </tbody> </table>	Option	Description	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.	<i>any</i>	Allow the server to choose the type of security.			
Option	Description													
<i>rdp</i>	Standard RDP encryption.													
<i>nla</i>	Network Level Authentication.													
<i>tls</i>	TLS encryption.													
<i>any</i>	Allow the server to choose the type of security.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of preconnection ID.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of preconnection ID.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.							
Option	Description													
<i>enable</i>	Enable sending of preconnection ID.													
<i>disable</i>	Disable sending of preconnection ID.													
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0										
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511											
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable restricted admin mode for RDP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable restricted admin mode for RDP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.							
Option	Description													
<i>enable</i>	Enable restricted admin mode for RDP.													
<i>disable</i>	Disable restricted admin mode for RDP.													
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0										
logon-user	Logon user.	var-string	Maximum length: 35											
logon-password	Logon password.	password	Not Specified											
color-depth	Color depth per pixel.	option	-	16										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>32</td> <td>32bits per pixel.</td> </tr> <tr> <td>16</td> <td>16bits per pixel.</td> </tr> <tr> <td>8</td> <td>8bits per pixel.</td> </tr> </tbody> </table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.			
Option	Description											
32	32bits per pixel.											
16	16bits per pixel.											
8	8bits per pixel.											
sso	Single Sign-On.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SSO.</td> </tr> <tr> <td><i>static</i></td> <td>Static SSO.</td> </tr> <tr> <td><i>auto</i></td> <td>Auto SSO.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.			
Option	Description											
<i>disable</i>	Disable SSO.											
<i>static</i>	Static SSO.											
<i>auto</i>	Auto SSO.											
sso-credential	Single sign-on credentials.	option	-	sslvpn-login								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sslvpn-login</i></td> <td>SSL-VPN login.</td> </tr> <tr> <td><i>alternative</i></td> <td>Alternative.</td> </tr> </tbody> </table>	Option	Description	<i>sslvpn-login</i>	SSL-VPN login.	<i>alternative</i>	Alternative.					
Option	Description											
<i>sslvpn-login</i>	SSL-VPN login.											
<i>alternative</i>	Alternative.											
sso-username	SSO user name.	var-string	Maximum length: 35									
sso-password	SSO password.	password	Not Specified									
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Single sign-on credentials are only sent once to remote server.</td> </tr> <tr> <td><i>disable</i></td> <td>Single sign-on credentials are sent to remote server for every HTTP request.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.					
Option	Description											
<i>enable</i>	Single sign-on credentials are only sent once to remote server.											
<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.											

#### config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

## config vpn ssl web user-bookmark

Configure SSL-VPN user bookmark.

```

config vpn ssl web user-bookmark
  Description: Configure SSL-VPN user bookmark.
  edit <name>
    set custom-lang {string}
  config bookmarks
    Description: Bookmark table.
    edit <name>
      set apptype [ftp|rdp|...]
      set url {var-string}
      set host {var-string}
      set folder {var-string}
      set domain {var-string}
      set additional-params {var-string}
      set description {var-string}
      set keyboard-layout [ar-101|ar-102|...]
      set security [rdp|nla|...]
      set send-preconnection-id [enable|disable]
      set preconnection-id {integer}
      set preconnection-blob {var-string}
      set load-balancing-info {var-string}
      set restricted-admin [enable|disable]
      set port {integer}
      set logon-user {var-string}
      set logon-password {password}
      set color-depth [32|16|...]
      set sso [disable|static|...]
    config form-data
      Description: Form data.
      edit <name>
        set value {var-string}
      next
    end
    set sso-credential [sslvpn-login|alternative]
    set sso-username {var-string}
    set sso-password {password}
    set sso-credential-sent-once [enable|disable]
  next
end
next
end

```

## config vpn ssl web user-bookmark

Parameter	Description	Type	Size	Default
custom-lang	Personal language.	string	Maximum length: 35	

## config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftp</i></td> <td>FTP.</td> </tr> <tr> <td><i>rdp</i></td> <td>RDP.</td> </tr> <tr> <td><i>sftp</i></td> <td>SFTP.</td> </tr> <tr> <td><i>smb</i></td> <td>SMB/CIFS.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH.</td> </tr> <tr> <td><i>telnet</i></td> <td>Telnet.</td> </tr> <tr> <td><i>vnc</i></td> <td>VNC.</td> </tr> <tr> <td><i>web</i></td> <td>HTTP/HTTPS.</td> </tr> </tbody> </table>	Option	Description	<i>ftp</i>	FTP.	<i>rdp</i>	RDP.	<i>sftp</i>	SFTP.	<i>smb</i>	SMB/CIFS.	<i>ssh</i>	SSH.	<i>telnet</i>	Telnet.	<i>vnc</i>	VNC.	<i>web</i>	HTTP/HTTPS.			
Option	Description																					
<i>ftp</i>	FTP.																					
<i>rdp</i>	RDP.																					
<i>sftp</i>	SFTP.																					
<i>smb</i>	SMB/CIFS.																					
<i>ssh</i>	SSH.																					
<i>telnet</i>	Telnet.																					
<i>vnc</i>	VNC.																					
<i>web</i>	HTTP/HTTPS.																					
url	URL parameter.	var-string	Maximum length: 128																			
host	Host name/IP parameter.	var-string	Maximum length: 128																			
folder	Network shared file folder parameter.	var-string	Maximum length: 128																			
domain	Login domain.	var-string	Maximum length: 128																			
additional-params	Additional parameters.	var-string	Maximum length: 128																			
description	Description.	var-string	Maximum length: 128																			
keyboard-layout	Keyboard layout.	option	-	en-us																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ar-101</i></td> <td>Arabic (101).</td> </tr> <tr> <td><i>ar-102</i></td> <td>Arabic (102).</td> </tr> <tr> <td><i>ar-102-azerty</i></td> <td>Arabic (102) AZERTY.</td> </tr> <tr> <td><i>can-mul</i></td> <td>Canadian Multilingual Standard.</td> </tr> <tr> <td><i>cz</i></td> <td>Czech.</td> </tr> <tr> <td><i>cz-qwerty</i></td> <td>Czech (QWERTY).</td> </tr> <tr> <td><i>cz-pr</i></td> <td>Czech Programmers.</td> </tr> <tr> <td><i>da</i></td> <td>Danish.</td> </tr> </tbody> </table>	Option	Description	<i>ar-101</i>	Arabic (101).	<i>ar-102</i>	Arabic (102).	<i>ar-102-azerty</i>	Arabic (102) AZERTY.	<i>can-mul</i>	Canadian Multilingual Standard.	<i>cz</i>	Czech.	<i>cz-qwerty</i>	Czech (QWERTY).	<i>cz-pr</i>	Czech Programmers.	<i>da</i>	Danish.			
Option	Description																					
<i>ar-101</i>	Arabic (101).																					
<i>ar-102</i>	Arabic (102).																					
<i>ar-102-azerty</i>	Arabic (102) AZERTY.																					
<i>can-mul</i>	Canadian Multilingual Standard.																					
<i>cz</i>	Czech.																					
<i>cz-qwerty</i>	Czech (QWERTY).																					
<i>cz-pr</i>	Czech Programmers.																					
<i>da</i>	Danish.																					

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>nl</i>	Dutch.		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgian.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ko</i>	Korean.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lav-std</i>	Latvian (Standard).		
	<i>lav-leg</i>	Latvian (Legacy).		
	<i>mk</i>	Macedonian (FYROM).		

Parameter	Description	Type	Size	Default																																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mk-std</i></td> <td>Macedonia (FYROM) - Standard.</td> </tr> <tr> <td><i>no</i></td> <td>Norwegian.</td> </tr> <tr> <td><i>no-sami</i></td> <td>Norwegian with Sami.</td> </tr> <tr> <td><i>pol-214</i></td> <td>Polish (214).</td> </tr> <tr> <td><i>pol-pr</i></td> <td>Polish (Programmers).</td> </tr> <tr> <td><i>pt</i></td> <td>Portuguese.</td> </tr> <tr> <td><i>pt-br</i></td> <td>Portuguese (Brazilian ABNT).</td> </tr> <tr> <td><i>pt-br-abnt2</i></td> <td>Portuguese (Brazilian ABNT2).</td> </tr> <tr> <td><i>ru</i></td> <td>Russian.</td> </tr> <tr> <td><i>ru-mne</i></td> <td>Russian - Mnemonic.</td> </tr> <tr> <td><i>ru-t</i></td> <td>Russian (Typewriter).</td> </tr> <tr> <td><i>sl</i></td> <td>Slovenian.</td> </tr> <tr> <td><i>sv</i></td> <td>Swedish.</td> </tr> <tr> <td><i>sv-sami</i></td> <td>Swedish with Sami.</td> </tr> <tr> <td><i>tuk</i></td> <td>Turkmen.</td> </tr> <tr> <td><i>tur-f</i></td> <td>Turkish F.</td> </tr> <tr> <td><i>tur-q</i></td> <td>Turkish Q.</td> </tr> <tr> <td><i>zh-sym-sg-us</i></td> <td>Chinese (Simplified, Singapore) - US keyboard.</td> </tr> <tr> <td><i>zh-sym-us</i></td> <td>Chinese (Simplified) - US Keyboard.</td> </tr> <tr> <td><i>zh-tr-hk</i></td> <td>Chinese (Traditional, Hong Kong S.A.R.).</td> </tr> <tr> <td><i>zh-tr-mo</i></td> <td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td> </tr> <tr> <td><i>zh-tr-us</i></td> <td>Chinese (Traditional) - US keyboard.</td> </tr> </tbody> </table>	Option	Description	<i>mk-std</i>	Macedonia (FYROM) - Standard.	<i>no</i>	Norwegian.	<i>no-sami</i>	Norwegian with Sami.	<i>pol-214</i>	Polish (214).	<i>pol-pr</i>	Polish (Programmers).	<i>pt</i>	Portuguese.	<i>pt-br</i>	Portuguese (Brazilian ABNT).	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>ru</i>	Russian.	<i>ru-mne</i>	Russian - Mnemonic.	<i>ru-t</i>	Russian (Typewriter).	<i>sl</i>	Slovenian.	<i>sv</i>	Swedish.	<i>sv-sami</i>	Swedish with Sami.	<i>tuk</i>	Turkmen.	<i>tur-f</i>	Turkish F.	<i>tur-q</i>	Turkish Q.	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
Option	Description																																																	
<i>mk-std</i>	Macedonia (FYROM) - Standard.																																																	
<i>no</i>	Norwegian.																																																	
<i>no-sami</i>	Norwegian with Sami.																																																	
<i>pol-214</i>	Polish (214).																																																	
<i>pol-pr</i>	Polish (Programmers).																																																	
<i>pt</i>	Portuguese.																																																	
<i>pt-br</i>	Portuguese (Brazilian ABNT).																																																	
<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																																																	
<i>ru</i>	Russian.																																																	
<i>ru-mne</i>	Russian - Mnemonic.																																																	
<i>ru-t</i>	Russian (Typewriter).																																																	
<i>sl</i>	Slovenian.																																																	
<i>sv</i>	Swedish.																																																	
<i>sv-sami</i>	Swedish with Sami.																																																	
<i>tuk</i>	Turkmen.																																																	
<i>tur-f</i>	Turkish F.																																																	
<i>tur-q</i>	Turkish Q.																																																	
<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.																																																	
<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.																																																	
<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).																																																	
<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.																																																	
<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.																																																	
security	Security mode for RDP connection.	option	-	any																																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rdp</i></td> <td>Standard RDP encryption.</td> </tr> <tr> <td><i>nla</i></td> <td>Network Level Authentication.</td> </tr> <tr> <td><i>tls</i></td> <td>TLS encryption.</td> </tr> <tr> <td><i>any</i></td> <td>Allow the server to choose the type of security.</td> </tr> </tbody> </table>	Option	Description	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.	<i>any</i>	Allow the server to choose the type of security.																																							
Option	Description																																																	
<i>rdp</i>	Standard RDP encryption.																																																	
<i>nla</i>	Network Level Authentication.																																																	
<i>tls</i>	TLS encryption.																																																	
<i>any</i>	Allow the server to choose the type of security.																																																	

Parameter	Description	Type	Size	Default								
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending of preconnection ID.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending of preconnection ID.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.					
Option	Description											
<i>enable</i>	Enable sending of preconnection ID.											
<i>disable</i>	Disable sending of preconnection ID.											
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0								
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511									
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511									
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable restricted admin mode for RDP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable restricted admin mode for RDP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.					
Option	Description											
<i>enable</i>	Enable restricted admin mode for RDP.											
<i>disable</i>	Disable restricted admin mode for RDP.											
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0								
logon-user	Logon user.	var-string	Maximum length: 35									
logon-password	Logon password.	password	Not Specified									
color-depth	Color depth per pixel.	option	-	16								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>32</td> <td>32bits per pixel.</td> </tr> <tr> <td>16</td> <td>16bits per pixel.</td> </tr> <tr> <td>8</td> <td>8bits per pixel.</td> </tr> </tbody> </table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.			
Option	Description											
32	32bits per pixel.											
16	16bits per pixel.											
8	8bits per pixel.											
sso	Single Sign-On.	option	-	disable								



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable SSO.</td> </tr> <tr> <td><i>static</i></td> <td>Static SSO.</td> </tr> <tr> <td><i>auto</i></td> <td>Auto SSO.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.			
Option	Description											
<i>disable</i>	Disable SSO.											
<i>static</i>	Static SSO.											
<i>auto</i>	Auto SSO.											
sso-credential	Single sign-on credentials.	option	-	sslvpn-login								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sslvpn-login</i></td> <td>SSL-VPN login.</td> </tr> <tr> <td><i>alternative</i></td> <td>Alternative.</td> </tr> </tbody> </table>	Option	Description	<i>sslvpn-login</i>	SSL-VPN login.	<i>alternative</i>	Alternative.					
Option	Description											
<i>sslvpn-login</i>	SSL-VPN login.											
<i>alternative</i>	Alternative.											
sso-username	SSO user name.	var-string	Maximum length: 35									
sso-password	SSO password.	password	Not Specified									
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Single sign-on credentials are only sent once to remote server.</td> </tr> <tr> <td><i>disable</i></td> <td>Single sign-on credentials are sent to remote server for every HTTP request.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.					
Option	Description											
<i>enable</i>	Single sign-on credentials are only sent once to remote server.											
<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.											

### config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

## config vpn ssl settings

Configure SSL-VPN.

```

config vpn ssl settings
  Description: Configure SSL-VPN.
  set status [enable|disable]
  set reqclientcert [enable|disable]
  set user-peer {string}
  set ssl-max-proto-ver [tls1-0|tls1-1|...]
  set ssl-min-proto-ver [tls1-0|tls1-1|...]
  set banned-cipher {option1}, {option2}, ...
  set ciphersuite {option1}, {option2}, ...
  set ssl-insert-empty-fragment [enable|disable]

```

```

set https-redirect [enable|disable]
set x-content-type-options [enable|disable]
set ssl-client-renegotiation [disable|enable]
set force-two-factor-auth [enable|disable]
set unsafe-legacy-renegotiation [enable|disable]
set servercert {string}
set algorithm [high|medium|...]
set idle-timeout {integer}
set auth-timeout {integer}
set login-attempt-limit {integer}
set login-block-time {integer}
set login-timeout {integer}
set dtls-hello-timeout {integer}
set tunnel-ip-pools <name1>, <name2>, ...
set tunnel-ipv6-pools <name1>, <name2>, ...
set dns-suffix {var-string}
set dns-server1 {ipv4-address}
set dns-server2 {ipv4-address}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-wins-server1 {ipv6-address}
set ipv6-wins-server2 {ipv6-address}
set url-obscuration [enable|disable]
set http-compression [enable|disable]
set http-only-cookie [enable|disable]
set deflate-compression-level {integer}
set deflate-min-data-size {integer}
set port {integer}
set port-precedence [enable|disable]
set auto-tunnel-static-route [enable|disable]
set header-x-forwarded-for [pass|add|...]
set source-interface <name1>, <name2>, ...
set source-address <name1>, <name2>, ...
set source-address-negate [enable|disable]
set source-address6 <name1>, <name2>, ...
set source-address6-negate [enable|disable]
set default-portal {string}
config authentication-rule
    Description: Authentication rule for SSL-VPN.
    edit <id>
        set source-interface <name1>, <name2>, ...
        set source-address <name1>, <name2>, ...
        set source-address-negate [enable|disable]
        set source-address6 <name1>, <name2>, ...
        set source-address6-negate [enable|disable]
        set users <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set portal {string}
        set realm {string}
        set client-cert [enable|disable]
        set user-peer {string}
        set cipher [any|high|...]
        set auth [any|local|...]
    next
end

```

```

set dtls-tunnel [enable|disable]
set dtls-max-proto-ver [dtls1-0|dtls1-2]
set dtls-min-proto-ver [dtls1-0|dtls1-2]
set check-referer [enable|disable]
set http-request-header-timeout {integer}
set http-request-body-timeout {integer}
set auth-session-check-source-ip [enable|disable]
set tunnel-connect-without-reauth [enable|disable]
set tunnel-user-session-timeout {integer}
set hsts-include-subdomains [enable|disable]
set transform-backward-slashes [enable|disable]
set encode-2f-sequence [enable|disable]
set encrypt-and-store-password [enable|disable]
set client-sigalgs [no-rsa-pss|all]
end

```

## config vpn ssl settings

Parameter	Description	Type	Size	Default										
status	Enable/disable SSL-VPN.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable SSL-VPN.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable SSL-VPN.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SSL-VPN.	<i>disable</i>	Disable SSL-VPN.							
Option	Description													
<i>enable</i>	Enable SSL-VPN.													
<i>disable</i>	Disable SSL-VPN.													
reqclientcert	Enable/disable to require client certificates for all SSL-VPN users.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
user-peer	Name of user peer.	string	Maximum length: 35											
ssl-max-proto-ver	SSL maximum protocol version.	option	-	tls1-3										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tls1-0</i></td> <td>TLS version 1.0.</td> </tr> <tr> <td><i>tls1-1</i></td> <td>TLS version 1.1.</td> </tr> <tr> <td><i>tls1-2</i></td> <td>TLS version 1.2.</td> </tr> <tr> <td><i>tls1-3</i></td> <td>TLS version 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>tls1-0</i>	TLS version 1.0.	<i>tls1-1</i>	TLS version 1.1.	<i>tls1-2</i>	TLS version 1.2.	<i>tls1-3</i>	TLS version 1.3.			
Option	Description													
<i>tls1-0</i>	TLS version 1.0.													
<i>tls1-1</i>	TLS version 1.1.													
<i>tls1-2</i>	TLS version 1.2.													
<i>tls1-3</i>	TLS version 1.3.													
ssl-min-proto-ver	SSL minimum protocol version.	option	-	tls1-2										

Parameter	Description	Type	Size	Default																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tls1-0</i></td> <td>TLS version 1.0.</td> </tr> <tr> <td><i>tls1-1</i></td> <td>TLS version 1.1.</td> </tr> <tr> <td><i>tls1-2</i></td> <td>TLS version 1.2.</td> </tr> <tr> <td><i>tls1-3</i></td> <td>TLS version 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>tls1-0</i>	TLS version 1.0.	<i>tls1-1</i>	TLS version 1.1.	<i>tls1-2</i>	TLS version 1.2.	<i>tls1-3</i>	TLS version 1.3.																											
Option	Description																																					
<i>tls1-0</i>	TLS version 1.0.																																					
<i>tls1-1</i>	TLS version 1.1.																																					
<i>tls1-2</i>	TLS version 1.2.																																					
<i>tls1-3</i>	TLS version 1.3.																																					
banned-cipher	Select one or more cipher technologies that cannot be used in SSL-VPN negotiations. Only applies to TLS 1.2 and below.	option	-																																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>RSA</i></td> <td>Ban the use of cipher suites using RSA key.</td> </tr> <tr> <td><i>DHE</i></td> <td>Ban the use of cipher suites using authenticated ephemeral DH key agreement.</td> </tr> <tr> <td><i>ECDHE</i></td> <td>Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.</td> </tr> <tr> <td><i>DSS</i></td> <td>Ban the use of cipher suites using DSS authentication.</td> </tr> <tr> <td><i>ECDSA</i></td> <td>Ban the use of cipher suites using ECDSA authentication.</td> </tr> <tr> <td><i>AES</i></td> <td>Ban the use of cipher suites using either 128 or 256 bit AES.</td> </tr> <tr> <td><i>AESGCM</i></td> <td>Ban the use of cipher suites AES in Galois Counter Mode (GCM).</td> </tr> <tr> <td><i>CAMELLIA</i></td> <td>Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.</td> </tr> <tr> <td><i>3DES</i></td> <td>Ban the use of cipher suites using triple DES</td> </tr> <tr> <td><i>SHA1</i></td> <td>Ban the use of cipher suites using HMAC-SHA1.</td> </tr> <tr> <td><i>SHA256</i></td> <td>Ban the use of cipher suites using HMAC-SHA256.</td> </tr> <tr> <td><i>SHA384</i></td> <td>Ban the use of cipher suites using HMAC-SHA384.</td> </tr> <tr> <td><i>STATIC</i></td> <td>Ban the use of cipher suites using static keys.</td> </tr> <tr> <td><i>CHACHA20</i></td> <td>Ban the use of cipher suites using ChaCha20.</td> </tr> <tr> <td><i>ARIA</i></td> <td>Ban the use of cipher suites using ARIA.</td> </tr> <tr> <td><i>AESCCM</i></td> <td>Ban the use of cipher suites using AESCCM.</td> </tr> </tbody> </table>	Option	Description	<i>RSA</i>	Ban the use of cipher suites using RSA key.	<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.	<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.	<i>DSS</i>	Ban the use of cipher suites using DSS authentication.	<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.	<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.	<i>AESGCM</i>	Ban the use of cipher suites AES in Galois Counter Mode (GCM).	<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.	<i>3DES</i>	Ban the use of cipher suites using triple DES	<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.	<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.	<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.	<i>STATIC</i>	Ban the use of cipher suites using static keys.	<i>CHACHA20</i>	Ban the use of cipher suites using ChaCha20.	<i>ARIA</i>	Ban the use of cipher suites using ARIA.	<i>AESCCM</i>	Ban the use of cipher suites using AESCCM.			
Option	Description																																					
<i>RSA</i>	Ban the use of cipher suites using RSA key.																																					
<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.																																					
<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.																																					
<i>DSS</i>	Ban the use of cipher suites using DSS authentication.																																					
<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.																																					
<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.																																					
<i>AESGCM</i>	Ban the use of cipher suites AES in Galois Counter Mode (GCM).																																					
<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.																																					
<i>3DES</i>	Ban the use of cipher suites using triple DES																																					
<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.																																					
<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.																																					
<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.																																					
<i>STATIC</i>	Ban the use of cipher suites using static keys.																																					
<i>CHACHA20</i>	Ban the use of cipher suites using ChaCha20.																																					
<i>ARIA</i>	Ban the use of cipher suites using ARIA.																																					
<i>AESCCM</i>	Ban the use of cipher suites using AESCCM.																																					

Parameter	Description	Type	Size	Default												
ciphersuite	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, set ssl-max-proto-ver to tls1-2 or below.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TLS-AES-128-GCM-SHA256</i></td> <td>Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.</td> </tr> <tr> <td><i>TLS-AES-256-GCM-SHA384</i></td> <td>Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.</td> </tr> <tr> <td><i>TLS-CHACHA20-POLY1305-SHA256</i></td> <td>Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.</td> </tr> <tr> <td><i>TLS-AES-128-CCM-SHA256</i></td> <td>Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.</td> </tr> <tr> <td><i>TLS-AES-128-CCM-8-SHA256</i></td> <td>Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.</td> </tr> </tbody> </table>	Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.	<i>TLS-AES-256-GCM-SHA384</i>	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.	<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.	<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.			
Option	Description															
<i>TLS-AES-128-GCM-SHA256</i>	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.															
<i>TLS-AES-256-GCM-SHA384</i>	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.															
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.															
<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.															
<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.															
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
https-redirect	Enable/disable redirect of port 80 to SSL-VPN port.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-	enable												

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
ssl-client-renegotiation	Enable/disable to allow client renegotiation by the server if the tunnel goes down.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Abort any SSL connection that attempts to renegotiate.</td> </tr> <tr> <td><i>enable</i></td> <td>Allow a SSL client to renegotiate.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Abort any SSL connection that attempts to renegotiate.	<i>enable</i>	Allow a SSL client to renegotiate.							
Option	Description													
<i>disable</i>	Abort any SSL connection that attempts to renegotiate.													
<i>enable</i>	Allow a SSL client to renegotiate.													
force-two-factor-auth	Enable/disable only PKI users with two-factor authentication for SSL-VPNs.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
servercert	Name of the server certificate to be used for SSL-VPNs.	string	Maximum length: 35	Fortinet_Factory**										
algorithm	Force the SSL-VPN security level. High allows only high. Medium allows medium and high. Low allows any.	option	-	high										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High algorithms.</td> </tr> <tr> <td><i>medium</i></td> <td>High and medium algorithms.</td> </tr> <tr> <td><i>default</i></td> <td>default</td> </tr> <tr> <td><i>low</i></td> <td>All algorithms.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High algorithms.	<i>medium</i>	High and medium algorithms.	<i>default</i>	default	<i>low</i>	All algorithms.			
Option	Description													
<i>high</i>	High algorithms.													
<i>medium</i>	High and medium algorithms.													
<i>default</i>	default													
<i>low</i>	All algorithms.													

Parameter	Description	Type	Size	Default
idle-timeout	SSL-VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200	300
auth-timeout	SSL-VPN authentication timeout .	integer	Minimum value: 0 Maximum value: 259200	28800
login-attempt-limit	SSL-VPN maximum login attempt times before block .	integer	Minimum value: 0 Maximum value: 4294967295	2
login-block-time	Time for which a user is blocked from logging in after too many failed login attempts .	integer	Minimum value: 0 Maximum value: 4294967295	60
login-timeout	SSLVPN maximum login timeout .	integer	Minimum value: 10 Maximum value: 180	30
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout .	integer	Minimum value: 10 Maximum value: 60	10
tunnel-ip-pools <name>	Names of the IPv4 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79	
tunnel-ipv6-pools <name>	Names of the IPv6 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79	
dns-suffix	DNS suffix used for SSL-VPN clients.	var-string	Maximum length: 253	
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0						
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0						
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::						
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::						
url-obscuration	Enable/disable to obscure the host name of the URL of the web browser display.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
http-compression	Enable/disable to allow HTTP compression over SSL-VPN tunnels.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
http-only-cookie	Enable/disable SSL-VPN support for HttpOnly cookies.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
deflate-compression-level	Compression level (0~9).	integer	Minimum value: 0 Maximum value: 9	6						



Parameter	Description	Type	Size	Default								
deflate-min-data-size	Minimum amount of data that triggers compression .	integer	Minimum value: 200 Maximum value: 65535	300								
port	SSL-VPN access port .	integer	Minimum value: 1 Maximum value: 65535	10443								
port-precedence	Enable/disable, Enable means that if SSL-VPN connections are allowed on an interface admin GUI connections are blocked on that interface.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
auto-tunnel-static-route	Enable/disable to auto-create static routes for the SSL-VPN tunnel IP addresses.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-	add								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35									
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79									
source-address-negate	Enable/disable negated source address match.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79							
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-portal	Default SSL-VPN portal.	string	Maximum length: 35							
dtls-tunnel	Enable/disable DTLS to prevent eavesdropping, tampering, or message forgery.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dtls-max-protocol-ver	DTLS maximum protocol version.	option	-	dtls1-2						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dtls1-0</i></td> <td>DTLS version 1.0.</td> </tr> <tr> <td><i>dtls1-2</i></td> <td>DTLS version 1.2.</td> </tr> </tbody> </table>	Option	Description	<i>dtls1-0</i>	DTLS version 1.0.	<i>dtls1-2</i>	DTLS version 1.2.			
Option	Description									
<i>dtls1-0</i>	DTLS version 1.0.									
<i>dtls1-2</i>	DTLS version 1.2.									
dtls-min-protocol-ver	DTLS minimum protocol version.	option	-	dtls1-0						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dtls1-0</i></td> <td>DTLS version 1.0.</td> </tr> <tr> <td><i>dtls1-2</i></td> <td>DTLS version 1.2.</td> </tr> </tbody> </table>	Option	Description	<i>dtls1-0</i>	DTLS version 1.0.	<i>dtls1-2</i>	DTLS version 1.2.			
Option	Description									
<i>dtls1-0</i>	DTLS version 1.0.									
<i>dtls1-2</i>	DTLS version 1.2.									
check-referer	Enable/disable verification of referer field in HTTP request header.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of referer field in HTTP request header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of referer field in HTTP request header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of referer field in HTTP request header.	<i>disable</i>	Disable verification of referer field in HTTP request header.			
Option	Description									
<i>enable</i>	Enable verification of referer field in HTTP request header.									
<i>disable</i>	Disable verification of referer field in HTTP request header.									
http-request-header-timeout	SSL-VPN session is disconnected if an HTTP request header is not received within this time .	integer	Minimum value: 0 Maximum value: 4294967295	20						
http-request-body-timeout	SSL-VPN session is disconnected if an HTTP request body is not received within this time .	integer	Minimum value: 0 Maximum value: 4294967295	30						
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable checking of source IP for authentication session.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable checking of source IP for authentication session.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable checking of source IP for authentication session.	<i>disable</i>	Disable checking of source IP for authentication session.			
Option	Description									
<i>enable</i>	Enable checking of source IP for authentication session.									
<i>disable</i>	Disable checking of source IP for authentication session.									
tunnel-connect-without-reauth	Enable/disable tunnel connection without re-authorization if previous connection dropped.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable tunnel connection without re-authorization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable tunnel connection without re-authorization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable tunnel connection without re-authorization.	<i>disable</i>	Disable tunnel connection without re-authorization.			
Option	Description									
<i>enable</i>	Enable tunnel connection without re-authorization.									
<i>disable</i>	Disable tunnel connection without re-authorization.									
tunnel-user-session-timeout	Time out value to clean up user session after tunnel connection is dropped .	integer	Minimum value: 1 Maximum value: 255	30						
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
encode-2f-sequence	Encode %2F sequence to forward slash in URLs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
encrypt-and-store-password	Encrypt and store user passwords for SSL-VPN web sessions.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
client-sigalgs	Set signature algorithms related to client authentication. Affects TLS version <= 1.2 only.	option	-	all						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-rsa-pss</i></td> <td>Disable RSA-PSS signature algorithms for client authentication.</td> </tr> <tr> <td><i>all</i></td> <td>Enable all supported signature algorithms for client authentication.</td> </tr> </tbody> </table>	Option	Description	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.	<i>all</i>	Enable all supported signature algorithms for client authentication.			
Option	Description									
<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.									
<i>all</i>	Enable all supported signature algorithms for client authentication.									

\*\* Values may differ between models.

### config authentication-rule

Parameter	Description	Type	Size	Default
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
source-address-negate	Enable/disable negated source address match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79							
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
users <name>	User name. User name.	string	Maximum length: 79							
groups <name>	User groups. Group name.	string	Maximum length: 79							
portal	SSL-VPN portal.	string	Maximum length: 35							
realm	SSL-VPN realm.	string	Maximum length: 35							
client-cert	Enable/disable SSL-VPN client certificate restrictive.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
user-peer	Name of user peer.	string	Maximum length: 35							
cipher	SSL-VPN cipher strength.	option	-	high						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Any cipher strength.</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Any cipher strength.					
Option	Description									
<i>any</i>	Any cipher strength.									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High cipher strength (&gt;= 168 bits).</td> </tr> <tr> <td><i>medium</i></td> <td>Medium cipher strength (&gt;= 128 bits).</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High cipher strength (>= 168 bits).	<i>medium</i>	Medium cipher strength (>= 128 bits).									
Option	Description															
<i>high</i>	High cipher strength (>= 168 bits).															
<i>medium</i>	Medium cipher strength (>= 128 bits).															
auth	SSL-VPN authentication method restriction.	option	-	any												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Any</td> </tr> <tr> <td><i>local</i></td> <td>Local</td> </tr> <tr> <td><i>radius</i></td> <td>RADIUS</td> </tr> <tr> <td><i>tacacs+</i></td> <td>TACACS+</td> </tr> <tr> <td><i>ldap</i></td> <td>LDAP</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Any	<i>local</i>	Local	<i>radius</i>	RADIUS	<i>tacacs+</i>	TACACS+	<i>ldap</i>	LDAP			
Option	Description															
<i>any</i>	Any															
<i>local</i>	Local															
<i>radius</i>	RADIUS															
<i>tacacs+</i>	TACACS+															
<i>ldap</i>	LDAP															

## config vpn ssl monitor

SSL-VPN session.

```
config vpn ssl monitor
  Description: SSL-VPN session.
end
```

## config vpn ipsec phase1

Configure VPN remote gateway.

```
config vpn ipsec phase1
  Description: Configure VPN remote gateway.
  edit <name>
    set type [static|dynamic|...]
    set interface {string}
    set ike-version [1|2]
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address}
    set remotegw-ddns {string}
    set keylife {integer}
    set certificate <name1>, <name2>, ...
    set authmethod [psk|signature]
    set authmethod-remote [psk|signature]
    set mode [aggressive|main]
    set peertype [any|one|...]
    set peerid {string}
    set usrgrp {string}
    set peer {string}
    set peergrp {string}
    set mode-cfg [disable|enable]
    set assign-ip [disable|enable]
```

```

set assign-ip-from [range|usrgrp|...]
set ipv4-start-ip {ipv4-address}
set ipv4-end-ip {ipv4-address}
set ipv4-netmask {ipv4-netmask}
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dns-mode [manual|auto]
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
set ipv4-split-include {string}
set split-include-service {string}
set ipv4-name {string}
set ipv6-start-ip {ipv6-address}
set ipv6-end-ip {ipv6-address}
set ipv6-prefix {integer}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set ipv6-split-include {string}
set ipv6-name {string}
set unity-support [disable|enable]
set domain {string}
set banner {var-string}
set include-local-lan [disable|enable]
set ipv4-split-exclude {string}
set ipv6-split-exclude {string}
set save-password [disable|enable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set backup-gateway <address1>, <address2>, ...
set proposal {option1}, {option2}, ...
set add-route [disable|enable]
set add-gw-route [enable|disable]
set psksecret {password-3}
set psksecret-remote {password-3}
set keepalive {integer}
set distance {integer}
set priority {integer}
set localid {string}
set localid-type [auto|fqdn|...]

```

```
set auto-negotiate [enable|disable]
set negotiate-timeout {integer}
set fragmentation [enable|disable]
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set forticlient-enforcement [enable|disable]
set comments {var-string}
set npu-offload [enable|disable]
set send-cert-chain [enable|disable]
set dhgrp {option1}, {option2}, ...
set suite-b [disable|suite-b-gcm-128|...]
set eap [enable|disable]
set eap-identity [use-id-payload|send-request]
set eap-exclude-peergrp {string}
set acct-verify [enable|disable]
set ppk [disable|allow|...]
set ppk-secret {password-3}
set ppk-identity {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
set reauth [disable|enable]
set authusr {string}
set authpasswd {password}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set authusrgrp {string}
set mesh-selector-type [disable|subnet|...]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ha-sync-esp-seqno [enable|disable]
set inbound-dscp-copy [enable|disable]
set natTraversal [enable|disable|...]
set fragmentation-mtu {integer}
set childless-ike [enable|disable]
set rekey [enable|disable]
set digital-signature-auth [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set rsa-signature-format [pkcs1|pss]
set enforce-unique-id [disable|keep-new|...]
set cert-id-validation [enable|disable]
set fec-egress [enable|disable]
set fec-send-timeout {integer}
set fec-base {integer}
set fec-codec {integer}
set fec-redundant {integer}
set fec-ingress [enable|disable]
set fec-receive-timeout {integer}
set network-overlay [disable|enable]
set network-id {integer}
next
end
```



## config vpn ipsec phase1

Parameter	Description	Type	Size	Default								
type	Remote gateway type.	option	-	static								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Remote VPN gateway has fixed IP address.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Remote VPN gateway has dynamic IP address.</td> </tr> <tr> <td><i>ddns</i></td> <td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Remote VPN gateway has fixed IP address.	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.			
Option	Description											
<i>static</i>	Remote VPN gateway has fixed IP address.											
<i>dynamic</i>	Remote VPN gateway has dynamic IP address.											
<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.											
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35									
ike-version	IKE protocol version.	option	-	1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Use IKEv1 protocol.</td> </tr> <tr> <td>2</td> <td>Use IKEv2 protocol.</td> </tr> </tbody> </table>	Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.					
Option	Description											
1	Use IKEv1 protocol.											
2	Use IKEv2 protocol.											
remote-gw	Remote VPN gateway.	ipv4-address	Not Specified	0.0.0.0								
local-gw	Local VPN gateway.	ipv4-address	Not Specified	0.0.0.0								
remotegw-ddns	Domain name of remote gateway (eg. name.DDNS.com).	string	Maximum length: 63									
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400								
certificate <name>	Names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79									
authmethod	Authentication method.	option	-	psk								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>psk</i></td> <td>PSK authentication method.</td> </tr> <tr> <td><i>signature</i></td> <td>Signature authentication method.</td> </tr> </tbody> </table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.					
Option	Description											
<i>psk</i>	PSK authentication method.											
<i>signature</i>	Signature authentication method.											
authmethod-remote	Authentication method (remote side).	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>psk</i></td> <td>PSK authentication method.</td> </tr> </tbody> </table>	Option	Description	<i>psk</i>	PSK authentication method.							
Option	Description											
<i>psk</i>	PSK authentication method.											

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>signature</i></td> <td>Signature authentication method.</td> </tr> </tbody> </table>	Option	Description	<i>signature</i>	Signature authentication method.											
Option	Description															
<i>signature</i>	Signature authentication method.															
mode	ID protection mode used to establish a secure channel.	option	-	main												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aggressive</i></td> <td>Aggressive mode.</td> </tr> <tr> <td><i>main</i></td> <td>Main mode.</td> </tr> </tbody> </table>	Option	Description	<i>aggressive</i>	Aggressive mode.	<i>main</i>	Main mode.									
Option	Description															
<i>aggressive</i>	Aggressive mode.															
<i>main</i>	Main mode.															
peertype	Accept this peer type.	option	-	peer												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Accept any peer ID.</td> </tr> <tr> <td><i>one</i></td> <td>Accept this peer ID.</td> </tr> <tr> <td><i>dialup</i></td> <td>Accept peer ID in dialup group.</td> </tr> <tr> <td><i>peer</i></td> <td>Accept this peer certificate.</td> </tr> <tr> <td><i>peergrp</i></td> <td>Accept this peer certificate group.</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.			
Option	Description															
<i>any</i>	Accept any peer ID.															
<i>one</i>	Accept this peer ID.															
<i>dialup</i>	Accept peer ID in dialup group.															
<i>peer</i>	Accept this peer certificate.															
<i>peergrp</i>	Accept this peer certificate group.															
peerid	Accept this peer identity.	string	Maximum length: 255													
usrgrp	User group name for dialup peers.	string	Maximum length: 35													
peer	Accept this peer certificate.	string	Maximum length: 35													
peergrp	Accept this peer certificate group.	string	Maximum length: 35													
mode-cfg	Enable/disable configuration method.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Configuration Method.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Configuration Method.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Configuration Method.	<i>enable</i>	Enable Configuration Method.									
Option	Description															
<i>disable</i>	Disable Configuration Method.															
<i>enable</i>	Enable Configuration Method.															
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not assign an IP address to the IPsec interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Assign an IP address to the IPsec interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not assign an IP address to the IPsec interface.	<i>enable</i>	Assign an IP address to the IPsec interface.									
Option	Description															
<i>disable</i>	Do not assign an IP address to the IPsec interface.															
<i>enable</i>	Assign an IP address to the IPsec interface.															

Parameter	Description	Type	Size	Default										
assign-ip-from	Method by which the IP address will be assigned.	option	-	range										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>range</i></td> <td>Assign IP address from locally defined range.</td> </tr> <tr> <td><i>usrgrp</i></td> <td>Assign IP address via user group.</td> </tr> <tr> <td><i>dhcp</i></td> <td>Assign IP address via DHCP.</td> </tr> <tr> <td><i>name</i></td> <td>Assign IP address from firewall address or group.</td> </tr> </tbody> </table>	Option	Description	<i>range</i>	Assign IP address from locally defined range.	<i>usrgrp</i>	Assign IP address via user group.	<i>dhcp</i>	Assign IP address via DHCP.	<i>name</i>	Assign IP address from firewall address or group.			
Option	Description													
<i>range</i>	Assign IP address from locally defined range.													
<i>usrgrp</i>	Assign IP address via user group.													
<i>dhcp</i>	Assign IP address via DHCP.													
<i>name</i>	Assign IP address from firewall address or group.													
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0										
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0										
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255										
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0										
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::										
dns-mode	DNS server mode.	option	-	manual										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>manual</i></td> <td>Manually configure DNS servers.</td> </tr> <tr> <td><i>auto</i></td> <td>Use default DNS servers.</td> </tr> </tbody> </table>	Option	Description	<i>manual</i>	Manually configure DNS servers.	<i>auto</i>	Use default DNS servers.							
Option	Description													
<i>manual</i>	Manually configure DNS servers.													
<i>auto</i>	Use default DNS servers.													
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0										
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0										
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0										
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0										
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0										
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79											
split-include-service	Split-include services.	string	Maximum length: 79											
ipv4-name	IPv4 address name.	string	Maximum length: 79											
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::										

Parameter	Description	Type	Size	Default						
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::						
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128						
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::						
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79							
ipv6-name	IPv6 address name.	string	Maximum length: 79							
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Cisco Unity Configuration Method Extensions.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Cisco Unity Configuration Method Extensions.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.	<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.			
Option	Description									
<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.									
<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.									
domain	Instruct unity clients about the default DNS domain.	string	Maximum length: 63							
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024							
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable local LAN access on Unity clients.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable local LAN access on Unity clients.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable local LAN access on Unity clients.	<i>enable</i>	Enable local LAN access on Unity clients.			
Option	Description									
<i>disable</i>	Disable local LAN access on Unity clients.									
<i>enable</i>	Enable local LAN access on Unity clients.									
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable						

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable saving XAuth username and password on VPN clients.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable saving XAuth username and password on VPN clients.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable saving XAuth username and password on VPN clients.	<i>enable</i>	Enable saving XAuth username and password on VPN clients.															
Option	Description																					
<i>disable</i>	Disable saving XAuth username and password on VPN clients.																					
<i>enable</i>	Enable saving XAuth username and password on VPN clients.																					
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable allowing the VPN client to bring up the tunnel when there is no traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable allowing the VPN client to bring up the tunnel when there is no traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.															
Option	Description																					
<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.																					
<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.																					
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable allowing the VPN client to keep the tunnel up when there is no traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable allowing the VPN client to keep the tunnel up when there is no traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.															
Option	Description																					
<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.																					
<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.																					
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79																			
proposal	Phase1 proposal.	option	-																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>des-md5</i></td> <td>des-md5</td> </tr> <tr> <td><i>des-sha1</i></td> <td>des-sha1</td> </tr> <tr> <td><i>des-sha256</i></td> <td>des-sha256</td> </tr> <tr> <td><i>des-sha384</i></td> <td>des-sha384</td> </tr> <tr> <td><i>des-sha512</i></td> <td>des-sha512</td> </tr> <tr> <td><i>3des-md5</i></td> <td>3des-md5</td> </tr> <tr> <td><i>3des-sha1</i></td> <td>3des-sha1</td> </tr> <tr> <td><i>3des-sha256</i></td> <td>3des-sha256</td> </tr> </tbody> </table>	Option	Description	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256			
Option	Description																					
<i>des-md5</i>	des-md5																					
<i>des-sha1</i>	des-sha1																					
<i>des-sha256</i>	des-sha256																					
<i>des-sha384</i>	des-sha384																					
<i>des-sha512</i>	des-sha512																					
<i>3des-md5</i>	3des-md5																					
<i>3des-sha1</i>	3des-sha1																					
<i>3des-sha256</i>	3des-sha256																					

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1		
	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256		
	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384		
	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1		
	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256		
	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1		
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256		
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384		
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512		

Parameter	Description	Type	Size	Default																																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aria128-md5</i></td> <td>aria128-md5</td> </tr> <tr> <td><i>aria128-sha1</i></td> <td>aria128-sha1</td> </tr> <tr> <td><i>aria128-sha256</i></td> <td>aria128-sha256</td> </tr> <tr> <td><i>aria128-sha384</i></td> <td>aria128-sha384</td> </tr> <tr> <td><i>aria128-sha512</i></td> <td>aria128-sha512</td> </tr> <tr> <td><i>aria192-md5</i></td> <td>aria192-md5</td> </tr> <tr> <td><i>aria192-sha1</i></td> <td>aria192-sha1</td> </tr> <tr> <td><i>aria192-sha256</i></td> <td>aria192-sha256</td> </tr> <tr> <td><i>aria192-sha384</i></td> <td>aria192-sha384</td> </tr> <tr> <td><i>aria192-sha512</i></td> <td>aria192-sha512</td> </tr> <tr> <td><i>aria256-md5</i></td> <td>aria256-md5</td> </tr> <tr> <td><i>aria256-sha1</i></td> <td>aria256-sha1</td> </tr> <tr> <td><i>aria256-sha256</i></td> <td>aria256-sha256</td> </tr> <tr> <td><i>aria256-sha384</i></td> <td>aria256-sha384</td> </tr> <tr> <td><i>aria256-sha512</i></td> <td>aria256-sha512</td> </tr> <tr> <td><i>seed-md5</i></td> <td>seed-md5</td> </tr> <tr> <td><i>seed-sha1</i></td> <td>seed-sha1</td> </tr> <tr> <td><i>seed-sha256</i></td> <td>seed-sha256</td> </tr> <tr> <td><i>seed-sha384</i></td> <td>seed-sha384</td> </tr> <tr> <td><i>seed-sha512</i></td> <td>seed-sha512</td> </tr> </tbody> </table>	Option	Description	<i>aria128-md5</i>	aria128-md5	<i>aria128-sha1</i>	aria128-sha1	<i>aria128-sha256</i>	aria128-sha256	<i>aria128-sha384</i>	aria128-sha384	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
Option	Description																																													
<i>aria128-md5</i>	aria128-md5																																													
<i>aria128-sha1</i>	aria128-sha1																																													
<i>aria128-sha256</i>	aria128-sha256																																													
<i>aria128-sha384</i>	aria128-sha384																																													
<i>aria128-sha512</i>	aria128-sha512																																													
<i>aria192-md5</i>	aria192-md5																																													
<i>aria192-sha1</i>	aria192-sha1																																													
<i>aria192-sha256</i>	aria192-sha256																																													
<i>aria192-sha384</i>	aria192-sha384																																													
<i>aria192-sha512</i>	aria192-sha512																																													
<i>aria256-md5</i>	aria256-md5																																													
<i>aria256-sha1</i>	aria256-sha1																																													
<i>aria256-sha256</i>	aria256-sha256																																													
<i>aria256-sha384</i>	aria256-sha384																																													
<i>aria256-sha512</i>	aria256-sha512																																													
<i>seed-md5</i>	seed-md5																																													
<i>seed-sha1</i>	seed-sha1																																													
<i>seed-sha256</i>	seed-sha256																																													
<i>seed-sha384</i>	seed-sha384																																													
<i>seed-sha512</i>	seed-sha512																																													
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	disable																																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add a route to destination of peer selector.</td> </tr> <tr> <td><i>enable</i></td> <td>Add route to destination of peer selector.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add a route to destination of peer selector.	<i>enable</i>	Add route to destination of peer selector.																																							
Option	Description																																													
<i>disable</i>	Do not add a route to destination of peer selector.																																													
<i>enable</i>	Add route to destination of peer selector.																																													
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable																																										

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Automatically add a route to the remote gateway.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not automatically add a route to the remote gateway.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Automatically add a route to the remote gateway.	<i>disable</i>	Do not automatically add a route to the remote gateway.											
Option	Description																	
<i>enable</i>	Automatically add a route to the remote gateway.																	
<i>disable</i>	Do not automatically add a route to the remote gateway.																	
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified															
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified															
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10														
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255	15														
priority	Priority for routes added by IKE .	integer	Minimum value: 0 Maximum value: 4294967295	0														
localid	Local ID.	string	Maximum length: 63															
localid-type	Local ID type.	option	-	auto														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Select ID type automatically.</td> </tr> <tr> <td><i>fqdn</i></td> <td>Use fully qualified domain name.</td> </tr> <tr> <td><i>user-fqdn</i></td> <td>Use user fully qualified domain name.</td> </tr> <tr> <td><i>keyid</i></td> <td>Use key-id string.</td> </tr> <tr> <td><i>address</i></td> <td>Use local IP address.</td> </tr> <tr> <td><i>asn1dn</i></td> <td>Use ASN.1 distinguished name.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Select ID type automatically.	<i>fqdn</i>	Use fully qualified domain name.	<i>user-fqdn</i>	Use user fully qualified domain name.	<i>keyid</i>	Use key-id string.	<i>address</i>	Use local IP address.	<i>asn1dn</i>	Use ASN.1 distinguished name.			
Option	Description																	
<i>auto</i>	Select ID type automatically.																	
<i>fqdn</i>	Use fully qualified domain name.																	
<i>user-fqdn</i>	Use user fully qualified domain name.																	
<i>keyid</i>	Use key-id string.																	
<i>address</i>	Use local IP address.																	
<i>asn1dn</i>	Use ASN.1 distinguished name.																	
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable														



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic initiation of IKE SA negotiation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic initiation of IKE SA negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.					
Option	Description											
<i>enable</i>	Enable automatic initiation of IKE SA negotiation.											
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.											
negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300	30								
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable intra-IKE fragmentation support on re-transmission.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable intra-IKE fragmentation support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.					
Option	Description											
<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.											
<i>disable</i>	Disable intra-IKE fragmentation support.											
dpd	Dead Peer Detection mode.	option	-	on-demand								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Dead Peer Detection.</td> </tr> <tr> <td><i>on-idle</i></td> <td>Trigger Dead Peer Detection when IPsec is idle.</td> </tr> <tr> <td><i>on-demand</i></td> <td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Dead Peer Detection.	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.			
Option	Description											
<i>disable</i>	Disable Dead Peer Detection.											
<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.											
<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.											
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3								
dpd-retryinterval	DPD retry interval.	user	Not Specified									
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiClient enforcement.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiClient enforcement.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiClient enforcement.	<i>disable</i>	Disable FortiClient enforcement.					
Option	Description											
<i>enable</i>	Enable FortiClient enforcement.											
<i>disable</i>	Disable FortiClient enforcement.											
comments	Comment.	var-string	Maximum length: 255									
npu-offload *	Enable/disable offloading NPU.	option	-	enable								

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NPU offloading.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NPU offloading.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.																																	
Option	Description																																							
<i>enable</i>	Enable NPU offloading.																																							
<i>disable</i>	Disable NPU offloading.																																							
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending certificate chain.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending certificate chain.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending certificate chain.	<i>disable</i>	Disable sending certificate chain.																																	
Option	Description																																							
<i>enable</i>	Enable sending certificate chain.																																							
<i>disable</i>	Disable sending certificate chain.																																							
dhgrp	DH group.	option	-	14																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>DH Group 1.</td> </tr> <tr> <td>2</td> <td>DH Group 2.</td> </tr> <tr> <td>5</td> <td>DH Group 5.</td> </tr> <tr> <td>14</td> <td>DH Group 14.</td> </tr> <tr> <td>15</td> <td>DH Group 15.</td> </tr> <tr> <td>16</td> <td>DH Group 16.</td> </tr> <tr> <td>17</td> <td>DH Group 17.</td> </tr> <tr> <td>18</td> <td>DH Group 18.</td> </tr> <tr> <td>19</td> <td>DH Group 19.</td> </tr> <tr> <td>20</td> <td>DH Group 20.</td> </tr> <tr> <td>21</td> <td>DH Group 21.</td> </tr> <tr> <td>27</td> <td>DH Group 27.</td> </tr> <tr> <td>28</td> <td>DH Group 28.</td> </tr> <tr> <td>29</td> <td>DH Group 29.</td> </tr> <tr> <td>30</td> <td>DH Group 30.</td> </tr> <tr> <td>31</td> <td>DH Group 31.</td> </tr> <tr> <td>32</td> <td>DH Group 32.</td> </tr> </tbody> </table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
Option	Description																																							
1	DH Group 1.																																							
2	DH Group 2.																																							
5	DH Group 5.																																							
14	DH Group 14.																																							
15	DH Group 15.																																							
16	DH Group 16.																																							
17	DH Group 17.																																							
18	DH Group 18.																																							
19	DH Group 19.																																							
20	DH Group 20.																																							
21	DH Group 21.																																							
27	DH Group 27.																																							
28	DH Group 28.																																							
29	DH Group 29.																																							
30	DH Group 30.																																							
31	DH Group 31.																																							
32	DH Group 32.																																							
suite-b	Use Suite-B.	option	-	disable																																				

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not use UI suite.</td> </tr> <tr> <td><i>suite-b-gcm-128</i></td> <td>Use Suite-B-GCM-128.</td> </tr> <tr> <td><i>suite-b-gcm-256</i></td> <td>Use Suite-B-GCM-256.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not use UI suite.	<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.	<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.			
Option	Description											
<i>disable</i>	Do not use UI suite.											
<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.											
<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.											
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 EAP authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKEv2 EAP authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.					
Option	Description											
<i>enable</i>	Enable IKEv2 EAP authentication.											
<i>disable</i>	Disable IKEv2 EAP authentication.											
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>use-id-payload</i></td> <td>Use IKEv2 IDi payload to resolve peer identity.</td> </tr> <tr> <td><i>send-request</i></td> <td>Use EAP identity request to resolve peer identity.</td> </tr> </tbody> </table>	Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.					
Option	Description											
<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.											
<i>send-request</i>	Use EAP identity request to resolve peer identity.											
eap-exclude-peergp	Peer group excluded from EAP authentication.	string	Maximum length: 35									
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of RADIUS accounting record.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of RADIUS accounting record.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of RADIUS accounting record.	<i>disable</i>	Disable verification of RADIUS accounting record.					
Option	Description											
<i>enable</i>	Enable verification of RADIUS accounting record.											
<i>disable</i>	Disable verification of RADIUS accounting record.											
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td> </tr> <tr> <td><i>allow</i></td> <td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td> </tr> <tr> <td><i>require</i></td> <td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).			
Option	Description											
<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).											
<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).											
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).											
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified									

Parameter	Description	Type	Size	Default																												
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35																													
wizard-type	GUI VPN Wizard Type.	option	-	custom																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>custom</i></td> <td>Custom VPN configuration.</td> </tr> <tr> <td><i>dialup-forticlient</i></td> <td>Dial Up - FortiClient Windows, Mac and Android.</td> </tr> <tr> <td><i>dialup-ios</i></td> <td>Dial Up - iPhone / iPad Native IPsec Client.</td> </tr> <tr> <td><i>dialup-android</i></td> <td>Dial Up - Android Native IPsec Client.</td> </tr> <tr> <td><i>dialup-windows</i></td> <td>Dial Up - Windows Native IPsec Client.</td> </tr> <tr> <td><i>dialup-cisco</i></td> <td>Dial Up - Cisco IPsec Client.</td> </tr> <tr> <td><i>static-fortigate</i></td> <td>Site to Site - FortiGate.</td> </tr> <tr> <td><i>dialup-fortigate</i></td> <td>Dial Up - FortiGate.</td> </tr> <tr> <td><i>static-cisco</i></td> <td>Site to Site - Cisco.</td> </tr> <tr> <td><i>dialup-cisco-fw</i></td> <td>Dialup Up - Cisco Firewall.</td> </tr> <tr> <td><i>simplified-static-fortigate</i></td> <td>Site to Site - FortiGate (SD-WAN).</td> </tr> <tr> <td><i>hub-fortigate-auto-discovery</i></td> <td>Hub role in a Hub-and-Spoke auto-discovery VPN.</td> </tr> <tr> <td><i>spoke-fortigate-auto-discovery</i></td> <td>Spoke role in a Hub-and-Spoke auto-discovery VPN.</td> </tr> </tbody> </table>	Option	Description	<i>custom</i>	Custom VPN configuration.	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	<i>static-fortigate</i>	Site to Site - FortiGate.	<i>dialup-fortigate</i>	Dial Up - FortiGate.	<i>static-cisco</i>	Site to Site - Cisco.	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.			
Option	Description																															
<i>custom</i>	Custom VPN configuration.																															
<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.																															
<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.																															
<i>dialup-android</i>	Dial Up - Android Native IPsec Client.																															
<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.																															
<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.																															
<i>static-fortigate</i>	Site to Site - FortiGate.																															
<i>dialup-fortigate</i>	Dial Up - FortiGate.																															
<i>static-cisco</i>	Site to Site - Cisco.																															
<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.																															
<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).																															
<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.																															
<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.																															
xauthtype	XAuth type.	option	-	disable																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>client</i></td> <td>Enable as client.</td> </tr> <tr> <td><i>pap</i></td> <td>Enable as server PAP.</td> </tr> <tr> <td><i>chap</i></td> <td>Enable as server CHAP.</td> </tr> <tr> <td><i>auto</i></td> <td>Enable as server auto.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>client</i>	Enable as client.	<i>pap</i>	Enable as server PAP.	<i>chap</i>	Enable as server CHAP.	<i>auto</i>	Enable as server auto.																			
Option	Description																															
<i>disable</i>	Disable.																															
<i>client</i>	Enable as client.																															
<i>pap</i>	Enable as server PAP.																															
<i>chap</i>	Enable as server CHAP.																															
<i>auto</i>	Enable as server auto.																															
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable																												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IKE SA re-authentication.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable IKE SA re-authentication.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.					
Option	Description											
<i>disable</i>	Disable IKE SA re-authentication.											
<i>enable</i>	Enable IKE SA re-authentication.											
authusr	XAuth user name.	string	Maximum length: 64									
authpasswd	XAuth password (max 35 characters).	password	Not Specified									
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 IDi group authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKEv2 IDi group authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 IDi group authentication.	<i>disable</i>	Disable IKEv2 IDi group authentication.					
Option	Description											
<i>enable</i>	Enable IKEv2 IDi group authentication.											
<i>disable</i>	Disable IKEv2 IDi group authentication.											
group-authentication-secret	Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by a leading 0x.)	password-3	Not Specified									
authusrgrp	Authentication user group.	string	Maximum length: 35									
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>subnet</i></td> <td>Enable addition of matching subnet selector.</td> </tr> <tr> <td><i>host</i></td> <td>Enable addition of host to host selector.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>subnet</i>	Enable addition of matching subnet selector.	<i>host</i>	Enable addition of host to host selector.			
Option	Description											
<i>disable</i>	Disable.											
<i>subnet</i>	Enable addition of matching subnet selector.											
<i>host</i>	Enable addition of host to host selector.											
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec tunnel idle timeout.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec tunnel idle timeout.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec tunnel idle timeout.	<i>disable</i>	Disable IPsec tunnel idle timeout.					
Option	Description											
<i>enable</i>	Enable IPsec tunnel idle timeout.											
<i>disable</i>	Disable IPsec tunnel idle timeout.											
idle-timeoutinterval	IPsec tunnel idle timeout in minutes .	integer	Minimum value: 5 Maximum value: 43200	15								
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HA syncing of ESP sequence numbers.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HA syncing of ESP sequence numbers.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HA syncing of ESP sequence numbers.	<i>disable</i>	Disable HA syncing of ESP sequence numbers.					
Option	Description											
<i>enable</i>	Enable HA syncing of ESP sequence numbers.											
<i>disable</i>	Disable HA syncing of ESP sequence numbers.											
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable copy the dscp in the ESP header to the inner IP Header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable copy the dscp in the ESP header to the inner IP Header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.	<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.					
Option	Description											
<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.											
<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.											
nattraversal	Enable/disable NAT traversal.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec NAT traversal.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec NAT traversal.</td> </tr> <tr> <td><i>forced</i></td> <td>Force IPsec NAT traversal on.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.			
Option	Description											
<i>enable</i>	Enable IPsec NAT traversal.											
<i>disable</i>	Disable IPsec NAT traversal.											
<i>forced</i>	Force IPsec NAT traversal on.											
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000	1200								
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable childless IKEv2 initiation (RFC 6023).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable childless IKEv2 initiation (RFC 6023).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).					
Option	Description											
<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).											
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).											
rekey	Enable/disable phase1 rekey.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable phase1 rekey.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable phase1 rekey.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.					
Option	Description											
<i>enable</i>	Enable phase1 rekey.											
<i>disable</i>	Disable phase1 rekey.											
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable								

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).	<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).							
Option	Description													
<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).													
<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).													
signature-hash- alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha1</i></td> <td>SHA1.</td> </tr> <tr> <td><i>sha2-256</i></td> <td>SHA2-256.</td> </tr> <tr> <td><i>sha2-384</i></td> <td>SHA2-384.</td> </tr> <tr> <td><i>sha2-512</i></td> <td>SHA2-512.</td> </tr> </tbody> </table>	Option	Description	<i>sha1</i>	SHA1.	<i>sha2-256</i>	SHA2-256.	<i>sha2-384</i>	SHA2-384.	<i>sha2-512</i>	SHA2-512.			
Option	Description													
<i>sha1</i>	SHA1.													
<i>sha2-256</i>	SHA2-256.													
<i>sha2-384</i>	SHA2-384.													
<i>sha2-512</i>	SHA2-512.													
rsa-signature- format	Digital Signature Authentication RSA signature format.	option	-	pkcs1										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pkcs1</i></td> <td>RSASSA PKCS#1 v1.5.</td> </tr> <tr> <td><i>pss</i></td> <td>RSASSA Probabilistic Signature Scheme (PSS).</td> </tr> </tbody> </table>	Option	Description	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).							
Option	Description													
<i>pkcs1</i>	RSASSA PKCS#1 v1.5.													
<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).													
enforce-unique- id	Enable/disable peer ID uniqueness check.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable peer ID uniqueness enforcement.</td> </tr> <tr> <td><i>keep-new</i></td> <td>Enforce peer ID uniqueness, keep new connection if collision found.</td> </tr> <tr> <td><i>keep-old</i></td> <td>Enforce peer ID uniqueness, keep old connection if collision found.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable peer ID uniqueness enforcement.	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.					
Option	Description													
<i>disable</i>	Disable peer ID uniqueness enforcement.													
<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.													
<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.													
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.							
Option	Description													
<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.													
<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.													
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Forward Error Correction for egress IPsec traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Forward Error Correction for egress IPsec traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.			
Option	Description									
<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.									
<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.									
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 1000	8						
fec-base	Number of base Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100	20						
fec-codec	ipsec fec encoding/decoding algorithm (0: reed-solomon, 1: xor).	integer	Minimum value: 0 Maximum value: 1	1						
fec-redundant	Number of redundant Forward Error Correction packets (0 - 100, when fec-codec is reed-solomon or 1 when fec-codec is xor .	integer	Minimum value: 0 Maximum value: 100	1						
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Forward Error Correction for ingress IPsec traffic.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Forward Error Correction for ingress IPsec traffic.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.			
Option	Description									
<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.									
<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.									
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 10000	5000						
network-overlay	Enable/disable network overlays.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable network overlays.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable network overlays.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable network overlays.	<i>enable</i>	Enable network overlays.			
Option	Description									
<i>disable</i>	Disable network overlays.									
<i>enable</i>	Enable network overlays.									
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0						

\* This parameter may not exist in some models.



## config ipv4-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

## config ipv6-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::

## config vpn ipsec phase2

Configure VPN autokey tunnel.

```
config vpn ipsec phase2
  Description: Configure VPN autokey tunnel.
  edit <name>
    set phasename {string}
    set dhcp-ipsec [enable|disable]
    set use-natip [enable|disable]
    set selector-match [exact|subset|...]
    set proposal {option1}, {option2}, ...
    set pfs [enable|disable]
    set ipv4-df [enable|disable]
    set dhgrp {option1}, {option2}, ...
    set replay [enable|disable]
    set keepalive [enable|disable]
    set auto-negotiate [enable|disable]
    set add-route [phase1|enable|...]
    set inbound-dscp-copy [phase1|enable|...]
    set keylifeseconds {integer}
    set keylifekbs {integer}
    set keylife-type [seconds|kbs|...]
    set single-source [enable|disable]
    set route-overlap [use-old|use-new|...]
    set encapsulation [tunnel-mode|transport-mode]
    set l2tp [enable|disable]
    set comments {var-string}
    set initiator-ts-narrow [enable|disable]
    set diffserv [enable|disable]
    set diffservcode {user}
    set protocol {integer}
    set src-name {string}
    set src-name6 {string}
```

```

set src-addr-type [subnet|range|...]
set src-start-ip {ipv4-address-any}
set src-start-ip6 {ipv6-address}
set src-end-ip {ipv4-address-any}
set src-end-ip6 {ipv6-address}
set src-subnet {ipv4-classnet-any}
set src-subnet6 {ipv6-prefix}
set src-port {integer}
set dst-name {string}
set dst-name6 {string}
set dst-addr-type [subnet|range|...]
set dst-start-ip {ipv4-address-any}
set dst-start-ip6 {ipv6-address}
set dst-end-ip {ipv4-address-any}
set dst-end-ip6 {ipv6-address}
set dst-subnet {ipv4-classnet-any}
set dst-subnet6 {ipv6-prefix}
set dst-port {integer}
next
end

```

## config vpn ipsec phase2

Parameter	Description	Type	Size	Default								
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 35									
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
use-natip	Enable to use the FortiGate public IP as the source selector when outbound NAT is used.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Replace source selector with interface IP when using outbound NAT.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not modify source selector when using outbound NAT.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Replace source selector with interface IP when using outbound NAT.	<i>disable</i>	Do not modify source selector when using outbound NAT.					
Option	Description											
<i>enable</i>	Replace source selector with interface IP when using outbound NAT.											
<i>disable</i>	Do not modify source selector when using outbound NAT.											
selector-match	Match type to use when comparing selectors.	option	-	auto								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exact</i></td> <td>Match selectors exactly.</td> </tr> <tr> <td><i>subset</i></td> <td>Match selectors by subset.</td> </tr> <tr> <td><i>auto</i></td> <td>Use subset or exact match depending on selector address type.</td> </tr> </tbody> </table>	Option	Description	<i>exact</i>	Match selectors exactly.	<i>subset</i>	Match selectors by subset.	<i>auto</i>	Use subset or exact match depending on selector address type.			
Option	Description											
<i>exact</i>	Match selectors exactly.											
<i>subset</i>	Match selectors by subset.											
<i>auto</i>	Use subset or exact match depending on selector address type.											

Parameter	Description	Type	Size	Default																																																										
proposal	Phase2 proposal.	option	-																																																											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr><td><i>null-md5</i></td><td>null-md5</td></tr> <tr><td><i>null-sha1</i></td><td>null-sha1</td></tr> <tr><td><i>null-sha256</i></td><td>null-sha256</td></tr> <tr><td><i>null-sha384</i></td><td>null-sha384</td></tr> <tr><td><i>null-sha512</i></td><td>null-sha512</td></tr> <tr><td><i>des-null</i></td><td>des-null</td></tr> <tr><td><i>des-md5</i></td><td>des-md5</td></tr> <tr><td><i>des-sha1</i></td><td>des-sha1</td></tr> <tr><td><i>des-sha256</i></td><td>des-sha256</td></tr> <tr><td><i>des-sha384</i></td><td>des-sha384</td></tr> <tr><td><i>des-sha512</i></td><td>des-sha512</td></tr> <tr><td><i>3des-null</i></td><td>3des-null</td></tr> <tr><td><i>3des-md5</i></td><td>3des-md5</td></tr> <tr><td><i>3des-sha1</i></td><td>3des-sha1</td></tr> <tr><td><i>3des-sha256</i></td><td>3des-sha256</td></tr> <tr><td><i>3des-sha384</i></td><td>3des-sha384</td></tr> <tr><td><i>3des-sha512</i></td><td>3des-sha512</td></tr> <tr><td><i>aes128-null</i></td><td>aes128-null</td></tr> <tr><td><i>aes128-md5</i></td><td>aes128-md5</td></tr> <tr><td><i>aes128-sha1</i></td><td>aes128-sha1</td></tr> <tr><td><i>aes128-sha256</i></td><td>aes128-sha256</td></tr> <tr><td><i>aes128-sha384</i></td><td>aes128-sha384</td></tr> <tr><td><i>aes128-sha512</i></td><td>aes128-sha512</td></tr> <tr><td><i>aes128gcm</i></td><td>aes128gcm</td></tr> <tr><td><i>aes192-null</i></td><td>aes192-null</td></tr> <tr><td><i>aes192-md5</i></td><td>aes192-md5</td></tr> <tr><td><i>aes192-sha1</i></td><td>aes192-sha1</td></tr> <tr><td><i>aes192-sha256</i></td><td>aes192-sha256</td></tr> </tbody> </table>	Option	Description	<i>null-md5</i>	null-md5	<i>null-sha1</i>	null-sha1	<i>null-sha256</i>	null-sha256	<i>null-sha384</i>	null-sha384	<i>null-sha512</i>	null-sha512	<i>des-null</i>	des-null	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-null</i>	3des-null	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384	<i>3des-sha512</i>	3des-sha512	<i>aes128-null</i>	aes128-null	<i>aes128-md5</i>	aes128-md5	<i>aes128-sha1</i>	aes128-sha1	<i>aes128-sha256</i>	aes128-sha256	<i>aes128-sha384</i>	aes128-sha384	<i>aes128-sha512</i>	aes128-sha512	<i>aes128gcm</i>	aes128gcm	<i>aes192-null</i>	aes192-null	<i>aes192-md5</i>	aes192-md5	<i>aes192-sha1</i>	aes192-sha1	<i>aes192-sha256</i>	aes192-sha256			
Option	Description																																																													
<i>null-md5</i>	null-md5																																																													
<i>null-sha1</i>	null-sha1																																																													
<i>null-sha256</i>	null-sha256																																																													
<i>null-sha384</i>	null-sha384																																																													
<i>null-sha512</i>	null-sha512																																																													
<i>des-null</i>	des-null																																																													
<i>des-md5</i>	des-md5																																																													
<i>des-sha1</i>	des-sha1																																																													
<i>des-sha256</i>	des-sha256																																																													
<i>des-sha384</i>	des-sha384																																																													
<i>des-sha512</i>	des-sha512																																																													
<i>3des-null</i>	3des-null																																																													
<i>3des-md5</i>	3des-md5																																																													
<i>3des-sha1</i>	3des-sha1																																																													
<i>3des-sha256</i>	3des-sha256																																																													
<i>3des-sha384</i>	3des-sha384																																																													
<i>3des-sha512</i>	3des-sha512																																																													
<i>aes128-null</i>	aes128-null																																																													
<i>aes128-md5</i>	aes128-md5																																																													
<i>aes128-sha1</i>	aes128-sha1																																																													
<i>aes128-sha256</i>	aes128-sha256																																																													
<i>aes128-sha384</i>	aes128-sha384																																																													
<i>aes128-sha512</i>	aes128-sha512																																																													
<i>aes128gcm</i>	aes128gcm																																																													
<i>aes192-null</i>	aes192-null																																																													
<i>aes192-md5</i>	aes192-md5																																																													
<i>aes192-sha1</i>	aes192-sha1																																																													
<i>aes192-sha256</i>	aes192-sha256																																																													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-null</i>	aria192-null		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		
	<i>aria192-sha384</i>	aria192-sha384		
	<i>aria192-sha512</i>	aria192-sha512		
	<i>aria256-null</i>	aria256-null		
	<i>aria256-md5</i>	aria256-md5		
	<i>aria256-sha1</i>	aria256-sha1		
	<i>aria256-sha256</i>	aria256-sha256		
	<i>aria256-sha384</i>	aria256-sha384		
	<i>aria256-sha512</i>	aria256-sha512		
	<i>seed-null</i>	seed-null		

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>seed-md5</i></td> <td>seed-md5</td> </tr> <tr> <td><i>seed-sha1</i></td> <td>seed-sha1</td> </tr> <tr> <td><i>seed-sha256</i></td> <td>seed-sha256</td> </tr> <tr> <td><i>seed-sha384</i></td> <td>seed-sha384</td> </tr> <tr> <td><i>seed-sha512</i></td> <td>seed-sha512</td> </tr> </tbody> </table>	Option	Description	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512																	
Option	Description																													
<i>seed-md5</i>	seed-md5																													
<i>seed-sha1</i>	seed-sha1																													
<i>seed-sha256</i>	seed-sha256																													
<i>seed-sha384</i>	seed-sha384																													
<i>seed-sha512</i>	seed-sha512																													
pfs	Enable/disable PFS feature.	option	-	enable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																							
Option	Description																													
<i>enable</i>	Enable setting.																													
<i>disable</i>	Disable setting.																													
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Set IPv4 DF.</td> </tr> <tr> <td><i>disable</i></td> <td>Reset IPv4 DF.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Set IPv4 DF.	<i>disable</i>	Reset IPv4 DF.																							
Option	Description																													
<i>enable</i>	Set IPv4 DF.																													
<i>disable</i>	Reset IPv4 DF.																													
dhgrp	Phase2 DH group.	option	-	14																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>DH Group 1.</td> </tr> <tr> <td>2</td> <td>DH Group 2.</td> </tr> <tr> <td>5</td> <td>DH Group 5.</td> </tr> <tr> <td>14</td> <td>DH Group 14.</td> </tr> <tr> <td>15</td> <td>DH Group 15.</td> </tr> <tr> <td>16</td> <td>DH Group 16.</td> </tr> <tr> <td>17</td> <td>DH Group 17.</td> </tr> <tr> <td>18</td> <td>DH Group 18.</td> </tr> <tr> <td>19</td> <td>DH Group 19.</td> </tr> <tr> <td>20</td> <td>DH Group 20.</td> </tr> <tr> <td>21</td> <td>DH Group 21.</td> </tr> <tr> <td>27</td> <td>DH Group 27.</td> </tr> </tbody> </table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.			
Option	Description																													
1	DH Group 1.																													
2	DH Group 2.																													
5	DH Group 5.																													
14	DH Group 14.																													
15	DH Group 15.																													
16	DH Group 16.																													
17	DH Group 17.																													
18	DH Group 18.																													
19	DH Group 19.																													
20	DH Group 20.																													
21	DH Group 21.																													
27	DH Group 27.																													

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>28</td> <td>DH Group 28.</td> </tr> <tr> <td>29</td> <td>DH Group 29.</td> </tr> <tr> <td>30</td> <td>DH Group 30.</td> </tr> <tr> <td>31</td> <td>DH Group 31.</td> </tr> <tr> <td>32</td> <td>DH Group 32.</td> </tr> </tbody> </table>	Option	Description	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
Option	Description															
28	DH Group 28.															
29	DH Group 29.															
30	DH Group 30.															
31	DH Group 31.															
32	DH Group 32.															
replay	Enable/disable replay detection.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
keepalive	Enable/disable keep alive.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
add-route	Enable/disable automatic route addition.	option	-	phase1												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>phase1</i></td> <td>Add route according to phase1 add-route setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Add route for remote proxy ID.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not add route for remote proxy ID.</td> </tr> </tbody> </table>	Option	Description	<i>phase1</i>	Add route according to phase1 add-route setting.	<i>enable</i>	Add route for remote proxy ID.	<i>disable</i>	Do not add route for remote proxy ID.							
Option	Description															
<i>phase1</i>	Add route according to phase1 add-route setting.															
<i>enable</i>	Add route for remote proxy ID.															
<i>disable</i>	Do not add route for remote proxy ID.															
inbound-dscp-copy	Enable/disable copying of the DSCP field in the ESP header to the inner IP header.	option	-	phase1												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>phase1</i></td> <td>Enable/disable copying the DSCP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.</td> </tr> </tbody> </table>	Option	Description	<i>phase1</i>	Enable/disable copying the DSCP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.											
Option	Description															
<i>phase1</i>	Enable/disable copying the DSCP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable copy the DSCP in the ESP header to the inner IP Header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable copy the DSCP in the ESP header to the inner IP Header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable copy the DSCP in the ESP header to the inner IP Header.	<i>disable</i>	Disable copy the DSCP in the ESP header to the inner IP Header.					
Option	Description											
<i>enable</i>	Enable copy the DSCP in the ESP header to the inner IP Header.											
<i>disable</i>	Disable copy the DSCP in the ESP header to the inner IP Header.											
keylifeseconds	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800	43200								
keylifekbs	Phase2 key life in number of kilobytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295	5120								
keylife-type	Keylife type.	option	-	seconds								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>seconds</i></td> <td>Key life in seconds.</td> </tr> <tr> <td><i>kbs</i></td> <td>Key life in kilobytes.</td> </tr> <tr> <td><i>both</i></td> <td>Key life both.</td> </tr> </tbody> </table>	Option	Description	<i>seconds</i>	Key life in seconds.	<i>kbs</i>	Key life in kilobytes.	<i>both</i>	Key life both.			
Option	Description											
<i>seconds</i>	Key life in seconds.											
<i>kbs</i>	Key life in kilobytes.											
<i>both</i>	Key life both.											
single-source	Enable/disable single source IP restriction.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Only single source IP will be accepted.</td> </tr> <tr> <td><i>disable</i></td> <td>Source IP range will be accepted.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Only single source IP will be accepted.	<i>disable</i>	Source IP range will be accepted.					
Option	Description											
<i>enable</i>	Only single source IP will be accepted.											
<i>disable</i>	Source IP range will be accepted.											
route-overlap	Action for overlapping routes.	option	-	use-new								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>use-old</i></td> <td>Use the old route and do not add the new route.</td> </tr> <tr> <td><i>use-new</i></td> <td>Delete the old route and add the new route.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow overlapping routes.</td> </tr> </tbody> </table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.	<i>use-new</i>	Delete the old route and add the new route.	<i>allow</i>	Allow overlapping routes.			
Option	Description											
<i>use-old</i>	Use the old route and do not add the new route.											
<i>use-new</i>	Delete the old route and add the new route.											
<i>allow</i>	Allow overlapping routes.											
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel-mode</i></td> <td>Use tunnel mode encapsulation.</td> </tr> <tr> <td><i>transport-mode</i></td> <td>Use transport mode encapsulation.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel-mode</i>	Use tunnel mode encapsulation.	<i>transport-mode</i>	Use transport mode encapsulation.					
Option	Description											
<i>tunnel-mode</i>	Use tunnel mode encapsulation.											
<i>transport-mode</i>	Use transport mode encapsulation.											

Parameter	Description	Type	Size	Default										
l2tp	Enable/disable L2TP over IPsec.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable L2TP over IPsec.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable L2TP over IPsec.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable L2TP over IPsec.	<i>disable</i>	Disable L2TP over IPsec.							
Option	Description													
<i>enable</i>	Enable L2TP over IPsec.													
<i>disable</i>	Disable L2TP over IPsec.													
comments	Comment.	var-string	Maximum length: 255											
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified											
protocol	Quick mode protocol selector .	integer	Minimum value: 0 Maximum value: 255	0										
src-name	Local proxy ID name.	string	Maximum length: 79											
src-name6	Local proxy ID name.	string	Maximum length: 79											
src-addr-type	Local proxy ID type.	option	-	subnet										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subnet</i></td> <td>IPv4 subnet.</td> </tr> <tr> <td><i>range</i></td> <td>IPv4 range.</td> </tr> <tr> <td><i>ip</i></td> <td>IPv4 IP.</td> </tr> <tr> <td><i>name</i></td> <td>IPv4 firewall address or group name.</td> </tr> </tbody> </table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.			
Option	Description													
<i>subnet</i>	IPv4 subnet.													
<i>range</i>	IPv4 range.													
<i>ip</i>	IPv4 IP.													
<i>name</i>	IPv4 firewall address or group name.													



Parameter	Description	Type	Size	Default										
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0										
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::										
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0										
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::										
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0										
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0										
src-port	Quick mode source port .	integer	Minimum value: 0 Maximum value: 65535	0										
dst-name	Remote proxy ID name.	string	Maximum length: 79											
dst-name6	Remote proxy ID name.	string	Maximum length: 79											
dst-addr-type	Remote proxy ID type.	option	-	subnet										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subnet</i></td> <td>IPv4 subnet.</td> </tr> <tr> <td><i>range</i></td> <td>IPv4 range.</td> </tr> <tr> <td><i>ip</i></td> <td>IPv4 IP.</td> </tr> <tr> <td><i>name</i></td> <td>IPv4 firewall address or group name.</td> </tr> </tbody> </table>		Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.		
Option	Description													
<i>subnet</i>	IPv4 subnet.													
<i>range</i>	IPv4 range.													
<i>ip</i>	IPv4 IP.													
<i>name</i>	IPv4 firewall address or group name.													
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0										
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::										
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0										
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::										
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0										

Parameter	Description	Type	Size	Default
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
dst-port	Quick mode destination port .	integer	Minimum value: 0 Maximum value: 65535	0

## config vpn ipsec manualkey

Configure IPsec manual keys.

```

config vpn ipsec manualkey
  Description: Configure IPsec manual keys.
  edit <name>
    set interface {string}
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address-any}
    set authentication [null|md5|...]
    set encryption [null|des|...]
    set authkey {user}
    set enckey {user}
    set localspi {user}
    set remotespi {user}
    set npu-offload [enable|disable]
  next
end

```

## config vpn ipsec manualkey

Parameter	Description	Type	Size	Default
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15	
remote-gw	Peer gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	Local gateway.	ipv4-address-any	Not Specified	0.0.0.0
authentication	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null
	<b>Option</b>	<b>Description</b>		
	<i>null</i>	Null.		
	<i>md5</i>	MD5.		

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha1</i></td> <td>SHA1.</td> </tr> <tr> <td><i>sha256</i></td> <td>SHA256.</td> </tr> <tr> <td><i>sha384</i></td> <td>SHA384.</td> </tr> <tr> <td><i>sha512</i></td> <td>SHA512.</td> </tr> </tbody> </table>	Option	Description	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.															
Option	Description																									
<i>sha1</i>	SHA1.																									
<i>sha256</i>	SHA256.																									
<i>sha384</i>	SHA384.																									
<i>sha512</i>	SHA512.																									
encryption	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null</i></td> <td>Null.</td> </tr> <tr> <td><i>des</i></td> <td>DES.</td> </tr> <tr> <td><i>3des</i></td> <td>3DES.</td> </tr> <tr> <td><i>aes128</i></td> <td>AES128.</td> </tr> <tr> <td><i>aes192</i></td> <td>AES192.</td> </tr> <tr> <td><i>aes256</i></td> <td>AES256.</td> </tr> <tr> <td><i>aria128</i></td> <td>ARIA128.</td> </tr> <tr> <td><i>aria192</i></td> <td>ARIA192.</td> </tr> <tr> <td><i>aria256</i></td> <td>ARIA256.</td> </tr> <tr> <td><i>seed</i></td> <td>Seed.</td> </tr> </tbody> </table>	Option	Description	<i>null</i>	Null.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.	<i>aria128</i>	ARIA128.	<i>aria192</i>	ARIA192.	<i>aria256</i>	ARIA256.	<i>seed</i>	Seed.			
Option	Description																									
<i>null</i>	Null.																									
<i>des</i>	DES.																									
<i>3des</i>	3DES.																									
<i>aes128</i>	AES128.																									
<i>aes192</i>	AES192.																									
<i>aes256</i>	AES256.																									
<i>aria128</i>	ARIA128.																									
<i>aria192</i>	ARIA192.																									
<i>aria256</i>	ARIA256.																									
<i>seed</i>	Seed.																									
authkey	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user		Not Specified																						
enckey	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user		Not Specified																						
localspi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user		Not Specified																						
remotespi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user		Not Specified																						
npu-offload *	Enable/disable NPU offloading.	option	-	enable																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NPU offloading.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NPU offloading.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.																			
Option	Description																									
<i>enable</i>	Enable NPU offloading.																									
<i>disable</i>	Disable NPU offloading.																									

\* This parameter may not exist in some models.

## config vpn ipsec concentrator

Concentrator configuration.

```
config vpn ipsec concentrator
  Description: Concentrator configuration.
  edit <name>
    set src-check [disable|enable]
    set member <name1>, <name2>, ...
  next
end
```

## config vpn ipsec concentrator

Parameter	Description	Type	Size	Default						
src-check	Enable to check source address of phase 2 selector. Disable to check only the destination selector.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Ignore source selector when choosing tunnel.</td></tr><tr><td><i>enable</i></td><td>Use source selector to choose tunnel.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Ignore source selector when choosing tunnel.	<i>enable</i>	Use source selector to choose tunnel.			
Option	Description									
<i>disable</i>	Ignore source selector when choosing tunnel.									
<i>enable</i>	Use source selector to choose tunnel.									
member <name>	Names of up to 3 VPN tunnels to add to the concentrator. Member name.	string	Maximum length: 79							

## config vpn ipsec phase1-interface

Configure VPN remote gateway.

```
config vpn ipsec phase1-interface
  Description: Configure VPN remote gateway.
  edit <name>
    set type [static|dynamic|...]
    set interface {string}
    set ip-version [4|6]
    set ike-version [1|2]
    set local-gw {ipv4-address}
    set local-gw6 {ipv6-address}
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set remotegw-ddns {string}
    set keylife {integer}
    set certificate <name1>, <name2>, ...
    set authmethod [psk|signature]
    set authmethod-remote [psk|signature]
    set mode [aggressive|main]
    set peertype [any|one|...]
    set peerid {string}
    set default-gw {ipv4-address}
    set default-gw-priority {integer}
```

```

set usrgrp {string}
set peer {string}
set peergrp {string}
set monitor {string}
set monitor-hold-down-type [immediate|delay|...]
set monitor-hold-down-delay {integer}
set monitor-hold-down-weekday [everyday|sunday|...]
set monitor-hold-down-time {user}
set net-device [enable|disable]
set tunnel-search [selectors|nexthop]
set passive-mode [enable|disable]
set exchange-interface-ip [enable|disable]
set exchange-ip-addr4 {ipv4-address}
set exchange-ip-addr6 {ipv6-address}
set aggregate-member [enable|disable]
set aggregate-weight {integer}
set mode-cfg [disable|enable]
set assign-ip [disable|enable]
set assign-ip-from [range|usrgrp|...]
set ipv4-start-ip {ipv4-address}
set ipv4-end-ip {ipv4-address}
set ipv4-netmask {ipv4-netmask}
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dns-mode [manual|auto]
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
set ipv4-split-include {string}
set split-include-service {string}
set ipv4-name {string}
set ipv6-start-ip {ipv6-address}
set ipv6-end-ip {ipv6-address}
set ipv6-prefix {integer}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set ipv6-split-include {string}
set ipv6-name {string}
set unity-support [disable|enable]
set domain {string}

```

---

```
set banner {var-string}
set include-local-lan [disable|enable]
set ipv4-split-exclude {string}
set ipv6-split-exclude {string}
set save-password [disable|enable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set backup-gateway <address1>, <address2>, ...
set proposal {option1}, {option2}, ...
set add-route [disable|enable]
set add-gw-route [enable|disable]
set psksecret {password-3}
set psksecret-remote {password-3}
set keepalive {integer}
set distance {integer}
set priority {integer}
set localid {string}
set localid-type [auto|fqdn|...]
set auto-negotiate [enable|disable]
set negotiate-timeout {integer}
set fragmentation [enable|disable]
set ip-fragmentation [pre-encapsulation|post-encapsulation]
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set forticlient-enforcement [enable|disable]
set comments {var-string}
set npu-offload [enable|disable]
set send-cert-chain [enable|disable]
set dhgrp {option1}, {option2}, ...
set suite-b [disable|suite-b-gcm-128|...]
set eap [enable|disable]
set eap-identity [use-id-payload|send-request]
set eap-exclude-peergrp {string}
set acct-verify [enable|disable]
set ppk [disable|allow|...]
set ppk-secret {password-3}
set ppk-identity {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
set reauth [disable|enable]
set authusr {string}
set authpasswd {password}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set authusrgrp {string}
set mesh-selector-type [disable|subnet|...]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ha-sync-esp-seqno [enable|disable]
set inbound-dscp-copy [enable|disable]
set auto-discovery-sender [enable|disable]
set auto-discovery-receiver [enable|disable]
set auto-discovery-forwarder [enable|disable]
set auto-discovery-psk [enable|disable]
set auto-discovery-shortcuts [independent|dependent]
set encapsulation [none|gre|...]
```

```

set encapsulation-address [ike|ipv4|...]
set encap-local-gw4 {ipv4-address}
set encap-local-gw6 {ipv6-address}
set encap-remote-gw4 {ipv4-address}
set encap-remote-gw6 {ipv6-address}
set vni {integer}
set nattraversal [enable|disable|...]
set fragmentation-mtu {integer}
set childless-ike [enable|disable]
set rekey [enable|disable]
set digital-signature-auth [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set rsa-signature-format [pkcs1|pss]
set enforce-unique-id [disable|keep-new|...]
set cert-id-validation [enable|disable]
set fec-egress [enable|disable]
set fec-send-timeout {integer}
set fec-base {integer}
set fec-codec {integer}
set fec-redundant {integer}
set fec-ingress [enable|disable]
set fec-receive-timeout {integer}
set network-overlay [disable|enable]
set network-id {integer}
next
end

```

## config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default								
type	Remote gateway type.	option	-	static								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Remote VPN gateway has fixed IP address.</td> </tr> <tr> <td><i>dynamic</i></td> <td>Remote VPN gateway has dynamic IP address.</td> </tr> <tr> <td><i>ddns</i></td> <td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Remote VPN gateway has fixed IP address.	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.			
Option	Description											
<i>static</i>	Remote VPN gateway has fixed IP address.											
<i>dynamic</i>	Remote VPN gateway has dynamic IP address.											
<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.											
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35									
ip-version	IP version to use for VPN interface.	option	-	4								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Use IPv4 addressing for gateways.</td> </tr> <tr> <td>6</td> <td>Use IPv6 addressing for gateways.</td> </tr> </tbody> </table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.					
Option	Description											
4	Use IPv4 addressing for gateways.											
6	Use IPv6 addressing for gateways.											
ike-version	IKE protocol version.	option	-	1								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Use IKEv1 protocol.</td> </tr> <tr> <td>2</td> <td>Use IKEv2 protocol.</td> </tr> </tbody> </table>	Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.			
Option	Description									
1	Use IKEv1 protocol.									
2	Use IKEv2 protocol.									
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
local-gw6	IPv6 address of the local gateway's external interface.	ipv6-address	Not Specified	::						
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
remote-gw6	IPv6 address of the remote gateway's external interface.	ipv6-address	Not Specified	::						
remotegw-ddns	Domain name of remote gateway (eg. name.DDNS.com).	string	Maximum length: 63							
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400						
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79							
authmethod	Authentication method.	option	-	psk						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>psk</i></td> <td>PSK authentication method.</td> </tr> <tr> <td><i>signature</i></td> <td>Signature authentication method.</td> </tr> </tbody> </table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.			
Option	Description									
<i>psk</i>	PSK authentication method.									
<i>signature</i>	Signature authentication method.									
authmethod-remote	Authentication method (remote side).	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>psk</i></td> <td>PSK authentication method.</td> </tr> <tr> <td><i>signature</i></td> <td>Signature authentication method.</td> </tr> </tbody> </table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.			
Option	Description									
<i>psk</i>	PSK authentication method.									
<i>signature</i>	Signature authentication method.									
mode	The ID protection mode used to establish a secure channel.	option	-	main						



Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aggressive</i></td> <td>Aggressive mode.</td> </tr> <tr> <td><i>main</i></td> <td>Main mode.</td> </tr> </tbody> </table>	Option	Description	<i>aggressive</i>	Aggressive mode.	<i>main</i>	Main mode.									
Option	Description															
<i>aggressive</i>	Aggressive mode.															
<i>main</i>	Main mode.															
peertype	Accept this peer type.	option	-	peer												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>any</i></td> <td>Accept any peer ID.</td> </tr> <tr> <td><i>one</i></td> <td>Accept this peer ID.</td> </tr> <tr> <td><i>dialup</i></td> <td>Accept peer ID in dialup group.</td> </tr> <tr> <td><i>peer</i></td> <td>Accept this peer certificate.</td> </tr> <tr> <td><i>peergrp</i></td> <td>Accept this peer certificate group.</td> </tr> </tbody> </table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.			
Option	Description															
<i>any</i>	Accept any peer ID.															
<i>one</i>	Accept this peer ID.															
<i>dialup</i>	Accept peer ID in dialup group.															
<i>peer</i>	Accept this peer certificate.															
<i>peergrp</i>	Accept this peer certificate group.															
peerid	Accept this peer identity.	string	Maximum length: 255													
default-gw	IPv4 address of default route gateway to use for traffic exiting the interface.	ipv4-address	Not Specified	0.0.0.0												
default-gw-priority	Priority for default gateway route. A higher priority number signifies a less preferred route.	integer	Minimum value: 0 Maximum value: 4294967295	0												
usrgrp	User group name for dialup peers.	string	Maximum length: 35													
peer	Accept this peer certificate.	string	Maximum length: 35													
peergrp	Accept this peer certificate group.	string	Maximum length: 35													
monitor	IPsec interface as backup for primary interface.	string	Maximum length: 35													
monitor-hold-down-type	Recovery time method when primary interface re-establishes.	option	-	immediate												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>immediate</i></td> <td>Fail back immediately after primary recovers.</td> </tr> <tr> <td><i>delay</i></td> <td>Number of seconds to delay fail back after primary recovers.</td> </tr> <tr> <td><i>time</i></td> <td>Specify a time at which to fail back after primary recovers.</td> </tr> </tbody> </table>	Option	Description	<i>immediate</i>	Fail back immediately after primary recovers.	<i>delay</i>	Number of seconds to delay fail back after primary recovers.	<i>time</i>	Specify a time at which to fail back after primary recovers.							
Option	Description															
<i>immediate</i>	Fail back immediately after primary recovers.															
<i>delay</i>	Number of seconds to delay fail back after primary recovers.															
<i>time</i>	Specify a time at which to fail back after primary recovers.															

Parameter	Description	Type	Size	Default																		
monitor-hold-down-delay	Time to wait in seconds before recovery once primary re-establishes.	integer	Minimum value: 0 Maximum value: 31536000	0																		
monitor-hold-down-weekday	Day of the week to recover once primary re-establishes.	option	-	sunday																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>everyday</i></td> <td>Every Day.</td> </tr> <tr> <td><i>sunday</i></td> <td>Sunday.</td> </tr> <tr> <td><i>monday</i></td> <td>Monday.</td> </tr> <tr> <td><i>tuesday</i></td> <td>Tuesday.</td> </tr> <tr> <td><i>wednesday</i></td> <td>Wednesday.</td> </tr> <tr> <td><i>thursday</i></td> <td>Thursday.</td> </tr> <tr> <td><i>friday</i></td> <td>Friday.</td> </tr> <tr> <td><i>saturday</i></td> <td>Saturday.</td> </tr> </tbody> </table>	Option	Description	<i>everyday</i>	Every Day.	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.			
Option	Description																					
<i>everyday</i>	Every Day.																					
<i>sunday</i>	Sunday.																					
<i>monday</i>	Monday.																					
<i>tuesday</i>	Tuesday.																					
<i>wednesday</i>	Wednesday.																					
<i>thursday</i>	Thursday.																					
<i>friday</i>	Friday.																					
<i>saturday</i>	Saturday.																					
monitor-hold-down-time	Time of day at which to fail back to primary after it re-establishes.	user	Not Specified																			
net-device	Enable/disable kernel device creation.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Create a kernel device for every tunnel.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not create a kernel device for tunnels.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Create a kernel device for every tunnel.	<i>disable</i>	Do not create a kernel device for tunnels.															
Option	Description																					
<i>enable</i>	Create a kernel device for every tunnel.																					
<i>disable</i>	Do not create a kernel device for tunnels.																					
tunnel-search	Tunnel search method for when the interface is shared.	option	-	selectors																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>selectors</i></td> <td>Search for tunnel in selectors.</td> </tr> <tr> <td><i>nexthop</i></td> <td>Search for tunnel using nexthop.</td> </tr> </tbody> </table>	Option	Description	<i>selectors</i>	Search for tunnel in selectors.	<i>nexthop</i>	Search for tunnel using nexthop.															
Option	Description																					
<i>selectors</i>	Search for tunnel in selectors.																					
<i>nexthop</i>	Search for tunnel using nexthop.																					
passive-mode	Enable/disable IPsec passive mode for static tunnels.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec passive mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec passive mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec passive mode.	<i>disable</i>	Disable IPsec passive mode.															
Option	Description																					
<i>enable</i>	Enable IPsec passive mode.																					
<i>disable</i>	Disable IPsec passive mode.																					

Parameter	Description	Type	Size	Default						
exchange-interface-ip	Enable/disable exchange of IPsec interface IP address.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable exchange of IPsec interface IP address.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable exchange of IPsec interface IP address.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable exchange of IPsec interface IP address.	<i>disable</i>	Disable exchange of IPsec interface IP address.			
Option	Description									
<i>enable</i>	Enable exchange of IPsec interface IP address.									
<i>disable</i>	Disable exchange of IPsec interface IP address.									
exchange-ip-addr4	IPv4 address to exchange with peers.	ipv4-address	Not Specified	0.0.0.0						
exchange-ip-addr6	IPv6 address to exchange with peers	ipv6-address	Not Specified	::						
aggregate-member	Enable/disable use as an aggregate member.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use as an aggregate member.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use as an aggregate member.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use as an aggregate member.	<i>disable</i>	Disable use as an aggregate member.			
Option	Description									
<i>enable</i>	Enable use as an aggregate member.									
<i>disable</i>	Disable use as an aggregate member.									
aggregate-weight	Link weight for aggregate.	integer	Minimum value: 1 Maximum value: 100	1						
mode-cfg	Enable/disable configuration method.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Configuration Method.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Configuration Method.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Configuration Method.	<i>enable</i>	Enable Configuration Method.			
Option	Description									
<i>disable</i>	Disable Configuration Method.									
<i>enable</i>	Enable Configuration Method.									
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not assign an IP address to the IPsec interface.</td> </tr> <tr> <td><i>enable</i></td> <td>Assign an IP address to the IPsec interface.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not assign an IP address to the IPsec interface.	<i>enable</i>	Assign an IP address to the IPsec interface.			
Option	Description									
<i>disable</i>	Do not assign an IP address to the IPsec interface.									
<i>enable</i>	Assign an IP address to the IPsec interface.									
assign-ip-from	Method by which the IP address will be assigned.	option	-	range						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>range</i></td> <td>Assign IP address from locally defined range.</td> </tr> </tbody> </table>	Option	Description	<i>range</i>	Assign IP address from locally defined range.					
Option	Description									
<i>range</i>	Assign IP address from locally defined range.									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>usrgrp</i></td> <td>Assign IP address via user group.</td> </tr> <tr> <td><i>dhcp</i></td> <td>Assign IP address via DHCP.</td> </tr> <tr> <td><i>name</i></td> <td>Assign IP address from firewall address or group.</td> </tr> </tbody> </table>	Option	Description	<i>usrgrp</i>	Assign IP address via user group.	<i>dhcp</i>	Assign IP address via DHCP.	<i>name</i>	Assign IP address from firewall address or group.			
Option	Description											
<i>usrgrp</i>	Assign IP address via user group.											
<i>dhcp</i>	Assign IP address via DHCP.											
<i>name</i>	Assign IP address from firewall address or group.											
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0								
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0								
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255								
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0								
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::								
dns-mode	DNS server mode.	option	-	manual								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>manual</i></td> <td>Manually configure DNS servers.</td> </tr> <tr> <td><i>auto</i></td> <td>Use default DNS servers.</td> </tr> </tbody> </table>	Option	Description	<i>manual</i>	Manually configure DNS servers.	<i>auto</i>	Use default DNS servers.					
Option	Description											
<i>manual</i>	Manually configure DNS servers.											
<i>auto</i>	Use default DNS servers.											
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0								
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0								
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0								
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0								
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0								
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79									
split-include-service	Split-include services.	string	Maximum length: 79									
ipv4-name	IPv4 address name.	string	Maximum length: 79									
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::								
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::								

Parameter	Description	Type	Size	Default						
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128						
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::						
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79							
ipv6-name	IPv6 address name.	string	Maximum length: 79							
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Cisco Unity Configuration Method Extensions.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Cisco Unity Configuration Method Extensions.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.	<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.			
Option	Description									
<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.									
<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.									
domain	Instruct unity clients about the default DNS domain.	string	Maximum length: 63							
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024							
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable local LAN access on Unity clients.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable local LAN access on Unity clients.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable local LAN access on Unity clients.	<i>enable</i>	Enable local LAN access on Unity clients.			
Option	Description									
<i>disable</i>	Disable local LAN access on Unity clients.									
<i>enable</i>	Enable local LAN access on Unity clients.									
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable saving XAuth username and password on VPN clients.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable saving XAuth username and password on VPN clients.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable saving XAuth username and password on VPN clients.	<i>enable</i>	Enable saving XAuth username and password on VPN clients.			
Option	Description									
<i>disable</i>	Disable saving XAuth username and password on VPN clients.									
<i>enable</i>	Enable saving XAuth username and password on VPN clients.									

Parameter	Description	Type	Size	Default																								
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable allowing the VPN client to bring up the tunnel when there is no traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable allowing the VPN client to bring up the tunnel when there is no traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.																					
Option	Description																											
<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.																											
<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.																											
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable allowing the VPN client to keep the tunnel up when there is no traffic.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable allowing the VPN client to keep the tunnel up when there is no traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.																					
Option	Description																											
<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.																											
<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.																											
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79																									
proposal	Phase1 proposal.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>des-md5</i></td> <td>des-md5</td> </tr> <tr> <td><i>des-sha1</i></td> <td>des-sha1</td> </tr> <tr> <td><i>des-sha256</i></td> <td>des-sha256</td> </tr> <tr> <td><i>des-sha384</i></td> <td>des-sha384</td> </tr> <tr> <td><i>des-sha512</i></td> <td>des-sha512</td> </tr> <tr> <td><i>3des-md5</i></td> <td>3des-md5</td> </tr> <tr> <td><i>3des-sha1</i></td> <td>3des-sha1</td> </tr> <tr> <td><i>3des-sha256</i></td> <td>3des-sha256</td> </tr> <tr> <td><i>3des-sha384</i></td> <td>3des-sha384</td> </tr> <tr> <td><i>3des-sha512</i></td> <td>3des-sha512</td> </tr> <tr> <td><i>aes128-md5</i></td> <td>aes128-md5</td> </tr> </tbody> </table>	Option	Description	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384	<i>3des-sha512</i>	3des-sha512	<i>aes128-md5</i>	aes128-md5			
Option	Description																											
<i>des-md5</i>	des-md5																											
<i>des-sha1</i>	des-sha1																											
<i>des-sha256</i>	des-sha256																											
<i>des-sha384</i>	des-sha384																											
<i>des-sha512</i>	des-sha512																											
<i>3des-md5</i>	3des-md5																											
<i>3des-sha1</i>	3des-sha1																											
<i>3des-sha256</i>	3des-sha256																											
<i>3des-sha384</i>	3des-sha384																											
<i>3des-sha512</i>	3des-sha512																											
<i>aes128-md5</i>	aes128-md5																											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1		
	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256		
	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384		
	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1		
	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256		
	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1		
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256		
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384		
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aria128-sha384</i></td> <td>aria128-sha384</td> </tr> <tr> <td><i>aria128-sha512</i></td> <td>aria128-sha512</td> </tr> <tr> <td><i>aria192-md5</i></td> <td>aria192-md5</td> </tr> <tr> <td><i>aria192-sha1</i></td> <td>aria192-sha1</td> </tr> <tr> <td><i>aria192-sha256</i></td> <td>aria192-sha256</td> </tr> <tr> <td><i>aria192-sha384</i></td> <td>aria192-sha384</td> </tr> <tr> <td><i>aria192-sha512</i></td> <td>aria192-sha512</td> </tr> <tr> <td><i>aria256-md5</i></td> <td>aria256-md5</td> </tr> <tr> <td><i>aria256-sha1</i></td> <td>aria256-sha1</td> </tr> <tr> <td><i>aria256-sha256</i></td> <td>aria256-sha256</td> </tr> <tr> <td><i>aria256-sha384</i></td> <td>aria256-sha384</td> </tr> <tr> <td><i>aria256-sha512</i></td> <td>aria256-sha512</td> </tr> <tr> <td><i>seed-md5</i></td> <td>seed-md5</td> </tr> <tr> <td><i>seed-sha1</i></td> <td>seed-sha1</td> </tr> <tr> <td><i>seed-sha256</i></td> <td>seed-sha256</td> </tr> <tr> <td><i>seed-sha384</i></td> <td>seed-sha384</td> </tr> <tr> <td><i>seed-sha512</i></td> <td>seed-sha512</td> </tr> </tbody> </table>	Option	Description	<i>aria128-sha384</i>	aria128-sha384	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
Option	Description																																							
<i>aria128-sha384</i>	aria128-sha384																																							
<i>aria128-sha512</i>	aria128-sha512																																							
<i>aria192-md5</i>	aria192-md5																																							
<i>aria192-sha1</i>	aria192-sha1																																							
<i>aria192-sha256</i>	aria192-sha256																																							
<i>aria192-sha384</i>	aria192-sha384																																							
<i>aria192-sha512</i>	aria192-sha512																																							
<i>aria256-md5</i>	aria256-md5																																							
<i>aria256-sha1</i>	aria256-sha1																																							
<i>aria256-sha256</i>	aria256-sha256																																							
<i>aria256-sha384</i>	aria256-sha384																																							
<i>aria256-sha512</i>	aria256-sha512																																							
<i>seed-md5</i>	seed-md5																																							
<i>seed-sha1</i>	seed-sha1																																							
<i>seed-sha256</i>	seed-sha256																																							
<i>seed-sha384</i>	seed-sha384																																							
<i>seed-sha512</i>	seed-sha512																																							
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	enable																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not add a route to destination of peer selector.</td> </tr> <tr> <td><i>enable</i></td> <td>Add route to destination of peer selector.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not add a route to destination of peer selector.	<i>enable</i>	Add route to destination of peer selector.																																	
Option	Description																																							
<i>disable</i>	Do not add a route to destination of peer selector.																																							
<i>enable</i>	Add route to destination of peer selector.																																							
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Automatically add a route to the remote gateway.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not automatically add a route to the remote gateway.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Automatically add a route to the remote gateway.	<i>disable</i>	Do not automatically add a route to the remote gateway.																																	
Option	Description																																							
<i>enable</i>	Automatically add a route to the remote gateway.																																							
<i>disable</i>	Do not automatically add a route to the remote gateway.																																							



Parameter	Description	Type	Size	Default														
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified															
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified															
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10														
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255	15														
priority	Priority for routes added by IKE .	integer	Minimum value: 0 Maximum value: 4294967295	0														
localid	Local ID.	string	Maximum length: 63															
localid-type	Local ID type.	option	-	auto														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Select ID type automatically.</td> </tr> <tr> <td><i>fqdn</i></td> <td>Use fully qualified domain name.</td> </tr> <tr> <td><i>user-fqdn</i></td> <td>Use user fully qualified domain name.</td> </tr> <tr> <td><i>keyid</i></td> <td>Use key-id string.</td> </tr> <tr> <td><i>address</i></td> <td>Use local IP address.</td> </tr> <tr> <td><i>asn1dn</i></td> <td>Use ASN.1 distinguished name.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Select ID type automatically.	<i>fqdn</i>	Use fully qualified domain name.	<i>user-fqdn</i>	Use user fully qualified domain name.	<i>keyid</i>	Use key-id string.	<i>address</i>	Use local IP address.	<i>asn1dn</i>	Use ASN.1 distinguished name.			
Option	Description																	
<i>auto</i>	Select ID type automatically.																	
<i>fqdn</i>	Use fully qualified domain name.																	
<i>user-fqdn</i>	Use user fully qualified domain name.																	
<i>keyid</i>	Use key-id string.																	
<i>address</i>	Use local IP address.																	
<i>asn1dn</i>	Use ASN.1 distinguished name.																	
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic initiation of IKE SA negotiation.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic initiation of IKE SA negotiation.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.											
Option	Description																	
<i>enable</i>	Enable automatic initiation of IKE SA negotiation.																	
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.																	

Parameter	Description	Type	Size	Default								
negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300	30								
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable intra-IKE fragmentation support on re-transmission.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable intra-IKE fragmentation support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.					
Option	Description											
<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.											
<i>disable</i>	Disable intra-IKE fragmentation support.											
ip-fragmentation	Determine whether IP packets are fragmented before or after IPsec encapsulation.	option	-	post-encapsulation								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pre-encapsulation</i></td> <td>Fragment before IPsec encapsulation.</td> </tr> <tr> <td><i>post-encapsulation</i></td> <td>Fragment after IPsec encapsulation (RFC compliant).</td> </tr> </tbody> </table>	Option	Description	<i>pre-encapsulation</i>	Fragment before IPsec encapsulation.	<i>post-encapsulation</i>	Fragment after IPsec encapsulation (RFC compliant).					
Option	Description											
<i>pre-encapsulation</i>	Fragment before IPsec encapsulation.											
<i>post-encapsulation</i>	Fragment after IPsec encapsulation (RFC compliant).											
dpd	Dead Peer Detection mode.	option	-	on-demand								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Dead Peer Detection.</td> </tr> <tr> <td><i>on-idle</i></td> <td>Trigger Dead Peer Detection when IPsec is idle.</td> </tr> <tr> <td><i>on-demand</i></td> <td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Dead Peer Detection.	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.			
Option	Description											
<i>disable</i>	Disable Dead Peer Detection.											
<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.											
<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.											
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3								
dpd-retryinterval	DPD retry interval.	user	Not Specified									
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiClient enforcement.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiClient enforcement.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiClient enforcement.	<i>disable</i>	Disable FortiClient enforcement.					
Option	Description											
<i>enable</i>	Enable FortiClient enforcement.											
<i>disable</i>	Disable FortiClient enforcement.											

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
npu-offload *	Enable/disable offloading NPU.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sending certificate chain.		
	<i>disable</i>	Disable sending certificate chain.		
dhgrp	DH group.	option	-	14
	<b>Option</b>	<b>Description</b>		
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		
	14	DH Group 14.		
	15	DH Group 15.		
	16	DH Group 16.		
	17	DH Group 17.		
	18	DH Group 18.		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
	27	DH Group 27.		
	28	DH Group 28.		
	29	DH Group 29.		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		

Parameter	Description	Type	Size	Default								
suite-b	Use Suite-B.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Do not use UI suite.</td> </tr> <tr> <td><i>suite-b-gcm-128</i></td> <td>Use Suite-B-GCM-128.</td> </tr> <tr> <td><i>suite-b-gcm-256</i></td> <td>Use Suite-B-GCM-256.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not use UI suite.	<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.	<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.			
Option	Description											
<i>disable</i>	Do not use UI suite.											
<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.											
<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.											
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 EAP authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKEv2 EAP authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.					
Option	Description											
<i>enable</i>	Enable IKEv2 EAP authentication.											
<i>disable</i>	Disable IKEv2 EAP authentication.											
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>use-id-payload</i></td> <td>Use IKEv2 IDi payload to resolve peer identity.</td> </tr> <tr> <td><i>send-request</i></td> <td>Use EAP identity request to resolve peer identity.</td> </tr> </tbody> </table>	Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.					
Option	Description											
<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.											
<i>send-request</i>	Use EAP identity request to resolve peer identity.											
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35									
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable verification of RADIUS accounting record.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable verification of RADIUS accounting record.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable verification of RADIUS accounting record.	<i>disable</i>	Disable verification of RADIUS accounting record.					
Option	Description											
<i>enable</i>	Enable verification of RADIUS accounting record.											
<i>disable</i>	Disable verification of RADIUS accounting record.											
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td> </tr> <tr> <td><i>allow</i></td> <td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td> </tr> <tr> <td><i>require</i></td> <td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).			
Option	Description											
<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).											
<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).											
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).											
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified									

Parameter	Description	Type	Size	Default																												
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35																													
wizard-type	GUI VPN Wizard Type.	option	-	custom																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>custom</i></td> <td>Custom VPN configuration.</td> </tr> <tr> <td><i>dialup-forticlient</i></td> <td>Dial Up - FortiClient Windows, Mac and Android.</td> </tr> <tr> <td><i>dialup-ios</i></td> <td>Dial Up - iPhone / iPad Native IPsec Client.</td> </tr> <tr> <td><i>dialup-android</i></td> <td>Dial Up - Android Native IPsec Client.</td> </tr> <tr> <td><i>dialup-windows</i></td> <td>Dial Up - Windows Native IPsec Client.</td> </tr> <tr> <td><i>dialup-cisco</i></td> <td>Dial Up - Cisco IPsec Client.</td> </tr> <tr> <td><i>static-fortigate</i></td> <td>Site to Site - FortiGate.</td> </tr> <tr> <td><i>dialup-fortigate</i></td> <td>Dial Up - FortiGate.</td> </tr> <tr> <td><i>static-cisco</i></td> <td>Site to Site - Cisco.</td> </tr> <tr> <td><i>dialup-cisco-fw</i></td> <td>Dialup Up - Cisco Firewall.</td> </tr> <tr> <td><i>simplified-static-fortigate</i></td> <td>Site to Site - FortiGate (SD-WAN).</td> </tr> <tr> <td><i>hub-fortigate-auto-discovery</i></td> <td>Hub role in a Hub-and-Spoke auto-discovery VPN.</td> </tr> <tr> <td><i>spoke-fortigate-auto-discovery</i></td> <td>Spoke role in a Hub-and-Spoke auto-discovery VPN.</td> </tr> </tbody> </table>	Option	Description	<i>custom</i>	Custom VPN configuration.	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	<i>static-fortigate</i>	Site to Site - FortiGate.	<i>dialup-fortigate</i>	Dial Up - FortiGate.	<i>static-cisco</i>	Site to Site - Cisco.	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.			
Option	Description																															
<i>custom</i>	Custom VPN configuration.																															
<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.																															
<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.																															
<i>dialup-android</i>	Dial Up - Android Native IPsec Client.																															
<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.																															
<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.																															
<i>static-fortigate</i>	Site to Site - FortiGate.																															
<i>dialup-fortigate</i>	Dial Up - FortiGate.																															
<i>static-cisco</i>	Site to Site - Cisco.																															
<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.																															
<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).																															
<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.																															
<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.																															
xauthtype	XAuth type.	option	-	disable																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>client</i></td> <td>Enable as client.</td> </tr> <tr> <td><i>pap</i></td> <td>Enable as server PAP.</td> </tr> <tr> <td><i>chap</i></td> <td>Enable as server CHAP.</td> </tr> <tr> <td><i>auto</i></td> <td>Enable as server auto.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>client</i>	Enable as client.	<i>pap</i>	Enable as server PAP.	<i>chap</i>	Enable as server CHAP.	<i>auto</i>	Enable as server auto.																			
Option	Description																															
<i>disable</i>	Disable.																															
<i>client</i>	Enable as client.																															
<i>pap</i>	Enable as server PAP.																															
<i>chap</i>	Enable as server CHAP.																															
<i>auto</i>	Enable as server auto.																															
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable																												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable IKE SA re-authentication.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable IKE SA re-authentication.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.					
Option	Description											
<i>disable</i>	Disable IKE SA re-authentication.											
<i>enable</i>	Enable IKE SA re-authentication.											
authusr	XAuth user name.	string	Maximum length: 64									
authpasswd	XAuth password (max 35 characters).	password	Not Specified									
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 IDi group authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKEv2 IDi group authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 IDi group authentication.	<i>disable</i>	Disable IKEv2 IDi group authentication.					
Option	Description											
<i>enable</i>	Enable IKEv2 IDi group authentication.											
<i>disable</i>	Disable IKEv2 IDi group authentication.											
group-authentication-secret	Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by a leading 0x.)	password-3	Not Specified									
authusrgrp	Authentication user group.	string	Maximum length: 35									
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable.</td> </tr> <tr> <td><i>subnet</i></td> <td>Enable addition of matching subnet selector.</td> </tr> <tr> <td><i>host</i></td> <td>Enable addition of host to host selector.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>subnet</i>	Enable addition of matching subnet selector.	<i>host</i>	Enable addition of host to host selector.			
Option	Description											
<i>disable</i>	Disable.											
<i>subnet</i>	Enable addition of matching subnet selector.											
<i>host</i>	Enable addition of host to host selector.											
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec tunnel idle timeout.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec tunnel idle timeout.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec tunnel idle timeout.	<i>disable</i>	Disable IPsec tunnel idle timeout.					
Option	Description											
<i>enable</i>	Enable IPsec tunnel idle timeout.											
<i>disable</i>	Disable IPsec tunnel idle timeout.											
idle-timeoutinterval	IPsec tunnel idle timeout in minutes .	integer	Minimum value: 5 Maximum value: 43200	15								
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable HA syncing of ESP sequence numbers.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable HA syncing of ESP sequence numbers.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HA syncing of ESP sequence numbers.	<i>disable</i>	Disable HA syncing of ESP sequence numbers.			
Option	Description									
<i>enable</i>	Enable HA syncing of ESP sequence numbers.									
<i>disable</i>	Disable HA syncing of ESP sequence numbers.									
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable copy the dscp in the ESP header to the inner IP Header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable copy the dscp in the ESP header to the inner IP Header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.	<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.			
Option	Description									
<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.									
<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.									
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sending auto-discovery short-cut messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending auto-discovery short-cut messages.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.			
Option	Description									
<i>enable</i>	Enable sending auto-discovery short-cut messages.									
<i>disable</i>	Disable sending auto-discovery short-cut messages.									
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable receiving auto-discovery short-cut messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable receiving auto-discovery short-cut messages.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable receiving auto-discovery short-cut messages.	<i>disable</i>	Disable receiving auto-discovery short-cut messages.			
Option	Description									
<i>enable</i>	Enable receiving auto-discovery short-cut messages.									
<i>disable</i>	Disable receiving auto-discovery short-cut messages.									
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forwarding auto-discovery short-cut messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forwarding auto-discovery short-cut messages.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.			
Option	Description									
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.									
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.									
auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of pre-shared-secret authentication for auto-discovery tunnels.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.	<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.			
Option	Description									
<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.									
<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.									

Parameter	Description	Type	Size	Default								
auto-discovery-shortcuts	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>independent</i></td> <td>Short-cut tunnels remain up if the parent tunnel goes down.</td> </tr> <tr> <td><i>dependent</i></td> <td>Short-cut tunnels are brought down if the parent tunnel goes down.</td> </tr> </tbody> </table>	Option	Description	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.	<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.					
Option	Description											
<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.											
<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.											
encapsulation	Enable/disable GRE/VXLAN encapsulation.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>No additional encapsulation.</td> </tr> <tr> <td><i>gre</i></td> <td>GRE encapsulation.</td> </tr> <tr> <td><i>vxlan</i></td> <td>VXLAN encapsulation.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	No additional encapsulation.	<i>gre</i>	GRE encapsulation.	<i>vxlan</i>	VXLAN encapsulation.			
Option	Description											
<i>none</i>	No additional encapsulation.											
<i>gre</i>	GRE encapsulation.											
<i>vxlan</i>	VXLAN encapsulation.											
encapsulation-address	Source for GRE/VXLAN tunnel address.	option	-	ike								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ike</i></td> <td>Use IKE/IPsec gateway addresses.</td> </tr> <tr> <td><i>ipv4</i></td> <td>Specify separate GRE/VXLAN tunnel address.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Specify separate GRE/VXLAN tunnel address.</td> </tr> </tbody> </table>	Option	Description	<i>ike</i>	Use IKE/IPsec gateway addresses.	<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.	<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.			
Option	Description											
<i>ike</i>	Use IKE/IPsec gateway addresses.											
<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.											
<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.											
encap-local-gw4	Local IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0								
encap-local-gw6	Local IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::								
encap-remote-gw4	Remote IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0								
encap-remote-gw6	Remote IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::								
vni	VNI of VXLAN tunnel.	integer	Minimum value: 1 Maximum value: 16777215	0								
nattraversal	Enable/disable NAT traversal.	option	-	enable								



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IPsec NAT traversal.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IPsec NAT traversal.</td> </tr> <tr> <td><i>forced</i></td> <td>Force IPsec NAT traversal on.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.					
Option	Description													
<i>enable</i>	Enable IPsec NAT traversal.													
<i>disable</i>	Disable IPsec NAT traversal.													
<i>forced</i>	Force IPsec NAT traversal on.													
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000	1200										
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable childless IKEv2 initiation (RFC 6023).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable childless IKEv2 initiation (RFC 6023).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).							
Option	Description													
<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).													
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).													
rekey	Enable/disable phase1 rekey.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable phase1 rekey.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable phase1 rekey.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.							
Option	Description													
<i>enable</i>	Enable phase1 rekey.													
<i>disable</i>	Disable phase1 rekey.													
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).	<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).							
Option	Description													
<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).													
<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).													
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sha1</i></td> <td>SHA1.</td> </tr> <tr> <td><i>sha2-256</i></td> <td>SHA2-256.</td> </tr> <tr> <td><i>sha2-384</i></td> <td>SHA2-384.</td> </tr> <tr> <td><i>sha2-512</i></td> <td>SHA2-512.</td> </tr> </tbody> </table>	Option	Description	<i>sha1</i>	SHA1.	<i>sha2-256</i>	SHA2-256.	<i>sha2-384</i>	SHA2-384.	<i>sha2-512</i>	SHA2-512.			
Option	Description													
<i>sha1</i>	SHA1.													
<i>sha2-256</i>	SHA2-256.													
<i>sha2-384</i>	SHA2-384.													
<i>sha2-512</i>	SHA2-512.													

Parameter	Description	Type	Size	Default
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1
	<b>Option</b>	<b>Description</b>		
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.		
	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).		
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable peer ID uniqueness enforcement.		
	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.		
	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.		
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.		
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 1000	8
fec-base	Number of base Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100	20

Parameter	Description	Type	Size	Default
fec-codec	ipsec fec encoding/decoding algorithm (0: reed-solomon, 1: xor).	integer	Minimum value: 0 Maximum value: 1	1
fec-redundant	Number of redundant Forward Error Correction packets (0 - 100, when fec-codec is reed-solomon or 1 when fec-codec is xor .	integer	Minimum value: 0 Maximum value: 100	1
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.		
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 10000	5000
network-overlay	Enable/disable network overlays.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable network overlays.		
	<i>enable</i>	Enable network overlays.		
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0

\* This parameter may not exist in some models.

### config ipv4-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

## config ipv6-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::

## config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```
config vpn ipsec phase2-interface
  Description: Configure VPN autokey tunnel.
  edit <name>
    set phase1name {string}
    set dhcp-ipsec [enable|disable]
    set proposal {option1}, {option2}, ...
    set pfs [enable|disable]
    set ipv4-df [enable|disable]
    set dhgrp {option1}, {option2}, ...
    set replay [enable|disable]
    set keepalive [enable|disable]
    set auto-negotiate [enable|disable]
    set add-route [phase1|enable|...]
    set inbound-dscp-copy [phase1|enable|...]
    set auto-discovery-sender [phase1|enable|...]
    set auto-discovery-forwarder [phase1|enable|...]
    set keylifeseconds {integer}
    set keylifekbs {integer}
    set keylife-type [seconds|kbs|...]
    set single-source [enable|disable]
    set route-overlap [use-old|use-new|...]
    set encapsulation [tunnel-mode|transport-mode]
    set l2tp [enable|disable]
    set comments {var-string}
    set initiator-ts-narrow [enable|disable]
    set diffserv [enable|disable]
    set diffservcode {user}
    set protocol {integer}
    set src-name {string}
    set src-name6 {string}
    set src-addr-type [subnet|range|...]
    set src-start-ip {ipv4-address-any}
    set src-start-ip6 {ipv6-address}
    set src-end-ip {ipv4-address-any}
    set src-end-ip6 {ipv6-address}
    set src-subnet {ipv4-classnet-any}
    set src-subnet6 {ipv6-prefix}
    set src-port {integer}
    set dst-name {string}
    set dst-name6 {string}
    set dst-addr-type [subnet|range|...]
```

```

set dst-start-ip {ipv4-address-any}
set dst-start-ip6 {ipv6-address}
set dst-end-ip {ipv4-address-any}
set dst-end-ip6 {ipv6-address}
set dst-subnet {ipv4-classnet-any}
set dst-subnet6 {ipv6-prefix}
set dst-port {integer}
next
end

```

## config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default																														
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15																															
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																											
Option	Description																																	
<i>enable</i>	Enable setting.																																	
<i>disable</i>	Disable setting.																																	
proposal	Phase2 proposal.	option	-																															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null-md5</i></td> <td>null-md5</td> </tr> <tr> <td><i>null-sha1</i></td> <td>null-sha1</td> </tr> <tr> <td><i>null-sha256</i></td> <td>null-sha256</td> </tr> <tr> <td><i>null-sha384</i></td> <td>null-sha384</td> </tr> <tr> <td><i>null-sha512</i></td> <td>null-sha512</td> </tr> <tr> <td><i>des-null</i></td> <td>des-null</td> </tr> <tr> <td><i>des-md5</i></td> <td>des-md5</td> </tr> <tr> <td><i>des-sha1</i></td> <td>des-sha1</td> </tr> <tr> <td><i>des-sha256</i></td> <td>des-sha256</td> </tr> <tr> <td><i>des-sha384</i></td> <td>des-sha384</td> </tr> <tr> <td><i>des-sha512</i></td> <td>des-sha512</td> </tr> <tr> <td><i>3des-null</i></td> <td>3des-null</td> </tr> <tr> <td><i>3des-md5</i></td> <td>3des-md5</td> </tr> <tr> <td><i>3des-sha1</i></td> <td>3des-sha1</td> </tr> </tbody> </table>	Option	Description	<i>null-md5</i>	null-md5	<i>null-sha1</i>	null-sha1	<i>null-sha256</i>	null-sha256	<i>null-sha384</i>	null-sha384	<i>null-sha512</i>	null-sha512	<i>des-null</i>	des-null	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-null</i>	3des-null	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1			
Option	Description																																	
<i>null-md5</i>	null-md5																																	
<i>null-sha1</i>	null-sha1																																	
<i>null-sha256</i>	null-sha256																																	
<i>null-sha384</i>	null-sha384																																	
<i>null-sha512</i>	null-sha512																																	
<i>des-null</i>	des-null																																	
<i>des-md5</i>	des-md5																																	
<i>des-sha1</i>	des-sha1																																	
<i>des-sha256</i>	des-sha256																																	
<i>des-sha384</i>	des-sha384																																	
<i>des-sha512</i>	des-sha512																																	
<i>3des-null</i>	3des-null																																	
<i>3des-md5</i>	3des-md5																																	
<i>3des-sha1</i>	3des-sha1																																	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>3des-sha256</i>	3des-sha256		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-null</i>	aes128-null		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm</i>	aes128gcm		
	<i>aes192-null</i>	aes192-null		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		

Parameter	Description	Type	Size	Default																																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aria128-sha512</i></td> <td>aria128-sha512</td> </tr> <tr> <td><i>aria192-null</i></td> <td>aria192-null</td> </tr> <tr> <td><i>aria192-md5</i></td> <td>aria192-md5</td> </tr> <tr> <td><i>aria192-sha1</i></td> <td>aria192-sha1</td> </tr> <tr> <td><i>aria192-sha256</i></td> <td>aria192-sha256</td> </tr> <tr> <td><i>aria192-sha384</i></td> <td>aria192-sha384</td> </tr> <tr> <td><i>aria192-sha512</i></td> <td>aria192-sha512</td> </tr> <tr> <td><i>aria256-null</i></td> <td>aria256-null</td> </tr> <tr> <td><i>aria256-md5</i></td> <td>aria256-md5</td> </tr> <tr> <td><i>aria256-sha1</i></td> <td>aria256-sha1</td> </tr> <tr> <td><i>aria256-sha256</i></td> <td>aria256-sha256</td> </tr> <tr> <td><i>aria256-sha384</i></td> <td>aria256-sha384</td> </tr> <tr> <td><i>aria256-sha512</i></td> <td>aria256-sha512</td> </tr> <tr> <td><i>seed-null</i></td> <td>seed-null</td> </tr> <tr> <td><i>seed-md5</i></td> <td>seed-md5</td> </tr> <tr> <td><i>seed-sha1</i></td> <td>seed-sha1</td> </tr> <tr> <td><i>seed-sha256</i></td> <td>seed-sha256</td> </tr> <tr> <td><i>seed-sha384</i></td> <td>seed-sha384</td> </tr> <tr> <td><i>seed-sha512</i></td> <td>seed-sha512</td> </tr> </tbody> </table>	Option	Description	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-null</i>	aria192-null	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
Option	Description																																											
<i>aria128-sha512</i>	aria128-sha512																																											
<i>aria192-null</i>	aria192-null																																											
<i>aria192-md5</i>	aria192-md5																																											
<i>aria192-sha1</i>	aria192-sha1																																											
<i>aria192-sha256</i>	aria192-sha256																																											
<i>aria192-sha384</i>	aria192-sha384																																											
<i>aria192-sha512</i>	aria192-sha512																																											
<i>aria256-null</i>	aria256-null																																											
<i>aria256-md5</i>	aria256-md5																																											
<i>aria256-sha1</i>	aria256-sha1																																											
<i>aria256-sha256</i>	aria256-sha256																																											
<i>aria256-sha384</i>	aria256-sha384																																											
<i>aria256-sha512</i>	aria256-sha512																																											
<i>seed-null</i>	seed-null																																											
<i>seed-md5</i>	seed-md5																																											
<i>seed-sha1</i>	seed-sha1																																											
<i>seed-sha256</i>	seed-sha256																																											
<i>seed-sha384</i>	seed-sha384																																											
<i>seed-sha512</i>	seed-sha512																																											
pfs	Enable/disable PFS feature.	option	-	enable																																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																					
Option	Description																																											
<i>enable</i>	Enable setting.																																											
<i>disable</i>	Disable setting.																																											
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-	disable																																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Set IPv4 DF.</td> </tr> <tr> <td><i>disable</i></td> <td>Reset IPv4 DF.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Set IPv4 DF.	<i>disable</i>	Reset IPv4 DF.																																					
Option	Description																																											
<i>enable</i>	Set IPv4 DF.																																											
<i>disable</i>	Reset IPv4 DF.																																											

Parameter	Description	Type	Size	Default																																				
dhgrp	Phase2 DH group.	option	-	14																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>DH Group 1.</td> </tr> <tr> <td>2</td> <td>DH Group 2.</td> </tr> <tr> <td>5</td> <td>DH Group 5.</td> </tr> <tr> <td>14</td> <td>DH Group 14.</td> </tr> <tr> <td>15</td> <td>DH Group 15.</td> </tr> <tr> <td>16</td> <td>DH Group 16.</td> </tr> <tr> <td>17</td> <td>DH Group 17.</td> </tr> <tr> <td>18</td> <td>DH Group 18.</td> </tr> <tr> <td>19</td> <td>DH Group 19.</td> </tr> <tr> <td>20</td> <td>DH Group 20.</td> </tr> <tr> <td>21</td> <td>DH Group 21.</td> </tr> <tr> <td>27</td> <td>DH Group 27.</td> </tr> <tr> <td>28</td> <td>DH Group 28.</td> </tr> <tr> <td>29</td> <td>DH Group 29.</td> </tr> <tr> <td>30</td> <td>DH Group 30.</td> </tr> <tr> <td>31</td> <td>DH Group 31.</td> </tr> <tr> <td>32</td> <td>DH Group 32.</td> </tr> </tbody> </table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
Option	Description																																							
1	DH Group 1.																																							
2	DH Group 2.																																							
5	DH Group 5.																																							
14	DH Group 14.																																							
15	DH Group 15.																																							
16	DH Group 16.																																							
17	DH Group 17.																																							
18	DH Group 18.																																							
19	DH Group 19.																																							
20	DH Group 20.																																							
21	DH Group 21.																																							
27	DH Group 27.																																							
28	DH Group 28.																																							
29	DH Group 29.																																							
30	DH Group 30.																																							
31	DH Group 31.																																							
32	DH Group 32.																																							
replay	Enable/disable replay detection.	option	-	enable																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																	
Option	Description																																							
<i>enable</i>	Enable setting.																																							
<i>disable</i>	Disable setting.																																							
keepalive	Enable/disable keep alive.	option	-	disable																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																	
Option	Description																																							
<i>enable</i>	Enable setting.																																							
<i>disable</i>	Disable setting.																																							
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable																																				



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
add-route	Enable/disable automatic route addition.	option	-	phase1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>phase1</i></td> <td>Add route according to phase1 add-route setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Add route for remote proxy ID.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not add route for remote proxy ID.</td> </tr> </tbody> </table>	Option	Description	<i>phase1</i>	Add route according to phase1 add-route setting.	<i>enable</i>	Add route for remote proxy ID.	<i>disable</i>	Do not add route for remote proxy ID.			
Option	Description											
<i>phase1</i>	Add route according to phase1 add-route setting.											
<i>enable</i>	Add route for remote proxy ID.											
<i>disable</i>	Do not add route for remote proxy ID.											
inbound-dscp-copy	Enable/disable copying of the DSCP field in the ESP header to the inner IP header.	option	-	phase1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>phase1</i></td> <td>Enable/disable copying the DSCP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable copy the DSCP in the ESP header to the inner IP Header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable copy the DSCP in the ESP header to the inner IP Header.</td> </tr> </tbody> </table>	Option	Description	<i>phase1</i>	Enable/disable copying the DSCP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.	<i>enable</i>	Enable copy the DSCP in the ESP header to the inner IP Header.	<i>disable</i>	Disable copy the DSCP in the ESP header to the inner IP Header.			
Option	Description											
<i>phase1</i>	Enable/disable copying the DSCP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.											
<i>enable</i>	Enable copy the DSCP in the ESP header to the inner IP Header.											
<i>disable</i>	Disable copy the DSCP in the ESP header to the inner IP Header.											
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>phase1</i></td> <td>Send short-cut messages according to the phase1 auto-discovery-sender setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable sending auto-discovery short-cut messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sending auto-discovery short-cut messages.</td> </tr> </tbody> </table>	Option	Description	<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.											
<i>enable</i>	Enable sending auto-discovery short-cut messages.											
<i>disable</i>	Disable sending auto-discovery short-cut messages.											
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>phase1</i></td> <td>Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable forwarding auto-discovery short-cut messages.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forwarding auto-discovery short-cut messages.</td> </tr> </tbody> </table>	Option	Description	<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.											
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.											
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.											

Parameter	Description	Type	Size	Default								
keylifeseconds	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800	43200								
keylifekbs	Phase2 key life in number of kilobytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295	5120								
keylife-type	Keylife type.	option	-	seconds								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>seconds</i></td> <td>Key life in seconds.</td> </tr> <tr> <td><i>kbs</i></td> <td>Key life in kilobytes.</td> </tr> <tr> <td><i>both</i></td> <td>Key life both.</td> </tr> </tbody> </table>	Option	Description	<i>seconds</i>	Key life in seconds.	<i>kbs</i>	Key life in kilobytes.	<i>both</i>	Key life both.			
Option	Description											
<i>seconds</i>	Key life in seconds.											
<i>kbs</i>	Key life in kilobytes.											
<i>both</i>	Key life both.											
single-source	Enable/disable single source IP restriction.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Only single source IP will be accepted.</td> </tr> <tr> <td><i>disable</i></td> <td>Source IP range will be accepted.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Only single source IP will be accepted.	<i>disable</i>	Source IP range will be accepted.					
Option	Description											
<i>enable</i>	Only single source IP will be accepted.											
<i>disable</i>	Source IP range will be accepted.											
route-overlap	Action for overlapping routes.	option	-	use-new								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>use-old</i></td> <td>Use the old route and do not add the new route.</td> </tr> <tr> <td><i>use-new</i></td> <td>Delete the old route and add the new route.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow overlapping routes.</td> </tr> </tbody> </table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.	<i>use-new</i>	Delete the old route and add the new route.	<i>allow</i>	Allow overlapping routes.			
Option	Description											
<i>use-old</i>	Use the old route and do not add the new route.											
<i>use-new</i>	Delete the old route and add the new route.											
<i>allow</i>	Allow overlapping routes.											
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel-mode</i></td> <td>Use tunnel mode encapsulation.</td> </tr> <tr> <td><i>transport-mode</i></td> <td>Use transport mode encapsulation.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel-mode</i>	Use tunnel mode encapsulation.	<i>transport-mode</i>	Use transport mode encapsulation.					
Option	Description											
<i>tunnel-mode</i>	Use tunnel mode encapsulation.											
<i>transport-mode</i>	Use transport mode encapsulation.											
l2tp	Enable/disable L2TP over IPsec.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable L2TP over IPsec.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable L2TP over IPsec.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable L2TP over IPsec.	<i>disable</i>	Disable L2TP over IPsec.					
Option	Description											
<i>enable</i>	Enable L2TP over IPsec.											
<i>disable</i>	Disable L2TP over IPsec.											

Parameter	Description	Type	Size	Default																		
comments	Comment.	var-string	Maximum length: 255																			
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
Option	Description																					
<i>enable</i>	Enable setting.																					
<i>disable</i>	Disable setting.																					
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
Option	Description																					
<i>enable</i>	Enable setting.																					
<i>disable</i>	Disable setting.																					
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified																			
protocol	Quick mode protocol selector .	integer	Minimum value: 0 Maximum value: 255	0																		
src-name	Local proxy ID name.	string	Maximum length: 79																			
src-name6	Local proxy ID name.	string	Maximum length: 79																			
src-addr-type	Local proxy ID type.	option	-	subnet																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subnet</i></td> <td>IPv4 subnet.</td> </tr> <tr> <td><i>range</i></td> <td>IPv4 range.</td> </tr> <tr> <td><i>ip</i></td> <td>IPv4 IP.</td> </tr> <tr> <td><i>name</i></td> <td>IPv4 firewall address or group name.</td> </tr> <tr> <td><i>subnet6</i></td> <td>IPv6 subnet.</td> </tr> <tr> <td><i>range6</i></td> <td>IPv6 range.</td> </tr> <tr> <td><i>ip6</i></td> <td>IPv6 IP.</td> </tr> <tr> <td><i>name6</i></td> <td>IPv6 firewall address or group name.</td> </tr> </tbody> </table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.	<i>subnet6</i>	IPv6 subnet.	<i>range6</i>	IPv6 range.	<i>ip6</i>	IPv6 IP.	<i>name6</i>	IPv6 firewall address or group name.			
Option	Description																					
<i>subnet</i>	IPv4 subnet.																					
<i>range</i>	IPv4 range.																					
<i>ip</i>	IPv4 IP.																					
<i>name</i>	IPv4 firewall address or group name.																					
<i>subnet6</i>	IPv6 subnet.																					
<i>range6</i>	IPv6 range.																					
<i>ip6</i>	IPv6 IP.																					
<i>name6</i>	IPv6 firewall address or group name.																					

Parameter	Description	Type	Size	Default																		
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0																		
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::																		
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0																		
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::																		
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0																		
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0																		
src-port	Quick mode source port .	integer	Minimum value: 0 Maximum value: 65535	0																		
dst-name	Remote proxy ID name.	string	Maximum length: 79																			
dst-name6	Remote proxy ID name.	string	Maximum length: 79																			
dst-addr-type	Remote proxy ID type.	option	-	subnet																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>subnet</i></td> <td>IPv4 subnet.</td> </tr> <tr> <td><i>range</i></td> <td>IPv4 range.</td> </tr> <tr> <td><i>ip</i></td> <td>IPv4 IP.</td> </tr> <tr> <td><i>name</i></td> <td>IPv4 firewall address or group name.</td> </tr> <tr> <td><i>subnet6</i></td> <td>IPv6 subnet.</td> </tr> <tr> <td><i>range6</i></td> <td>IPv6 range.</td> </tr> <tr> <td><i>ip6</i></td> <td>IPv6 IP.</td> </tr> <tr> <td><i>name6</i></td> <td>IPv6 firewall address or group name.</td> </tr> </tbody> </table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.	<i>subnet6</i>	IPv6 subnet.	<i>range6</i>	IPv6 range.	<i>ip6</i>	IPv6 IP.	<i>name6</i>	IPv6 firewall address or group name.			
Option	Description																					
<i>subnet</i>	IPv4 subnet.																					
<i>range</i>	IPv4 range.																					
<i>ip</i>	IPv4 IP.																					
<i>name</i>	IPv4 firewall address or group name.																					
<i>subnet6</i>	IPv6 subnet.																					
<i>range6</i>	IPv6 range.																					
<i>ip6</i>	IPv6 IP.																					
<i>name6</i>	IPv6 firewall address or group name.																					
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0																		
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::																		

Parameter	Description	Type	Size	Default
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
dst-port	Quick mode destination port .	integer	Minimum value: 0 Maximum value: 65535	0

## config vpn ipsec manualkey-interface

Configure IPsec manual keys.

```

config vpn ipsec manualkey-interface
  Description: Configure IPsec manual keys.
  edit <name>
    set interface {string}
    set ip-version [4|6]
    set addr-type [4|6]
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set auth-alg [null|md5|...]
    set enc-alg [null|des|...]
    set auth-key {user}
    set enc-key {user}
    set local-spi {user}
    set remote-spi {user}
    set npu-offload [enable|disable]
  next
end

```

## config vpn ipsec manualkey-interface

Parameter	Description	Type	Size	Default
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15	
ip-version	IP version to use for VPN interface.	option	-	4

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Use IPv4 addressing for gateways.</td> </tr> <tr> <td>6</td> <td>Use IPv6 addressing for gateways.</td> </tr> </tbody> </table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.											
Option	Description																	
4	Use IPv4 addressing for gateways.																	
6	Use IPv6 addressing for gateways.																	
addr-type	IP version to use for IP packets.	option	-	4														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Use IPv4 addressing for IP packets.</td> </tr> <tr> <td>6</td> <td>Use IPv6 addressing for IP packets.</td> </tr> </tbody> </table>	Option	Description	4	Use IPv4 addressing for IP packets.	6	Use IPv6 addressing for IP packets.											
Option	Description																	
4	Use IPv4 addressing for IP packets.																	
6	Use IPv6 addressing for IP packets.																	
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0														
remote-gw6	Remote IPv6 address of VPN gateway.	ipv6-address	Not Specified	::														
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address-any	Not Specified	0.0.0.0														
local-gw6	Local IPv6 address of VPN gateway.	ipv6-address	Not Specified	::														
auth-alg	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null</i></td> <td>null</td> </tr> <tr> <td><i>md5</i></td> <td>md5</td> </tr> <tr> <td><i>sha1</i></td> <td>sha1</td> </tr> <tr> <td><i>sha256</i></td> <td>sha256</td> </tr> <tr> <td><i>sha384</i></td> <td>sha384</td> </tr> <tr> <td><i>sha512</i></td> <td>sha512</td> </tr> </tbody> </table>	Option	Description	<i>null</i>	null	<i>md5</i>	md5	<i>sha1</i>	sha1	<i>sha256</i>	sha256	<i>sha384</i>	sha384	<i>sha512</i>	sha512			
Option	Description																	
<i>null</i>	null																	
<i>md5</i>	md5																	
<i>sha1</i>	sha1																	
<i>sha256</i>	sha256																	
<i>sha384</i>	sha384																	
<i>sha512</i>	sha512																	
enc-alg	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>null</i></td> <td>null</td> </tr> <tr> <td><i>des</i></td> <td>des</td> </tr> <tr> <td><i>3des</i></td> <td>3des</td> </tr> </tbody> </table>	Option	Description	<i>null</i>	null	<i>des</i>	des	<i>3des</i>	3des									
Option	Description																	
<i>null</i>	null																	
<i>des</i>	des																	
<i>3des</i>	3des																	

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes128</i></td> <td>aes128</td> </tr> <tr> <td><i>aes192</i></td> <td>aes192</td> </tr> <tr> <td><i>aes256</i></td> <td>aes256</td> </tr> <tr> <td><i>aria128</i></td> <td>aria128</td> </tr> <tr> <td><i>aria192</i></td> <td>aria192</td> </tr> <tr> <td><i>aria256</i></td> <td>aria256</td> </tr> <tr> <td><i>seed</i></td> <td>seed</td> </tr> </tbody> </table>	Option	Description	<i>aes128</i>	aes128	<i>aes192</i>	aes192	<i>aes256</i>	aes256	<i>aria128</i>	aria128	<i>aria192</i>	aria192	<i>aria256</i>	aria256	<i>seed</i>	seed			
Option	Description																			
<i>aes128</i>	aes128																			
<i>aes192</i>	aes192																			
<i>aes256</i>	aes256																			
<i>aria128</i>	aria128																			
<i>aria192</i>	aria192																			
<i>aria256</i>	aria256																			
<i>seed</i>	seed																			
auth-key	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																	
enc-key	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																	
local-spi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified																	
remote-spi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified																	
npu-offload *	Enable/disable offloading IPsec VPN manual key sessions to NPUs.	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable NPU offloading.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable NPU offloading.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.													
Option	Description																			
<i>enable</i>	Enable NPU offloading.																			
<i>disable</i>	Disable NPU offloading.																			

\* This parameter may not exist in some models.

## config vpn ipsec forticlient

Configure FortiClient policy realm.

```

config vpn ipsec forticlient
  Description: Configure FortiClient policy realm.
  edit <realm>
    set usergroupname {string}
    set phase2name {string}
    set status [enable|disable]
  next
end

```

## config vpn ipsec forticlient

Parameter	Description	Type	Size	Default
usergroupname	User group name for FortiClient users.	string	Maximum length: 35	
phase2name	Phase 2 tunnel name that you defined in the FortiClient dialup configuration.	string	Maximum length: 35	
status	Enable/disable this FortiClient configuration.	option	-	enable

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

## config vpn ipsec stats crypto

IPsec crypto statistics.

```
config vpn ipsec stats crypto
  Description: IPsec crypto statistics.
end
```

## config vpn ipsec stats tunnel

IPsec tunnel statistics.

```
config vpn ipsec stats tunnel
  Description: IPsec tunnel statistics.
end
```

## config vpn ipsec tunnel details

List all IPsec tunnels in details.

```
config vpn ipsec tunnel details
  Description: List all IPsec tunnels in details.
end
```

## config vpn ipsec tunnel summary

List all IPsec tunnels in summary.

```
config vpn ipsec tunnel summary
  Description: List all IPsec tunnels in summary.
end
```



## config vpn ipsec tunnel name

List IPsec tunnel by name.

```
config vpn ipsec tunnel name
  Description: List IPsec tunnel by name.
end
```

## config vpn pptp

Configure PPTP.

```
config vpn pptp
  Description: Configure PPTP.
  set status [enable|disable]
  set ip-mode [range|usrgrp]
  set eip {ipv4-address}
  set sip {ipv4-address}
  set local-ip {ipv4-address}
  set usrgrp {string}
end
```

## config vpn pptp

Parameter	Description	Type	Size	Default						
status	Enable/disable FortiGate as a PPTP gateway.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ip-mode	IP assignment mode for PPTP client.	option	-	range						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>range</i></td><td>PPTP client IP from manual config (range from sip to eip).</td></tr><tr><td><i>usrgrp</i></td><td>PPTP client IP from user-group defined server.</td></tr></tbody></table>	Option	Description	<i>range</i>	PPTP client IP from manual config (range from sip to eip).	<i>usrgrp</i>	PPTP client IP from user-group defined server.			
Option	Description									
<i>range</i>	PPTP client IP from manual config (range from sip to eip).									
<i>usrgrp</i>	PPTP client IP from user-group defined server.									
eip	End IP.	ipv4-address	Not Specified	0.0.0.0						
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0						
local-ip	Local IP to be used for peer's remote IP.	ipv4-address	Not Specified	0.0.0.0						
usrgrp	User group.	string	Maximum length: 35							

## config vpn l2tp

Configure L2TP.

```
config vpn l2tp
  Description: Configure L2TP.
  set status [enable|disable]
  set eip {ipv4-address}
  set sip {ipv4-address}
  set usrgrp {string}
  set enforce-ipsec [enable|disable]
  set lcp-echo-interval {integer}
  set lcp-max-echo-fails {integer}
  set compress [enable|disable]
end
```

## config vpn l2tp

Parameter	Description	Type	Size	Default						
status	Enable/disable FortiGate as a L2TP gateway.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
eip	End IP.	ipv4-address	Not Specified	0.0.0.0						
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0						
usrgrp	User group.	string	Maximum length: 35							
enforce-ipsec	Enable/disable IPsec enforcement.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable enforce-ipsec</td></tr><tr><td><i>disable</i></td><td>Disable enforce-ipsec</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable enforce-ipsec	<i>disable</i>	Disable enforce-ipsec			
Option	Description									
<i>enable</i>	Enable enforce-ipsec									
<i>disable</i>	Disable enforce-ipsec									
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5						

Parameter	Description	Type	Size	Default
lcp-max-echo-fails	Maximum number of missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3
compress	Enable/disable data compression.	option	-	disable

Option	Description
<i>enable</i>	Enable compress
<i>disable</i>	Disable compress

## config vpn ocvpn

Configure Overlay Controller VPN settings.

```

config vpn ocvpn
  Description: Configure Overlay Controller VPN settings.
  set status [enable|disable]
  set role [spoke|primary-hub|...]
  set multipath [enable|disable]
  set sdwan [enable|disable]
  set wan-interface <name1>, <name2>, ...
  set ip-allocation-block {ipv4-classnet-any}
config overlays
  Description: Network overlays to register with Overlay Controller VPN service.
  edit <overlay-name>
    set inter-overlay [allow|deny]
    set assign-ip [enable|disable]
    set ipv4-start-ip {ipv4-address}
    set ipv4-end-ip {ipv4-address}
  config subnets
    Description: Internal subnets to register with OCVPN service.
    edit <id>
      set type [subnet|interface]
      set subnet {ipv4-classnet-any}
      set interface {string}
    next
  end
next
end
config forticlient-access
  Description: Configure FortiClient settings.
  set status [enable|disable]
  set psksecret {password-3}
config auth-groups
  Description: FortiClient user authentication groups.
  edit <name>
    set auth-group {string}
    set overlays <overlay-name1>, <overlay-name2>, ...
  next

```

```

    end
end
set auto-discovery [enable|disable]
set poll-interval {integer}
set eap [enable|disable]
set eap-users {string}
set nat [enable|disable]
end

```

## config vpn ocvpn

Parameter	Description	Type	Size	Default								
status	Enable/disable Overlay Controller cloud assisted VPN.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Overlay Controller VPN.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Overlay Controller VPN.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Overlay Controller VPN.	<i>disable</i>	Disable Overlay Controller VPN.					
Option	Description											
<i>enable</i>	Enable Overlay Controller VPN.											
<i>disable</i>	Disable Overlay Controller VPN.											
role	Set device role.	option	-	spoke								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>spoke</i></td> <td>Register device as static spoke.</td> </tr> <tr> <td><i>primary-hub</i></td> <td>Register device as primary hub.</td> </tr> <tr> <td><i>secondary-hub</i></td> <td>Register device as secondary hub.</td> </tr> </tbody> </table>	Option	Description	<i>spoke</i>	Register device as static spoke.	<i>primary-hub</i>	Register device as primary hub.	<i>secondary-hub</i>	Register device as secondary hub.			
Option	Description											
<i>spoke</i>	Register device as static spoke.											
<i>primary-hub</i>	Register device as primary hub.											
<i>secondary-hub</i>	Register device as secondary hub.											
multipath	Enable/disable multipath redundancy.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multipath redundancy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multipath redundancy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multipath redundancy.	<i>disable</i>	Disable multipath redundancy.					
Option	Description											
<i>enable</i>	Enable multipath redundancy.											
<i>disable</i>	Disable multipath redundancy.											
sdwan	Enable/disable adding OCVPN tunnels to SDWAN.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable adding OCVPN tunnels to SDWAN.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable adding OCVPN tunnels to SDWAN.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable adding OCVPN tunnels to SDWAN.	<i>disable</i>	Disable adding OCVPN tunnels to SDWAN.					
Option	Description											
<i>enable</i>	Enable adding OCVPN tunnels to SDWAN.											
<i>disable</i>	Disable adding OCVPN tunnels to SDWAN.											
wan-interface <name>	FortiGate WAN interfaces to use with OCVPN. Interface name.	string	Maximum length: 79									
ip-allocation- block	Class B subnet reserved for private IP address assignment.	ipv4- classnet- any	Not Specified	10.254.0.0 255.255.0.0								

Parameter	Description	Type	Size	Default
auto-discovery	Enable/disable auto-discovery shortcuts.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ADVPN auto-discovery shortcuts.		
	<i>disable</i>	Disable ADVPN auto-discovery shortcuts.		
poll-interval	Overlay Controller VPN polling interval.	integer	Minimum value: 30 Maximum value: 120	30
eap	Enable/disable EAP client authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable EAP client authentication.		
	<i>disable</i>	Disable EAP client authentication.		
eap-users	EAP authentication user group.	string	Maximum length: 35	
nat	Enable/disable inter-overlay source NAT.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable inter-overlay source NAT.		
	<i>disable</i>	Disable inter-overlay source NAT.		

## config overlays

Parameter	Description	Type	Size	Default
inter-overlay	Allow or deny traffic from other overlays.	option	-	deny
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow traffic from other overlays.		
	<i>deny</i>	Deny traffic from other overlays.		
assign-ip	Enable/disable mode-cfg address assignment.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable client IPv4 address assignment.		
	<i>disable</i>	Disable client IPv4 address assignment.		

Parameter	Description	Type	Size	Default
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0

### config subnets

Parameter	Description	Type	Size	Default
type	Subnet type.	option	-	subnet
	<b>Option</b>	<b>Description</b>		
	<i>subnet</i>	Configure participating subnet IP and mask.		
	<i>interface</i>	Configure participating LAN interface.		
subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
interface	LAN interface.	string	Maximum length: 15	

### config forticlient-access

Parameter	Description	Type	Size	Default
status	Enable/disable FortiClient to access OCVPN networks.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiClient access to OCVPN overlays.		
	<i>disable</i>	Disable FortiClient access to OCVPN overlays.		
psksecret	Pre-shared secret for FortiClient PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	

### config auth-groups

Parameter	Description	Type	Size	Default
auth-group	Authentication user group for FortiClient access.	string	Maximum length: 35	
overlays <overlay-name>	OCVPN overlays to allow access to. Overlay name.	string	Maximum length: 79	

---

## config vpn ike gateway

List gateways.

```
config vpn ike gateway
  Description: List gateways.
  set <name> {string}
end
```

## config vpn ike gateway

Parameter	Description	Type	Size	Default
<name>	Name of IKE gateway to list.	string	Maximum length: -1	

## config vpn status l2tp

Display L2TP status.

```
config vpn status l2tp
  Description: Display L2TP status.
end
```

## config vpn status pptp

Display PPTP status.

```
config vpn status pptp
  Description: Display PPTP status.
end
```

## config vpn status ssl list

List current connections.

```
config vpn status ssl list
  Description: List current connections.
end
```

## config vpn status ssl hw-acceleration-status

SSL hardware acceleration status.

```
config vpn status ssl hw-acceleration-status
  Description: SSL hardware acceleration status.
end
```

## waf

This section includes syntax for the following commands:

- [config waf sub-class on page 1344](#)
- [config waf profile on page 1345](#)
- [config waf signature on page 1345](#)
- [config waf main-class on page 1344](#)

### config waf main-class

Hidden table for datasource.

```
config waf main-class
  Description: Hidden table for datasource.
  edit <id>
    set name {string}
  next
end
```

### config waf main-class

Parameter	Description	Type	Size	Default
name	Main signature class name.	string	Maximum length: 127	

### config waf sub-class

Hidden table for datasource.

```
config waf sub-class
  Description: Hidden table for datasource.
  edit <id>
    set name {string}
  next
end
```

### config waf sub-class

Parameter	Description	Type	Size	Default
name	Signature subclass name.	string	Maximum length: 127	



---

## config waf signature

Hidden table for datasource.

```
config waf signature
  Description: Hidden table for datasource.
  edit <id>
    set desc {string}
  next
end
```

## config waf signature

Parameter	Description	Type	Size	Default
desc	Signature description.	string	Maximum length: 511	

## config waf profile

Web application firewall configuration.

```
config waf profile
  Description: Web application firewall configuration.
  edit <name>
    set external [disable|enable]
    set extended-log [enable|disable]
    config signature
      Description: WAF signatures.
      config main-class
        Description: Main signature class.
        edit <id>
          set status [enable|disable]
          set action [allow|block|...]
          set log [enable|disable]
          set severity [high|medium|...]
        next
      end
      set disabled-sub-class <id1>, <id2>, ...
      set disabled-signature <id1>, <id2>, ...
      set credit-card-detection-threshold {integer}
    config custom-signature
      Description: Custom signature.
      edit <name>
        set status [enable|disable]
        set action [allow|block|...]
        set log [enable|disable]
        set severity [high|medium|...]
        set direction [request|response]
        set case-sensitivity [disable|enable]
        set pattern {string}
        set target {option1}, {option2}, ...
      next
    end
```

```
end
config constraint
  Description: WAF HTTP protocol restrictions.
  config header-length
    Description: HTTP header length in request.
    set status [enable|disable]
    set length {integer}
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
  config content-length
    Description: HTTP content length in request.
    set status [enable|disable]
    set length {integer}
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
  config param-length
    Description: Maximum length of parameter in URL, HTTP POST request or HTTP body.
    set status [enable|disable]
    set length {integer}
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
  config line-length
    Description: HTTP line length in request.
    set status [enable|disable]
    set length {integer}
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
  config url-param-length
    Description: Maximum length of parameter in URL.
    set status [enable|disable]
    set length {integer}
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
  config version
    Description: Enable/disable HTTP version check.
    set status [enable|disable]
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
  config method
    Description: Enable/disable HTTP method check.
    set status [enable|disable]
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
  end
end
```

---

```

config hostname
  Description: Enable/disable hostname check.
  set status [enable|disable]
  set action [allow|block]
  set log [enable|disable]
  set severity [high|medium|...]
end
config malformed
  Description: Enable/disable malformed HTTP request check.
  set status [enable|disable]
  set action [allow|block]
  set log [enable|disable]
  set severity [high|medium|...]
end
config max-cookie
  Description: Maximum number of cookies in HTTP request.
  set status [enable|disable]
  set max-cookie {integer}
  set action [allow|block]
  set log [enable|disable]
  set severity [high|medium|...]
end
config max-header-line
  Description: Maximum number of HTTP header line.
  set status [enable|disable]
  set max-header-line {integer}
  set action [allow|block]
  set log [enable|disable]
  set severity [high|medium|...]
end
config max-url-param
  Description: Maximum number of parameters in URL.
  set status [enable|disable]
  set max-url-param {integer}
  set action [allow|block]
  set log [enable|disable]
  set severity [high|medium|...]
end
config max-range-segment
  Description: Maximum number of range segments in HTTP range line.
  set status [enable|disable]
  set max-range-segment {integer}
  set action [allow|block]
  set log [enable|disable]
  set severity [high|medium|...]
end
config exception
  Description: HTTP constraint exception.
  edit <id>
    set pattern {string}
    set regex [enable|disable]
    set address {string}
    set header-length [enable|disable]
    set content-length [enable|disable]
    set param-length [enable|disable]
    set line-length [enable|disable]
    set url-param-length [enable|disable]

```

```

        set version [enable|disable]
        set method [enable|disable]
        set hostname [enable|disable]
        set malformed [enable|disable]
        set max-cookie [enable|disable]
        set max-header-line [enable|disable]
        set max-url-param [enable|disable]
        set max-range-segment [enable|disable]
    next
end
end
config method
    Description: Method restriction.
    set status [enable|disable]
    set log [enable|disable]
    set severity [high|medium|...]
    set default-allowed-methods {option1}, {option2}, ...
    config method-policy
        Description: HTTP method policy.
        edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}
            set allowed-methods {option1}, {option2}, ...
        next
    end
end
config address-list
    Description: Black address list and white address list.
    set status [enable|disable]
    set blocked-log [enable|disable]
    set severity [high|medium|...]
    set trusted-address <name1>, <name2>, ...
    set blocked-address <name1>, <name2>, ...
end
config url-access
    Description: URL access list
    edit <id>
        set address {string}
        set action [bypass|permit|...]
        set log [enable|disable]
        set severity [high|medium|...]
        config access-pattern
            Description: URL access pattern.
            edit <id>
                set srcaddr {string}
                set pattern {string}
                set regex [enable|disable]
                set negate [enable|disable]
            next
        end
    next
end
    set comment {var-string}
next
end

```

## config waf profile

Parameter	Description	Type	Size	Default						
external	Disable/Enable external HTTP Inspection.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable external inspection.</td></tr><tr><td><i>enable</i></td><td>Enable external inspection.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable external inspection.	<i>enable</i>	Enable external inspection.			
Option	Description									
<i>disable</i>	Disable external inspection.									
<i>enable</i>	Enable external inspection.									
extended-log	Enable/disable extended logging.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
comment	Comment.	var-string	Maximum length: 1023							

## config signature

Parameter	Description	Type	Size	Default
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	
disabled-signature <id>	Disabled signatures Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	
credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 Maximum value: 128	3

## config main-class

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> <tr> <td><i>erase</i></td> <td>Erase credit card numbers.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.	<i>erase</i>	Erase credit card numbers.			
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
<i>erase</i>	Erase credit card numbers.											
log	Enable/disable logging.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config custom-signature

Parameter	Description	Type	Size	Default						
status	Status.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
action	Action.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.			
Option	Description									
<i>allow</i>	Allow.									
<i>block</i>	Block.									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>erase</i></td> <td>Erase credit card numbers.</td> </tr> </tbody> </table>	Option	Description	<i>erase</i>	Erase credit card numbers.											
Option	Description															
<i>erase</i>	Erase credit card numbers.															
log	Enable/disable logging.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
severity	Severity.	option	-	medium												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.							
Option	Description															
<i>high</i>	High severity.															
<i>medium</i>	Medium severity.															
<i>low</i>	Low severity.															
direction	Traffic direction.	option	-	request												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>request</i></td> <td>Match HTTP request.</td> </tr> <tr> <td><i>response</i></td> <td>Match HTTP response.</td> </tr> </tbody> </table>	Option	Description	<i>request</i>	Match HTTP request.	<i>response</i>	Match HTTP response.									
Option	Description															
<i>request</i>	Match HTTP request.															
<i>response</i>	Match HTTP response.															
case-sensitivity	Case sensitivity in pattern.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Case insensitive in pattern.</td> </tr> <tr> <td><i>enable</i></td> <td>Case sensitive in pattern.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Case insensitive in pattern.	<i>enable</i>	Case sensitive in pattern.									
Option	Description															
<i>disable</i>	Case insensitive in pattern.															
<i>enable</i>	Case sensitive in pattern.															
pattern	Match pattern.	string	Maximum length: 511													
target	Match HTTP target.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>arg</i></td> <td>HTTP arguments.</td> </tr> <tr> <td><i>arg-name</i></td> <td>Names of HTTP arguments.</td> </tr> <tr> <td><i>req-body</i></td> <td>HTTP request body.</td> </tr> <tr> <td><i>req-cookie</i></td> <td>HTTP request cookies.</td> </tr> <tr> <td><i>req-cookie-name</i></td> <td>HTTP request cookie names.</td> </tr> </tbody> </table>	Option	Description	<i>arg</i>	HTTP arguments.	<i>arg-name</i>	Names of HTTP arguments.	<i>req-body</i>	HTTP request body.	<i>req-cookie</i>	HTTP request cookies.	<i>req-cookie-name</i>	HTTP request cookie names.			
Option	Description															
<i>arg</i>	HTTP arguments.															
<i>arg-name</i>	Names of HTTP arguments.															
<i>req-body</i>	HTTP request body.															
<i>req-cookie</i>	HTTP request cookies.															
<i>req-cookie-name</i>	HTTP request cookie names.															

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>req-filename</i></td> <td>HTTP request file name.</td> </tr> <tr> <td><i>req-header</i></td> <td>HTTP request headers.</td> </tr> <tr> <td><i>req-header-name</i></td> <td>HTTP request header names.</td> </tr> <tr> <td><i>req-raw-uri</i></td> <td>Raw URI of HTTP request.</td> </tr> <tr> <td><i>req-uri</i></td> <td>URI of HTTP request.</td> </tr> <tr> <td><i>resp-body</i></td> <td>HTTP response body.</td> </tr> <tr> <td><i>resp-hdr</i></td> <td>HTTP response headers.</td> </tr> <tr> <td><i>resp-status</i></td> <td>HTTP response status.</td> </tr> </tbody> </table>	Option	Description	<i>req-filename</i>	HTTP request file name.	<i>req-header</i>	HTTP request headers.	<i>req-header-name</i>	HTTP request header names.	<i>req-raw-uri</i>	Raw URI of HTTP request.	<i>req-uri</i>	URI of HTTP request.	<i>resp-body</i>	HTTP response body.	<i>resp-hdr</i>	HTTP response headers.	<i>resp-status</i>	HTTP response status.			
Option	Description																					
<i>req-filename</i>	HTTP request file name.																					
<i>req-header</i>	HTTP request headers.																					
<i>req-header-name</i>	HTTP request header names.																					
<i>req-raw-uri</i>	Raw URI of HTTP request.																					
<i>req-uri</i>	URI of HTTP request.																					
<i>resp-body</i>	HTTP response body.																					
<i>resp-hdr</i>	HTTP response headers.																					
<i>resp-status</i>	HTTP response status.																					

### config header-length

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192						
action	Action.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.			
Option	Description									
<i>allow</i>	Allow.									
<i>block</i>	Block.									
log	Enable/disable logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
severity	Severity.	option	-	medium						



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config content-length

Parameter	Description	Type	Size	Default								
status	Enable/disable the constraint.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	67108864								
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

## config param-length

Parameter	Description	Type	Size	Default								
status	Enable/disable the constraint.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
length	Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192								
action	Action.	option	-	allow								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>block</i></td><td>Block.</td></tr></tbody></table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr><tr><td><i>low</i></td><td>Low severity.</td></tr></tbody></table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

## config line-length

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default								
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024								
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config url-param-length

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192						
action	Action.	option	-	allow						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config version

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
action	Action.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.			
Option	Description									
<i>allow</i>	Allow.									
<i>block</i>	Block.									
log	Enable/disable logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
severity	Severity.	option	-	medium						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

### config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

### config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
log	Enable/disable logging.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
severity	Severity.	option	-	medium																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity</td> </tr> <tr> <td><i>medium</i></td> <td>medium severity</td> </tr> <tr> <td><i>low</i></td> <td>low severity</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity	<i>medium</i>	medium severity	<i>low</i>	low severity															
Option	Description																							
<i>high</i>	High severity																							
<i>medium</i>	medium severity																							
<i>low</i>	low severity																							
default-allowed-methods	Methods.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>get</i></td> <td>HTTP GET method.</td> </tr> <tr> <td><i>post</i></td> <td>HTTP POST method.</td> </tr> <tr> <td><i>put</i></td> <td>HTTP PUT method.</td> </tr> <tr> <td><i>head</i></td> <td>HTTP HEAD method.</td> </tr> <tr> <td><i>connect</i></td> <td>HTTP CONNECT method.</td> </tr> <tr> <td><i>trace</i></td> <td>HTTP TRACE method.</td> </tr> <tr> <td><i>options</i></td> <td>HTTP OPTIONS method.</td> </tr> <tr> <td><i>delete</i></td> <td>HTTP DELETE method.</td> </tr> <tr> <td><i>others</i></td> <td>Other HTTP methods.</td> </tr> </tbody> </table>	Option	Description	<i>get</i>	HTTP GET method.	<i>post</i>	HTTP POST method.	<i>put</i>	HTTP PUT method.	<i>head</i>	HTTP HEAD method.	<i>connect</i>	HTTP CONNECT method.	<i>trace</i>	HTTP TRACE method.	<i>options</i>	HTTP OPTIONS method.	<i>delete</i>	HTTP DELETE method.	<i>others</i>	Other HTTP methods.			
Option	Description																							
<i>get</i>	HTTP GET method.																							
<i>post</i>	HTTP POST method.																							
<i>put</i>	HTTP PUT method.																							
<i>head</i>	HTTP HEAD method.																							
<i>connect</i>	HTTP CONNECT method.																							
<i>trace</i>	HTTP TRACE method.																							
<i>options</i>	HTTP OPTIONS method.																							
<i>delete</i>	HTTP DELETE method.																							
<i>others</i>	Other HTTP methods.																							

### config hostname

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config malformed

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
action	Action.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.			
Option	Description									
<i>allow</i>	Allow.									
<i>block</i>	Block.									
log	Enable/disable logging.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config max-cookie

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16						
action	Action.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.			
Option	Description									
<i>allow</i>	Allow.									
<i>block</i>	Block.									
log	Enable/disable logging.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
severity	Severity.	option	-	medium						



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config max-header-line

Parameter	Description	Type	Size	Default								
status	Enable/disable the constraint.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	32								
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config max-url-param

Parameter	Description	Type	Size	Default								
status	Enable/disable the constraint.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16								
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config max-range-segment

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default								
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	5								
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow.</td> </tr> <tr> <td><i>block</i></td> <td>Block.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.					
Option	Description											
<i>allow</i>	Allow.											
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config exception

Parameter	Description	Type	Size	Default						
pattern	URL pattern.	string	Maximum length: 511							
regex	Enable/disable regular expression based pattern match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
address	Host address.	string	Maximum length: 79							
header-length	HTTP header length in request.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
content-length	HTTP content length in request.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
line-length	HTTP line length in request.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
url-param-length	Maximum length of parameter in URL.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
version	Enable/disable HTTP version check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
method	Enable/disable HTTP method check.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
hostname	Enable/disable hostname check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
malformed	Enable/disable malformed HTTP request check.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-cookie	Maximum number of cookies in HTTP request.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-header-line	Maximum number of HTTP header line.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-url-param	Maximum number of parameters in URL.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-range-segment	Maximum number of range segments in HTTP range line.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

### config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
action	Action.	option	-	allow
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium

### config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium
default-allowed-methods	Methods.	option	-	

### config method-policy

Parameter	Description	Type	Size	Default						
pattern	URL pattern.	string	Maximum length: 511							
regex	Enable/disable regular expression based pattern match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
address	Host address.	string	Maximum length: 79							
allowed-methods	Allowed Methods.	option	-							

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>get</i></td> <td>HTTP GET method.</td> </tr> <tr> <td><i>post</i></td> <td>HTTP POST method.</td> </tr> <tr> <td><i>put</i></td> <td>HTTP PUT method.</td> </tr> <tr> <td><i>head</i></td> <td>HTTP HEAD method.</td> </tr> <tr> <td><i>connect</i></td> <td>HTTP CONNECT method.</td> </tr> <tr> <td><i>trace</i></td> <td>HTTP TRACE method.</td> </tr> <tr> <td><i>options</i></td> <td>HTTP OPTIONS method.</td> </tr> <tr> <td><i>delete</i></td> <td>HTTP DELETE method.</td> </tr> <tr> <td><i>others</i></td> <td>Other HTTP methods.</td> </tr> </tbody> </table>	Option	Description	<i>get</i>	HTTP GET method.	<i>post</i>	HTTP POST method.	<i>put</i>	HTTP PUT method.	<i>head</i>	HTTP HEAD method.	<i>connect</i>	HTTP CONNECT method.	<i>trace</i>	HTTP TRACE method.	<i>options</i>	HTTP OPTIONS method.	<i>delete</i>	HTTP DELETE method.	<i>others</i>	Other HTTP methods.			
Option	Description																							
<i>get</i>	HTTP GET method.																							
<i>post</i>	HTTP POST method.																							
<i>put</i>	HTTP PUT method.																							
<i>head</i>	HTTP HEAD method.																							
<i>connect</i>	HTTP CONNECT method.																							
<i>trace</i>	HTTP TRACE method.																							
<i>options</i>	HTTP OPTIONS method.																							
<i>delete</i>	HTTP DELETE method.																							
<i>others</i>	Other HTTP methods.																							

### config address-list

Parameter	Description	Type	Size	Default								
status	Status.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
blocked-log	Enable/disable logging on blocked addresses.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	

### config url-access

Parameter	Description	Type	Size	Default								
address	Host address.	string	Maximum length: 79									
action	Action.	option	-	permit								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bypass</i></td> <td>Allow the HTTP request, also bypass further WAF scanning.</td> </tr> <tr> <td><i>permit</i></td> <td>Allow the HTTP request, and continue further WAF scanning.</td> </tr> <tr> <td><i>block</i></td> <td>Block HTTP request.</td> </tr> </tbody> </table>	Option	Description	<i>bypass</i>	Allow the HTTP request, also bypass further WAF scanning.	<i>permit</i>	Allow the HTTP request, and continue further WAF scanning.	<i>block</i>	Block HTTP request.			
Option	Description											
<i>bypass</i>	Allow the HTTP request, also bypass further WAF scanning.											
<i>permit</i>	Allow the HTTP request, and continue further WAF scanning.											
<i>block</i>	Block HTTP request.											
log	Enable/disable logging.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High severity.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium severity.</td> </tr> <tr> <td><i>low</i></td> <td>Low severity.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											

### config access-pattern

Parameter	Description	Type	Size	Default
srcaddr	Source address.	string	Maximum length: 79	
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
negate	Enable/disable match negation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

## web-proxy

This section includes syntax for the following commands:

- [config web-proxy wisp on page 1384](#)
- [config web-proxy debug-url on page 1384](#)
- [config web-proxy global on page 1374](#)
- [config web-proxy profile on page 1370](#)
- [config web-proxy url-match on page 1385](#)
- [config web-proxy forward-server-group on page 1382](#)
- [config web-proxy forward-server on page 1381](#)
- [config web-proxy explicit on page 1376](#)

### config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
  Description: Configure web proxy profiles.
  edit <name>
    set header-client-ip [pass|add|...]
    set header-via-request [pass|add|...]
    set header-via-response [pass|add|...]
    set header-x-forwarded-for [pass|add|...]
    set header-front-end-https [pass|add|...]
    set header-x-authenticated-user [pass|add|...]
    set header-x-authenticated-groups [pass|add|...]
    set strip-encoding [enable|disable]
    set log-header-change [enable|disable]
  config headers
    Description: Configure HTTP forwarded requests headers.
    edit <id>
      set name {string}
      set dstaddr <name1>, <name2>, ...
      set dstaddr6 <name1>, <name2>, ...
      set action [add-to-request|add-to-response|...]
      set content {string}
      set base64-encoding [disable|enable]
      set add-option [append|new-on-not-found|...]
      set protocol {option1}, {option2}, ...
    next
  end
next
end
```

## config web-proxy profile

Parameter	Description	Type	Size	Default								
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-x-forwarded-for	Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-front-end-https	Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-x-authenticated-user	Action to take on the HTTP x-authenticated-user header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-x-authenticated-groups	Action to take on the HTTP x-authenticated-groups header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Forward the same HTTP header.</td> </tr> <tr> <td><i>add</i></td> <td>Add the HTTP header.</td> </tr> <tr> <td><i>remove</i></td> <td>Remove the HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable stripping of unsupported encoding from the request header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable stripping of unsupported encoding from the request header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable stripping of unsupported encoding from the request header.	<i>disable</i>	Disable stripping of unsupported encoding from the request header.					
Option	Description											
<i>enable</i>	Enable stripping of unsupported encoding from the request header.											
<i>disable</i>	Disable stripping of unsupported encoding from the request header.											
log-header-change	Enable/disable logging HTTP header changes.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Enable/disable logging HTTP header changes.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Enable/disable logging HTTP header changes.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Enable/disable logging HTTP header changes.	<i>disable</i>	Disable Enable/disable logging HTTP header changes.					
Option	Description											
<i>enable</i>	Enable Enable/disable logging HTTP header changes.											
<i>disable</i>	Disable Enable/disable logging HTTP header changes.											

## config headers

Parameter	Description	Type	Size	Default										
name	HTTP forwarded header name.	string	Maximum length: 79											
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79											
dstaddr6 <name>	Destination address and address group names (IPv6). Address name.	string	Maximum length: 79											
action	Action when the HTTP header is forwarded.	option	-	add-to-request										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>add-to-request</i></td> <td>Add the HTTP header to request.</td> </tr> <tr> <td><i>add-to-response</i></td> <td>Add the HTTP header to response.</td> </tr> <tr> <td><i>remove-from-request</i></td> <td>Remove the HTTP header from request.</td> </tr> <tr> <td><i>remove-from-response</i></td> <td>Remove the HTTP header from response.</td> </tr> </tbody> </table>	Option	Description	<i>add-to-request</i>	Add the HTTP header to request.	<i>add-to-response</i>	Add the HTTP header to response.	<i>remove-from-request</i>	Remove the HTTP header from request.	<i>remove-from-response</i>	Remove the HTTP header from response.			
Option	Description													
<i>add-to-request</i>	Add the HTTP header to request.													
<i>add-to-response</i>	Add the HTTP header to response.													
<i>remove-from-request</i>	Remove the HTTP header from request.													
<i>remove-from-response</i>	Remove the HTTP header from response.													
content	HTTP header content.	string	Maximum length: 255											
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of base64 encoding of HTTP content.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of base64 encoding of HTTP content.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of base64 encoding of HTTP content.	<i>enable</i>	Enable use of base64 encoding of HTTP content.							
Option	Description													
<i>disable</i>	Disable use of base64 encoding of HTTP content.													
<i>enable</i>	Enable use of base64 encoding of HTTP content.													
add-option	Configure options to append content to existing HTTP header or add new HTTP header.	option	-	new										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>append</i></td> <td>Append content to existing HTTP header or create new header if HTTP header is not found.</td> </tr> <tr> <td><i>new-on-not-found</i></td> <td>Create new header only if existing HTTP header is not found.</td> </tr> <tr> <td><i>new</i></td> <td>Create new header regardless if existing HTTP header is found or not.</td> </tr> </tbody> </table>	Option	Description	<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.	<i>new</i>	Create new header regardless if existing HTTP header is found or not.					
Option	Description													
<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.													
<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.													
<i>new</i>	Create new header regardless if existing HTTP header is found or not.													
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-	https http										

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>https</i></td> <td>Perform add-option action on HTTPS.</td> </tr> <tr> <td><i>http</i></td> <td>Perform add-option action on HTTP.</td> </tr> </tbody> </table>	Option	Description	<i>https</i>	Perform add-option action on HTTPS.	<i>http</i>	Perform add-option action on HTTP.			
Option	Description									
<i>https</i>	Perform add-option action on HTTPS.									
<i>http</i>	Perform add-option action on HTTP.									

## config web-proxy global

Configure Web proxy global settings.

```
config web-proxy global
  Description: Configure Web proxy global settings.
  set ssl-cert {string}
  set ssl-ca-cert {string}
  set fast-policy-match [enable|disable]
  set proxy-fqdn {string}
  set max-request-length {integer}
  set max-message-length {integer}
  set strict-web-check [enable|disable]
  set forward-proxy-auth [enable|disable]
  set forward-server-affinity-timeout {integer}
  set max-waf-body-cache-length {integer}
  set webproxy-profile {string}
  set learn-client-ip [enable|disable]
  set learn-client-ip-from-header {option1}, {option2}, ...
  set learn-client-ip-srcaddr <name1>, <name2>, ...
  set learn-client-ip-srcaddr6 <name1>, <name2>, ...
end
```

## config web-proxy global

Parameter	Description	Type	Size	Default						
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	Fortinet_Factory						
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	Fortinet_CA_SSL						
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-fqdn	Fully Qualified Domain Name to connect to the explicit web proxy.	string	Maximum length: 255	default.fqdn						

Parameter	Description	Type	Size	Default						
max-request-length	Maximum length of HTTP request line .	integer	Minimum value: 2 Maximum value: 64	8						
max-message-length	Maximum length of HTTP message, not including body .	integer	Minimum value: 16 Maximum value: 256	32						
strict-web-check	Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP 1.1.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strict web checking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strict web checking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strict web checking.	<i>disable</i>	Disable strict web checking.			
Option	Description									
<i>enable</i>	Enable strict web checking.									
<i>disable</i>	Disable strict web checking.									
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable forwarding proxy authentication headers.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable forwarding proxy authentication headers.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable forwarding proxy authentication headers.	<i>disable</i>	Disable forwarding proxy authentication headers.			
Option	Description									
<i>enable</i>	Enable forwarding proxy authentication headers.									
<i>disable</i>	Disable forwarding proxy authentication headers.									
forward-server-affinity-timeout	Period of time before the source IP's traffic is no longer assigned to the forwarding server .	integer	Minimum value: 6 Maximum value: 60	30						
max-waf-body-cache-length	Maximum length of HTTP messages processed by Web Application Firewall .	integer	Minimum value: 10 Maximum value: 1024	32						
webproxy-profile	Name of the web proxy profile to apply when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.	string	Maximum length: 63							
learn-client-ip	Enable/disable learning the client's IP address from headers.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable learning the client's IP address from headers.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable learning the client's IP address from headers.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable learning the client's IP address from headers.	<i>disable</i>	Disable learning the client's IP address from headers.			
Option	Description									
<i>enable</i>	Enable learning the client's IP address from headers.									
<i>disable</i>	Disable learning the client's IP address from headers.									

Parameter	Description	Type	Size	Default								
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>true-client-ip</i></td> <td>Learn the client IP address from the True-Client-IP header.</td> </tr> <tr> <td><i>x-real-ip</i></td> <td>Learn the client IP address from the X-Real-IP header.</td> </tr> <tr> <td><i>x-forwarded-for</i></td> <td>Learn the client IP address from the X-Forwarded-For header.</td> </tr> </tbody> </table>	Option	Description	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.	<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.	<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.			
Option	Description											
<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.											
<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.											
<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.											
learn-client-ip-srcaddr <name>	Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79									
learn-client-ip-srcaddr6 <name>	IPv6 Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79									

## config web-proxy explicit

Configure explicit Web proxy settings.

```

config web-proxy explicit
  Description: Configure explicit Web proxy settings.
  set status [enable|disable]
  set ftp-over-http [enable|disable]
  set socks [enable|disable]
  set http-incoming-port {user}
  set https-incoming-port {user}
  set ftp-incoming-port {user}
  set socks-incoming-port {user}
  set incoming-ip {ipv4-address-any}
  set outgoing-ip {ipv4-address-any}
  set ipv6-status [enable|disable]
  set incoming-ip6 {ipv6-address}
  set outgoing-ip6 {ipv6-address}
  set strict-guest [enable|disable]
  set pref-dns-result [ipv4|ipv6]
  set unknown-http-version [reject|tunnel|...]
  set realm {string}
  set sec-default-action [accept|deny]
  set https-replacement-message [enable|disable]
  set message-upon-server-error [enable|disable]
  set pac-file-server-status [enable|disable]
  set pac-file-url {user}
  set pac-file-server-port {user}
  set pac-file-name {string}
  set pac-file-data {user}
config pac-policy
  Description: PAC policies.
  edit <policyid>

```



```

    set status [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set pac-file-name {string}
    set pac-file-data {user}
    set comments {var-string}
  next
end
set ssl-algorithm [high|medium|...]
set trace-auth-no-rsp [enable|disable]
end

```

## config web-proxy explicit

Parameter	Description	Type	Size	Default						
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the explicit web proxy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the explicit web proxy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the explicit web proxy.	<i>disable</i>	Disable the explicit web proxy.			
Option	Description									
<i>enable</i>	Enable the explicit web proxy.									
<i>disable</i>	Disable the explicit web proxy.									
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FTP-over-HTTP sessions.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FTP-over-HTTP sessions.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FTP-over-HTTP sessions.	<i>disable</i>	Disable FTP-over-HTTP sessions.			
Option	Description									
<i>enable</i>	Enable FTP-over-HTTP sessions.									
<i>disable</i>	Disable FTP-over-HTTP sessions.									
socks	Enable/disable the SOCKS proxy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable the SOCKS proxy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable the SOCKS proxy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable the SOCKS proxy.	<i>disable</i>	Disable the SOCKS proxy.			
Option	Description									
<i>enable</i>	Enable the SOCKS proxy.									
<i>disable</i>	Disable the SOCKS proxy.									
http-incoming-port	Accept incoming HTTP requests on one or more ports .	user	Not Specified							
https-incoming-port	Accept incoming HTTPS requests on one or more ports .	user	Not Specified							
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports .	user	Not Specified							
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports .	user	Not Specified							

Parameter	Description	Type	Size	Default						
incoming-ip	Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0						
outgoing-ip	Outgoing HTTP requests will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified							
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable allowing an IPv6 web proxy destination.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable allowing an IPv6 web proxy destination.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable allowing an IPv6 web proxy destination.	<i>disable</i>	Disable allowing an IPv6 web proxy destination.			
Option	Description									
<i>enable</i>	Enable allowing an IPv6 web proxy destination.									
<i>disable</i>	Disable allowing an IPv6 web proxy destination.									
incoming-ip6	Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::						
outgoing-ip6	Outgoing HTTP requests will leave this IPv6. Multiple interfaces can be specified. Interfaces must have these IPv6 addresses.	ipv6-address	Not Specified							
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable strict guest user checking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable strict guest user checking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strict guest user checking.	<i>disable</i>	Disable strict guest user checking.			
Option	Description									
<i>enable</i>	Enable strict guest user checking.									
<i>disable</i>	Disable strict guest user checking.									
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server .	option	-	ipv4						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Prefer the IPv4 DNS server.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Prefer the IPv6 DNS server.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	Prefer the IPv4 DNS server.	<i>ipv6</i>	Prefer the IPv6 DNS server.			
Option	Description									
<i>ipv4</i>	Prefer the IPv4 DNS server.									
<i>ipv6</i>	Prefer the IPv6 DNS server.									
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>reject</i></td> <td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td> </tr> </tbody> </table>	Option	Description	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.					
Option	Description									
<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.									

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td> </tr> <tr> <td><i>best-effort</i></td> <td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.			
Option	Description									
<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.									
<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.									
realm	Authentication realm used to identify the explicit web proxy (maximum of 63 characters).	string	Maximum length: 63	default						
sec-default-action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>accept</i></td> <td>Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny requests unless there is a matching explicit web proxy policy.</td> </tr> </tbody> </table>	Option	Description	<i>accept</i>	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.	<i>deny</i>	Deny requests unless there is a matching explicit web proxy policy.			
Option	Description									
<i>accept</i>	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.									
<i>deny</i>	Deny requests unless there is a matching explicit web proxy policy.									
https-replacement-message	Enable/disable sending the client a replacement message for HTTPS requests.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display a replacement message for HTTPS requests.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display a replacement message for HTTPS requests.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display a replacement message for HTTPS requests.	<i>disable</i>	Do not display a replacement message for HTTPS requests.			
Option	Description									
<i>enable</i>	Display a replacement message for HTTPS requests.									
<i>disable</i>	Do not display a replacement message for HTTPS requests.									
message-upon-server-error	Enable/disable displaying a replacement message when a server error is detected.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Display a replacement message when a server error is detected.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not display a replacement message when a server error is detected.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Display a replacement message when a server error is detected.	<i>disable</i>	Do not display a replacement message when a server error is detected.			
Option	Description									
<i>enable</i>	Display a replacement message when a server error is detected.									
<i>disable</i>	Do not display a replacement message when a server error is detected.									
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Proxy Auto-Configuration (PAC).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Proxy Auto-Configuration (PAC).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Proxy Auto-Configuration (PAC).	<i>disable</i>	Disable Proxy Auto-Configuration (PAC).			
Option	Description									
<i>enable</i>	Enable Proxy Auto-Configuration (PAC).									
<i>disable</i>	Disable Proxy Auto-Configuration (PAC).									

Parameter	Description	Type	Size	Default								
pac-file-url	PAC file access URL.	user	Not Specified									
pac-file-server-port	Port number that PAC traffic from client web browsers uses to connect to the explicit web proxy .	user	Not Specified									
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac								
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified									
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-	low								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>high</i></td> <td>High encryption. Allow only AES and ChaCha.</td> </tr> <tr> <td><i>medium</i></td> <td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td> </tr> <tr> <td><i>low</i></td> <td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td> </tr> </tbody> </table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
Option	Description											
<i>high</i>	High encryption. Allow only AES and ChaCha.											
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable logging timed-out authentication requests.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable logging timed-out authentication requests.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging timed-out authentication requests.	<i>disable</i>	Disable logging timed-out authentication requests.					
Option	Description											
<i>enable</i>	Enable logging timed-out authentication requests.											
<i>disable</i>	Disable logging timed-out authentication requests.											

### config pac-policy

Parameter	Description	Type	Size	Default						
status	Enable/disable policy.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable policy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable policy.	<i>disable</i>	Disable policy.			
Option	Description									
<i>enable</i>	Enable policy.									
<i>disable</i>	Disable policy.									
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79							
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
comments	Optional comments.	var-string	Maximum length: 1023	

## config web-proxy forward-server

Configure forward-server addresses.

```

config web-proxy forward-server
  Description: Configure forward-server addresses.
  edit <name>
    set addr-type [ip|fqdn]
    set ip {ipv4-address-any}
    set fqdn {string}
    set port {integer}
    set healthcheck [disable|enable]
    set monitor {string}
    set server-down-option [block|pass]
    set username {string}
    set password {password}
    set comment {string}
  next
end

```

## config web-proxy forward-server

Parameter	Description	Type	Size	Default						
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ip</i></td> <td>Use an IP address for the forwarding proxy server.</td> </tr> <tr> <td><i>fqdn</i></td> <td>Use the FQDN for the forwarding proxy server.</td> </tr> </tbody> </table>	Option	Description	<i>ip</i>	Use an IP address for the forwarding proxy server.	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.			
Option	Description									
<i>ip</i>	Use an IP address for the forwarding proxy server.									
<i>fqdn</i>	Use the FQDN for the forwarding proxy server.									
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0						
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255							

Parameter	Description	Type	Size	Default						
port	Port number that the forwarding server expects to receive HTTP sessions on .	integer	Minimum value: 1 Maximum value: 65535	3128						
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable health checking.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable health checking.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable health checking.	<i>enable</i>	Enable health checking.			
Option	Description									
<i>disable</i>	Disable health checking.									
<i>enable</i>	Enable health checking.									
monitor	URL for forward server health check monitoring .	string	Maximum length: 255	http://www.google.com						
server-down-option	Action to take when the forward server is found to be down: block sessions until the server is back up or pass sessions to their destination.	option	-	block						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block sessions until the server is back up.</td> </tr> <tr> <td><i>pass</i></td> <td>Pass sessions to their destination bypassing the forward server.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block sessions until the server is back up.	<i>pass</i>	Pass sessions to their destination bypassing the forward server.			
Option	Description									
<i>block</i>	Block sessions until the server is back up.									
<i>pass</i>	Pass sessions to their destination bypassing the forward server.									
username	HTTP authentication user name.	string	Maximum length: 64							
password	HTTP authentication password.	password	Not Specified							
comment	Comment.	string	Maximum length: 63							

## config web-proxy forward-server-group

Configure a forward server group consisting or multiple forward servers. Supports failover and load balancing.

```

config web-proxy forward-server-group
  Description: Configure a forward server group consisting or multiple forward servers.
              Supports failover and load balancing.
  edit <name>
    set affinity [enable|disable]
    set ldb-method [weighted|least-session|...]
    set group-down-option [block|pass]
    config server-list

```

```

Description: Add web forward servers to a list to form a server group. Optionally
            assign weights to each server.
edit <name>
    set weight {integer}
next
end
next
end

```

## config web-proxy forward-server-group

Parameter	Description	Type	Size	Default								
affinity	Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the forward-server-affinity-timeout is reached (under web-proxy global).	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable affinity.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable affinity.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable affinity.	<i>disable</i>	Disable affinity.					
Option	Description											
<i>enable</i>	Enable affinity.											
<i>disable</i>	Disable affinity.											
ldb-method	Load balance method: weighted or least-session.	option	-	weighted								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>weighted</i></td> <td>Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.</td> </tr> <tr> <td><i>least-session</i></td> <td>Send new sessions to the server with lowest session count.</td> </tr> <tr> <td><i>active-passive</i></td> <td>Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.</td> </tr> </tbody> </table>	Option	Description	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.	<i>least-session</i>	Send new sessions to the server with lowest session count.	<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.			
Option	Description											
<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.											
<i>least-session</i>	Send new sessions to the server with lowest session count.											
<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.											
group-down-option	Action to take when all of the servers in the forward server group are down: block sessions until at least one server is back up or pass sessions to their destination.	option	-	block								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block sessions until at least one server in the group is back up.</td> </tr> <tr> <td><i>pass</i></td> <td>Pass sessions to their destination bypassing servers in the forward server group.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block sessions until at least one server in the group is back up.	<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.					
Option	Description											
<i>block</i>	Block sessions until at least one server in the group is back up.											
<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.											

## config server-list

Parameter	Description	Type	Size	Default
weight	Optionally assign a weight of the forwarding server for weighted load balancing	integer	Minimum value: 1 Maximum value: 100	10

## config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
  Description: Configure debug URL addresses.
  edit <name>
    set url-pattern {string}
    set status [enable|disable]
    set exact [enable|disable]
  next
end
```

## config web-proxy debug-url

Parameter	Description	Type	Size	Default						
url-pattern	URL exemption pattern.	string	Maximum length: 511							
status	Enable/disable this URL exemption.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable this URL exemption.</td></tr><tr><td><i>disable</i></td><td>Disable this URL exemption.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable this URL exemption.	<i>disable</i>	Disable this URL exemption.			
Option	Description									
<i>enable</i>	Enable this URL exemption.									
<i>disable</i>	Disable this URL exemption.									
exact	Enable/disable matching the exact path.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable matching the exact path.</td></tr><tr><td><i>disable</i></td><td>Disable matching the exact path.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable matching the exact path.	<i>disable</i>	Disable matching the exact path.			
Option	Description									
<i>enable</i>	Enable matching the exact path.									
<i>disable</i>	Disable matching the exact path.									

## config web-proxy wisp

Configure Wireless Internet service provider (WISP) servers.

```
config web-proxy wisp
  Description: Configure Wireless Internet service provider (WISP) servers.
  edit <name>
```



```

    set comment {var-string}
    set outgoing-ip {ipv4-address-any}
    set server-ip {ipv4-address-any}
    set server-port {integer}
    set max-connections {integer}
    set timeout {integer}
  next
end

```

## config web-proxy wisp

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
outgoing-ip	WISP outgoing IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-ip	WISP server IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-port	WISP server port .	integer	Minimum value: 1 Maximum value: 65535	15868
max-connections	Maximum number of web proxy WISP connections .	integer	Minimum value: 4 Maximum value: 4096	64
timeout	Period of time before WISP requests time out .	integer	Minimum value: 1 Maximum value: 15	5

## config web-proxy url-match

Exempt URLs from web proxy forwarding and caching.

```

config web-proxy url-match
  Description: Exempt URLs from web proxy forwarding and caching.
  edit <name>
    set status [enable|disable]
    set url-pattern {string}
    set forward-server {string}
    set cache-exemption [enable|disable]
    set comment {var-string}
  next
end

```

## config web-proxy url-match

Parameter	Description	Type	Size	Default						
status	Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding and caching.	option	-	enable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable exempting the matching URLs.</td></tr><tr><td><i>disable</i></td><td>Disable exempting the matching URLs.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable exempting the matching URLs.	<i>disable</i>	Disable exempting the matching URLs.			
Option	Description									
<i>enable</i>	Enable exempting the matching URLs.									
<i>disable</i>	Disable exempting the matching URLs.									
url-pattern	URL pattern to be exempted from web proxy forwarding and caching.	string	Maximum length: 511							
forward-server	Forward server name.	string	Maximum length: 63							
cache-exemption	Enable/disable exempting this URL pattern from caching.	option	-	disable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable exempting this URL pattern from caching.</td></tr><tr><td><i>disable</i></td><td>Disable exempting this URL pattern from caching.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable exempting this URL pattern from caching.	<i>disable</i>	Disable exempting this URL pattern from caching.			
Option	Description									
<i>enable</i>	Enable exempting this URL pattern from caching.									
<i>disable</i>	Disable exempting this URL pattern from caching.									
comment	Comment.	var-string	Maximum length: 255							

## webfilter

This section includes syntax for the following commands:

- [config webfilter status on page 1416](#)
- [config webfilter profile on page 1395](#)
- [config webfilter override-usr on page 1417](#)
- [config webfilter fortiguard on page 1411](#)
- [config webfilter content on page 1388](#)
- [config webfilter ips-urlfilter-setting6 on page 1394](#)
- [config webfilter ftgd-statistics on page 1416](#)
- [config webfilter content-header on page 1389](#)
- [config webfilter ips-urlfilter-setting on page 1393](#)
- [config webfilter search-engine on page 1415](#)
- [config webfilter ftgd-local-cat on page 1387](#)
- [config webfilter ftgd-local-rating on page 1414](#)
- [config webfilter categories on page 1413](#)
- [config webfilter ips-urlfilter-cache-setting on page 1394](#)
- [config webfilter urlfilter on page 1390](#)
- [config webfilter override on page 1413](#)

### config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

```
config webfilter ftgd-local-cat
  Description: Configure FortiGuard Web Filter local categories.
  edit <desc>
    set status [enable|disable]
    set id {integer}
  next
end
```

### config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default						
status	Enable/disable the local category.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable the local category.</td></tr><tr><td><i>disable</i></td><td>Disable the local category.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable the local category.	<i>disable</i>	Disable the local category.			
Option	Description									
<i>enable</i>	Enable the local category.									
<i>disable</i>	Disable the local category.									

Parameter	Description	Type	Size	Default
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0

## config webfilter content

Configure Web filter banned word table.

```
config webfilter content
  Description: Configure Web filter banned word table.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Configure banned word entries.
      edit <name>
        set pattern-type [wildcard|regexp]
        set status [enable|disable]
        set lang [western|simch|...]
        set score {integer}
        set action [block|exempt]
      next
    end
  next
end
```

## config webfilter content

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard
	<b>Option</b>	<b>Description</b>		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regexp</i>	Perl regular expression.		

Parameter	Description	Type	Size	Default																				
status	Enable/disable banned word.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
lang	Language of banned word.	option	-	western																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>western</i></td> <td>Western.</td> </tr> <tr> <td><i>simch</i></td> <td>Simplified Chinese.</td> </tr> <tr> <td><i>trach</i></td> <td>Traditional Chinese.</td> </tr> <tr> <td><i>japanese</i></td> <td>Japanese.</td> </tr> <tr> <td><i>korean</i></td> <td>Korean.</td> </tr> <tr> <td><i>french</i></td> <td>French.</td> </tr> <tr> <td><i>thai</i></td> <td>Thai.</td> </tr> <tr> <td><i>spanish</i></td> <td>Spanish.</td> </tr> <tr> <td><i>cyrillic</i></td> <td>Cyrillic.</td> </tr> </tbody> </table>	Option	Description	<i>western</i>	Western.	<i>simch</i>	Simplified Chinese.	<i>trach</i>	Traditional Chinese.	<i>japanese</i>	Japanese.	<i>korean</i>	Korean.	<i>french</i>	French.	<i>thai</i>	Thai.	<i>spanish</i>	Spanish.	<i>cyrillic</i>	Cyrillic.			
Option	Description																							
<i>western</i>	Western.																							
<i>simch</i>	Simplified Chinese.																							
<i>trach</i>	Traditional Chinese.																							
<i>japanese</i>	Japanese.																							
<i>korean</i>	Korean.																							
<i>french</i>	French.																							
<i>thai</i>	Thai.																							
<i>spanish</i>	Spanish.																							
<i>cyrillic</i>	Cyrillic.																							
score	Score, to be applied every time the word appears on a web page .	integer	Minimum value: 0 Maximum value: 4294967295	10																				
action	Block or exempt word when a match is found.	option	-	block																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block matches.</td> </tr> <tr> <td><i>exempt</i></td> <td>Exempt matches.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block matches.	<i>exempt</i>	Exempt matches.																	
Option	Description																							
<i>block</i>	Block matches.																							
<i>exempt</i>	Exempt matches.																							

## config webfilter content-header

Configure content types used by Web filter.

```

config webfilter content-header
  Description: Configure content types used by Web filter.
  edit <id>
    set name {string}
    set comment {var-string}
  config entries
    Description: Configure content types used by web filter.

```

```

        edit <pattern>
            set action [block|allow|...]
            set category {user}
        next
    end
next
end

```

## config webfilter content-header

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

## config entries

Parameter	Description	Type	Size	Default								
action	Action to take for this content type.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block content type.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow content type.</td> </tr> <tr> <td><i>exempt</i></td> <td>Exempt content type.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block content type.	<i>allow</i>	Allow content type.	<i>exempt</i>	Exempt content type.			
Option	Description											
<i>block</i>	Block content type.											
<i>allow</i>	Allow content type.											
<i>exempt</i>	Exempt content type.											
category	Categories that this content type applies to.	user	Not Specified	all								

## config webfilter urlfilter

Configure URL filter lists.

```

config webfilter urlfilter
    Description: Configure URL filter lists.
    edit <id>
        set name {string}
        set comment {var-string}
        set one-arm-ips-urlfilter [enable|disable]
        set ip-addr-block [enable|disable]
        config entries
            Description: URL filter entries.
            edit <id>
                set url {string}
                set type [simple|regex|...]
                set action [exempt|block|...]
                set antiphish-action [block|log]
                set status [enable|disable]
            end
        end
    end
end

```

```

    set exempt {option1}, {option2}, ...
    set web-proxy-profile {string}
    set referrer-host {string}
    set dns-address-family [ipv4|ipv6|...]
  next
end
next
end

```

## config webfilter urlfilter

Parameter	Description	Type	Size	Default
name	Name of URL filter list.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.		
	<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.		
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.		
	<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.		

## config entries

Parameter	Description	Type	Size	Default
url	URL to be filtered.	string	Maximum length: 511	
type	Filter type (simple, regex, or wildcard).	option	-	simple
	<b>Option</b>	<b>Description</b>		
	<i>simple</i>	Simple URL string.		
	<i>regex</i>	Regular expression URL string.		
	<i>wildcard</i>	Wildcard URL string.		

Parameter	Description	Type	Size	Default														
action	Action to take for URL filter matches.	option	-	exempt														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exempt</i></td> <td>Exempt matches.</td> </tr> <tr> <td><i>block</i></td> <td>Block matches.</td> </tr> <tr> <td><i>allow</i></td> <td>Allow matches (no log).</td> </tr> <tr> <td><i>monitor</i></td> <td>Allow matches (with log).</td> </tr> </tbody> </table>	Option	Description	<i>exempt</i>	Exempt matches.	<i>block</i>	Block matches.	<i>allow</i>	Allow matches (no log).	<i>monitor</i>	Allow matches (with log).							
Option	Description																	
<i>exempt</i>	Exempt matches.																	
<i>block</i>	Block matches.																	
<i>allow</i>	Allow matches (no log).																	
<i>monitor</i>	Allow matches (with log).																	
antiphish-action	Action to take for AntiPhishing matches.	option	-	block														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block matches.</td> </tr> <tr> <td><i>log</i></td> <td>Allow matches with log.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block matches.	<i>log</i>	Allow matches with log.											
Option	Description																	
<i>block</i>	Block matches.																	
<i>log</i>	Allow matches with log.																	
status	Enable/disable this URL filter.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable this URL filter.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable this URL filter.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable this URL filter.	<i>disable</i>	Disable this URL filter.											
Option	Description																	
<i>enable</i>	Enable this URL filter.																	
<i>disable</i>	Disable this URL filter.																	
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>av</i></td> <td>AntiVirus scanning.</td> </tr> <tr> <td><i>web-content</i></td> <td>Web filter content matching.</td> </tr> <tr> <td><i>activex-java-cookie</i></td> <td>ActiveX, Java, and cookie filtering.</td> </tr> <tr> <td><i>dlp</i></td> <td>DLP scanning.</td> </tr> <tr> <td><i>fortiguard</i></td> <td>FortiGuard web filtering.</td> </tr> <tr> <td><i>range-block</i></td> <td>Range block feature.</td> </tr> </tbody> </table>	Option	Description	<i>av</i>	AntiVirus scanning.	<i>web-content</i>	Web filter content matching.	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.	<i>dlp</i>	DLP scanning.	<i>fortiguard</i>	FortiGuard web filtering.	<i>range-block</i>	Range block feature.			
Option	Description																	
<i>av</i>	AntiVirus scanning.																	
<i>web-content</i>	Web filter content matching.																	
<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.																	
<i>dlp</i>	DLP scanning.																	
<i>fortiguard</i>	FortiGuard web filtering.																	
<i>range-block</i>	Range block feature.																	



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>pass</i></td> <td>Pass single connection from all.</td> </tr> <tr> <td><i>antiphish</i></td> <td>AntiPhish credential checking.</td> </tr> <tr> <td><i>all</i></td> <td>Exempt from all security profiles.</td> </tr> </tbody> </table>	Option	Description	<i>pass</i>	Pass single connection from all.	<i>antiphish</i>	AntiPhish credential checking.	<i>all</i>	Exempt from all security profiles.			
Option	Description											
<i>pass</i>	Pass single connection from all.											
<i>antiphish</i>	AntiPhish credential checking.											
<i>all</i>	Exempt from all security profiles.											
web-proxy-profile	Web proxy profile.	string	Maximum length: 63									
referrer-host	Referrer host name.	string	Maximum length: 255									
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv4</i></td> <td>Resolve IPv4 address from DNS server.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Resolve IPv6 address from DNS server.</td> </tr> <tr> <td><i>both</i></td> <td>Resolve both IPv4 and IPv6 addresses from DNS server.</td> </tr> </tbody> </table>	Option	Description	<i>ipv4</i>	Resolve IPv4 address from DNS server.	<i>ipv6</i>	Resolve IPv6 address from DNS server.	<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.			
Option	Description											
<i>ipv4</i>	Resolve IPv4 address from DNS server.											
<i>ipv6</i>	Resolve IPv6 address from DNS server.											
<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.											

## config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

```
config webfilter ips-urlfilter-setting
  Description: Configure IPS URL filter settings.
  set device {string}
  set distance {integer}
  set gateway {ipv4-address}
  set geo-filter {var-string}
end
```

## config webfilter ips-urlfilter-setting

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway	Gateway IP address for this route.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

## config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

```
config webfilter ips-urlfilter-setting6
  Description: Configure IPS URL filter settings for IPv6.
  set device {string}
  set distance {integer}
  set gateway6 {ipv6-address}
  set geo-filter {var-string}
end
```

## config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway6	Gateway IPv6 address for this route.	ipv6-address	Not Specified	::
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IPv6 address belongs to the country in the filter.	var-string	Maximum length: 255	

## config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

```
config webfilter ips-urlfilter-cache-setting
  Description: Configure IPS URL filter cache settings.
  set dns-retry-interval {integer}
  set extended-ttl {integer}
end
```

## config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. 0 means use DNS server's TTL	integer	Minimum value: 0 Maximum value: 2147483	0

## config webfilter profile

Configure Web filter profiles.

```
config webfilter profile
  Description: Configure Web filter profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    set options {option1}, {option2}, ...
    set https-replacemsg [enable|disable]
    set ovr-d-perm {option1}, {option2}, ...
    set post-action [normal|block]
  config override
    Description: Web Filter override settings.
    set ovr-d-cookie [allow|deny]
    set ovr-d-scope [user|user-group|...]
    set profile-type [list|radius]
    set ovr-d-dur-mode [constant|ask]
    set ovr-d-dur {user}
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set ovr-d-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
  end
  config web
    Description: Web content filtering settings.
    set bword-threshold {integer}
    set bword-table {integer}
    set urlfilter-table {integer}
    set content-header-list {integer}
    set blacklist [enable|disable]
    set whitelist {option1}, {option2}, ...
    set safe-search {option1}, {option2}, ...
    set youtube-restrict [none|strict|...]
    set log-search [enable|disable]
    set keyword-match <pattern1>, <pattern2>, ...
  end
```

```

set youtube-channel-status [disable|blacklist|...]
config youtube-channel-filter
  Description: YouTube channel filter.
  edit <id>
    set channel-id {string}
    set comment {var-string}
  next
end
config ftgd-wf
  Description: FortiGuard Web Filter settings.
  set options {option1}, {option2}, ...
  set exempt-quota {user}
  set ovrd {user}
  config filters
    Description: FortiGuard filters.
    edit <id>
      set category {integer}
      set action [block|authenticate|...]
      set warn-duration {user}
      set auth-usr-grp <name1>, <name2>, ...
      set log [enable|disable]
      set override-replacemsg {string}
      set warning-prompt [per-domain|per-category]
      set warning-duration-type [session|timeout]
    next
  end
  config quota
    Description: FortiGuard traffic quota settings.
    edit <id>
      set category {user}
      set type [time|traffic]
      set unit [B|KB|...]
      set value {integer}
      set duration {user}
      set override-replacemsg {string}
    next
  end
  set max-quota-timeout {integer}
  set rate-javascript-urls [disable|enable]
  set rate-css-urls [disable|enable]
  set rate-crl-urls [disable|enable]
end
config antiphish
  Description: AntiPhishing profile.
  set status [enable|disable]
  set domain-controller {string}
  set default-action [exempt|log|...]
  set check-uri [enable|disable]
  set check-basic-auth [enable|disable]
  set check-username-only [enable|disable]
  set max-body-len {integer}
  config inspection-entries
    Description: AntiPhishing entries.
    edit <name>
      set fortiguard-category {user}
      set action [exempt|log|...]
    next

```

```

end
config custom-patterns
  Description: Custom username and password regex patterns.
  edit <pattern>
    set category [username|password]
  next
end
end
set wisp [enable|disable]
set wisp-servers <name1>, <name2>, ...
set wisp-algorithm [primary-secondary|round-robin|...]
set log-all-url [enable|disable]
set web-content-log [enable|disable]
set web-filter-activex-log [enable|disable]
set web-filter-command-block-log [enable|disable]
set web-filter-cookie-log [enable|disable]
set web-filter-applet-log [enable|disable]
set web-filter-jscript-log [enable|disable]
set web-filter-js-log [enable|disable]
set web-filter-vbs-log [enable|disable]
set web-filter-unknown-log [enable|disable]
set web-filter-referer-log [enable|disable]
set web-filter-cookie-removal-log [enable|disable]
set web-url-log [enable|disable]
set web-invalid-domain-log [enable|disable]
set web-ftgd-err-log [enable|disable]
set web-ftgd-quota-usage [enable|disable]
set extended-log [enable|disable]
set web-extended-all-action-log [enable|disable]
set web-antiphishing-log [enable|disable]
next
end

```

## config webfilter profile

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
feature-set	Flow/proxy feature set.	option	-	flow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>flow</i></td> <td>Flow feature set.</td> </tr> <tr> <td><i>proxy</i></td> <td>Proxy feature set.</td> </tr> </tbody> </table>	Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.			
Option	Description									
<i>flow</i>	Flow feature set.									
<i>proxy</i>	Proxy feature set.									
replacemsg-group	Replacement message group.	string	Maximum length: 35							
options	Options.	option	-							

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>activexfilter</i></td> <td>ActiveX filter.</td> </tr> <tr> <td><i>cookiefilter</i></td> <td>Cookie filter.</td> </tr> <tr> <td><i>javafilter</i></td> <td>Java applet filter.</td> </tr> <tr> <td><i>block-invalid-url</i></td> <td>Block sessions contained an invalid domain name.</td> </tr> <tr> <td><i>jscript</i></td> <td>Javascript block.</td> </tr> <tr> <td><i>js</i></td> <td>JS block.</td> </tr> <tr> <td><i>vbs</i></td> <td>VB script block.</td> </tr> <tr> <td><i>unknown</i></td> <td>Unknown script block.</td> </tr> <tr> <td><i>intrinsic</i></td> <td>Intrinsic script block.</td> </tr> <tr> <td><i>wf-referer</i></td> <td>Referring block.</td> </tr> <tr> <td><i>wf-cookie</i></td> <td>Cookie block.</td> </tr> </tbody> </table>	Option	Description	<i>activexfilter</i>	ActiveX filter.	<i>cookiefilter</i>	Cookie filter.	<i>javafilter</i>	Java applet filter.	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.	<i>jscript</i>	Javascript block.	<i>js</i>	JS block.	<i>vbs</i>	VB script block.	<i>unknown</i>	Unknown script block.	<i>intrinsic</i>	Intrinsic script block.	<i>wf-referer</i>	Referring block.	<i>wf-cookie</i>	Cookie block.			
Option	Description																											
<i>activexfilter</i>	ActiveX filter.																											
<i>cookiefilter</i>	Cookie filter.																											
<i>javafilter</i>	Java applet filter.																											
<i>block-invalid-url</i>	Block sessions contained an invalid domain name.																											
<i>jscript</i>	Javascript block.																											
<i>js</i>	JS block.																											
<i>vbs</i>	VB script block.																											
<i>unknown</i>	Unknown script block.																											
<i>intrinsic</i>	Intrinsic script block.																											
<i>wf-referer</i>	Referring block.																											
<i>wf-cookie</i>	Cookie block.																											
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
Option	Description																											
<i>enable</i>	Enable setting.																											
<i>disable</i>	Disable setting.																											
ovrd-perm	Permitted override types.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bannedword-override</i></td> <td>Banned word override.</td> </tr> <tr> <td><i>urlfilter-override</i></td> <td>URL filter override.</td> </tr> <tr> <td><i>fortiguard-wf-override</i></td> <td>FortiGuard Web Filter override.</td> </tr> <tr> <td><i>contenttype-check-override</i></td> <td>Content-type header override.</td> </tr> </tbody> </table>	Option	Description	<i>bannedword-override</i>	Banned word override.	<i>urlfilter-override</i>	URL filter override.	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.	<i>contenttype-check-override</i>	Content-type header override.																	
Option	Description																											
<i>bannedword-override</i>	Banned word override.																											
<i>urlfilter-override</i>	URL filter override.																											
<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.																											
<i>contenttype-check-override</i>	Content-type header override.																											
post-action	Action taken for HTTP POST traffic.	option	-	normal																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>normal</i></td> <td>Normal, POST requests are allowed.</td> </tr> <tr> <td><i>block</i></td> <td>POST requests are blocked.</td> </tr> </tbody> </table>	Option	Description	<i>normal</i>	Normal, POST requests are allowed.	<i>block</i>	POST requests are blocked.																					
Option	Description																											
<i>normal</i>	Normal, POST requests are allowed.																											
<i>block</i>	POST requests are blocked.																											

Parameter	Description	Type	Size	Default								
youtube-channel-status	YouTube channel filter status.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable YouTube channel filter.</td> </tr> <tr> <td><i>blacklist</i></td> <td>Block matches.</td> </tr> <tr> <td><i>whitelist</i></td> <td>Allow matches.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable YouTube channel filter.	<i>blacklist</i>	Block matches.	<i>whitelist</i>	Allow matches.			
Option	Description											
<i>disable</i>	Disable YouTube channel filter.											
<i>blacklist</i>	Block matches.											
<i>whitelist</i>	Allow matches.											
wisp	Enable/disable web proxy WISP.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable web proxy WISP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable web proxy WISP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable web proxy WISP.	<i>disable</i>	Disable web proxy WISP.					
Option	Description											
<i>enable</i>	Enable web proxy WISP.											
<i>disable</i>	Disable web proxy WISP.											
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79									
wisp-algorithm	WISP server selection algorithm.	option	-	auto-learning								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>primary-secondary</i></td> <td>Select the first healthy server in order.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Select the next healthy server.</td> </tr> <tr> <td><i>auto-learning</i></td> <td>Select the lightest loading healthy server.</td> </tr> </tbody> </table>	Option	Description	<i>primary-secondary</i>	Select the first healthy server in order.	<i>round-robin</i>	Select the next healthy server.	<i>auto-learning</i>	Select the lightest loading healthy server.			
Option	Description											
<i>primary-secondary</i>	Select the first healthy server in order.											
<i>round-robin</i>	Select the next healthy server.											
<i>auto-learning</i>	Select the lightest loading healthy server.											
log-all-url	Enable/disable logging all URLs visited.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
web-content-log	Enable/disable logging logging blocked web content.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
web-filter-activex-log	Enable/disable logging ActiveX.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-applet-log	Enable/disable logging Java applets.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-jscript-log	Enable/disable logging JScripts.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-js-log	Enable/disable logging Java scripts.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-	enable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-referer-log	Enable/disable logging referrers.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-url-log	Enable/disable logging URL filtering.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
extended-log	Enable/disable extended logging for web filtering.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-antiphishing-log	Enable/disable logging of AntiPhishing checks.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

### config override

Parameter	Description	Type	Size	Default						
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow browser-based (cookie) override.</td> </tr> <tr> <td><i>deny</i></td> <td>Deny browser-based (cookie) override.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow browser-based (cookie) override.	<i>deny</i>	Deny browser-based (cookie) override.			
Option	Description									
<i>allow</i>	Allow browser-based (cookie) override.									
<i>deny</i>	Deny browser-based (cookie) override.									

Parameter	Description	Type	Size	Default																
ovrd-scope	Override scope.	option	-	user																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>user</i></td> <td>Override for the user.</td> </tr> <tr> <td><i>user-group</i></td> <td>Override for the user's group.</td> </tr> <tr> <td><i>ip</i></td> <td>Override for the initiating IP.</td> </tr> <tr> <td><i>browser</i></td> <td>Create browser-based (cookie) override.</td> </tr> <tr> <td><i>ask</i></td> <td>Prompt for scope when initiating an override.</td> </tr> </tbody> </table>	Option	Description	<i>user</i>	Override for the user.	<i>user-group</i>	Override for the user's group.	<i>ip</i>	Override for the initiating IP.	<i>browser</i>	Create browser-based (cookie) override.	<i>ask</i>	Prompt for scope when initiating an override.							
Option	Description																			
<i>user</i>	Override for the user.																			
<i>user-group</i>	Override for the user's group.																			
<i>ip</i>	Override for the initiating IP.																			
<i>browser</i>	Create browser-based (cookie) override.																			
<i>ask</i>	Prompt for scope when initiating an override.																			
profile-type	Override profile type.	option	-	list																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>list</i></td> <td>Profile chosen from list.</td> </tr> <tr> <td><i>radius</i></td> <td>Profile determined by RADIUS server.</td> </tr> </tbody> </table>	Option	Description	<i>list</i>	Profile chosen from list.	<i>radius</i>	Profile determined by RADIUS server.													
Option	Description																			
<i>list</i>	Profile chosen from list.																			
<i>radius</i>	Profile determined by RADIUS server.																			
ovrd-dur-mode	Override duration mode.	option	-	constant																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>constant</i></td> <td>Constant mode.</td> </tr> <tr> <td><i>ask</i></td> <td>Prompt for duration when initiating an override.</td> </tr> </tbody> </table>	Option	Description	<i>constant</i>	Constant mode.	<i>ask</i>	Prompt for duration when initiating an override.													
Option	Description																			
<i>constant</i>	Constant mode.																			
<i>ask</i>	Prompt for duration when initiating an override.																			
ovrd-dur	Override duration.	user	Not Specified	15m																
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>User-Name</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Address</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IP-Netmask</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Filter-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-IP-Host</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Reply-Message</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.			
Option	Description																			
<i>User-Name</i>	Use this attribute.																			
<i>NAS-IP-Address</i>	Use this attribute.																			
<i>Framed-IP-Address</i>	Use this attribute.																			
<i>Framed-IP-Netmask</i>	Use this attribute.																			
<i>Filter-Id</i>	Use this attribute.																			
<i>Login-IP-Host</i>	Use this attribute.																			
<i>Reply-Message</i>	Use this attribute.																			

Parameter	Description	Type	Size	Default																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>Callback-Number</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Callback-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-Route</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-IPX-Network</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Class</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Called-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Calling-Station-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>NAS-Identifier</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Proxy-State</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Service</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Node</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Login-LAT-Group</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Framed-AppleTalk-Zone</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Session-Id</i></td> <td>Use this attribute.</td> </tr> <tr> <td><i>Acct-Multi-Session-Id</i></td> <td>Use this attribute.</td> </tr> </tbody> </table>	Option	Description	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.			
Option	Description																																			
<i>Callback-Number</i>	Use this attribute.																																			
<i>Callback-Id</i>	Use this attribute.																																			
<i>Framed-Route</i>	Use this attribute.																																			
<i>Framed-IPX-Network</i>	Use this attribute.																																			
<i>Class</i>	Use this attribute.																																			
<i>Called-Station-Id</i>	Use this attribute.																																			
<i>Calling-Station-Id</i>	Use this attribute.																																			
<i>NAS-Identifier</i>	Use this attribute.																																			
<i>Proxy-State</i>	Use this attribute.																																			
<i>Login-LAT-Service</i>	Use this attribute.																																			
<i>Login-LAT-Node</i>	Use this attribute.																																			
<i>Login-LAT-Group</i>	Use this attribute.																																			
<i>Framed-AppleTalk-Zone</i>	Use this attribute.																																			
<i>Acct-Session-Id</i>	Use this attribute.																																			
<i>Acct-Multi-Session-Id</i>	Use this attribute.																																			
ovrd-user-group <name>	User groups with permission to use the override. User group name.	string	Maximum length: 79																																	
profile <name>	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79																																	

## config web

Parameter	Description	Type	Size	Default
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10

Parameter	Description	Type	Size	Default														
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0														
urfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0														
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0														
blacklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blacklist.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
Option	Description																	
<i>enable</i>	Enable setting.																	
<i>disable</i>	Disable setting.																	
whitelist	FortiGuard whitelist settings.	option	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exempt-av</i></td> <td>Exempt antivirus.</td> </tr> <tr> <td><i>exempt-webcontent</i></td> <td>Exempt web content.</td> </tr> <tr> <td><i>exempt-activex-java-cookie</i></td> <td>Exempt ActiveX-JAVA-Cookie.</td> </tr> <tr> <td><i>exempt-dlp</i></td> <td>Exempt DLP.</td> </tr> <tr> <td><i>exempt-rangeblock</i></td> <td>Exempt RangeBlock.</td> </tr> <tr> <td><i>extended-log-others</i></td> <td>Support extended log.</td> </tr> </tbody> </table>	Option	Description	<i>exempt-av</i>	Exempt antivirus.	<i>exempt-webcontent</i>	Exempt web content.	<i>exempt-activex-java-cookie</i>	Exempt ActiveX-JAVA-Cookie.	<i>exempt-dlp</i>	Exempt DLP.	<i>exempt-rangeblock</i>	Exempt RangeBlock.	<i>extended-log-others</i>	Support extended log.			
Option	Description																	
<i>exempt-av</i>	Exempt antivirus.																	
<i>exempt-webcontent</i>	Exempt web content.																	
<i>exempt-activex-java-cookie</i>	Exempt ActiveX-JAVA-Cookie.																	
<i>exempt-dlp</i>	Exempt DLP.																	
<i>exempt-rangeblock</i>	Exempt RangeBlock.																	
<i>extended-log-others</i>	Support extended log.																	
safe-search	Safe search type.	option	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>url</i></td> <td>Insert safe search string into URL.</td> </tr> </tbody> </table>	Option	Description	<i>url</i>	Insert safe search string into URL.													
Option	Description																	
<i>url</i>	Insert safe search string into URL.																	

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>header</i></td> <td>Insert safe search header.</td> </tr> </tbody> </table>	Option	Description	<i>header</i>	Insert safe search header.							
Option	Description											
<i>header</i>	Insert safe search header.											
youtube-restrict	YouTube EDU filter level.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>none</i></td> <td>Full access for YouTube.</td> </tr> <tr> <td><i>strict</i></td> <td>Strict access for YouTube.</td> </tr> <tr> <td><i>moderate</i></td> <td>Moderate access for YouTube.</td> </tr> </tbody> </table>	Option	Description	<i>none</i>	Full access for YouTube.	<i>strict</i>	Strict access for YouTube.	<i>moderate</i>	Moderate access for YouTube.			
Option	Description											
<i>none</i>	Full access for YouTube.											
<i>strict</i>	Strict access for YouTube.											
<i>moderate</i>	Moderate access for YouTube.											
log-search	Enable/disable logging all search phrases.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79									

### config youtube-channel-filter

Parameter	Description	Type	Size	Default
channel-id	YouTube channel ID to be filtered.	string	Maximum length: 255	
comment	Comment.	var-string	Maximum length: 255	

### config ftgd-wf

Parameter	Description	Type	Size	Default								
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>error-allow</i></td> <td>Allow web pages with a rating error to pass through.</td> </tr> <tr> <td><i>rate-server-ip</i></td> <td>Rate the server IP in addition to the domain name.</td> </tr> <tr> <td><i>connect-request-bypass</i></td> <td>Bypass connection which has CONNECT request.</td> </tr> </tbody> </table>	Option	Description	<i>error-allow</i>	Allow web pages with a rating error to pass through.	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.			
Option	Description											
<i>error-allow</i>	Allow web pages with a rating error to pass through.											
<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.											
<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.											

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ftgd-disable</i></td> <td>Disable FortiGuard scanning.</td> </tr> </tbody> </table>	Option	Description	<i>ftgd-disable</i>	Disable FortiGuard scanning.					
Option	Description									
<i>ftgd-disable</i>	Disable FortiGuard scanning.									
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17						
ovrd	Allow web filter profile overrides.	user	Not Specified							
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300						
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rating JavaScript by URL.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rating JavaScript by URL.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rating JavaScript by URL.	<i>enable</i>	Enable rating JavaScript by URL.			
Option	Description									
<i>disable</i>	Disable rating JavaScript by URL.									
<i>enable</i>	Enable rating JavaScript by URL.									
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rating CSS by URL.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rating CSS by URL.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rating CSS by URL.	<i>enable</i>	Enable rating CSS by URL.			
Option	Description									
<i>disable</i>	Disable rating CSS by URL.									
<i>enable</i>	Enable rating CSS by URL.									
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rating CRL by URL.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rating CRL by URL.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rating CRL by URL.	<i>enable</i>	Enable rating CRL by URL.			
Option	Description									
<i>disable</i>	Disable rating CRL by URL.									
<i>enable</i>	Enable rating CRL by URL.									

### config filters

Parameter	Description	Type	Size	Default
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0
action	Action to take for matches.	option	-	monitor

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>block</i></td> <td>Block access.</td> </tr> <tr> <td><i>authenticate</i></td> <td>Authenticate user before allowing access.</td> </tr> <tr> <td><i>monitor</i></td> <td>Allow access while logging the action.</td> </tr> <tr> <td><i>warning</i></td> <td>Allow access after warning the user.</td> </tr> </tbody> </table>	Option	Description	<i>block</i>	Block access.	<i>authenticate</i>	Authenticate user before allowing access.	<i>monitor</i>	Allow access while logging the action.	<i>warning</i>	Allow access after warning the user.			
Option	Description													
<i>block</i>	Block access.													
<i>authenticate</i>	Authenticate user before allowing access.													
<i>monitor</i>	Allow access while logging the action.													
<i>warning</i>	Allow access after warning the user.													
warn-duration	Duration of warnings.	user	Not Specified	5m										
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79											
log	Enable/disable logging.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
override-replacemsg	Override replacement message.	string	Maximum length: 28											
warning-prompt	Warning prompts in each category or each domain.	option	-	per-category										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>per-domain</i></td> <td>Per-domain warnings.</td> </tr> <tr> <td><i>per-category</i></td> <td>Per-category warnings.</td> </tr> </tbody> </table>	Option	Description	<i>per-domain</i>	Per-domain warnings.	<i>per-category</i>	Per-category warnings.							
Option	Description													
<i>per-domain</i>	Per-domain warnings.													
<i>per-category</i>	Per-category warnings.													
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>session</i></td> <td>After session ends.</td> </tr> <tr> <td><i>timeout</i></td> <td>After timeout occurs.</td> </tr> </tbody> </table>	Option	Description	<i>session</i>	After session ends.	<i>timeout</i>	After timeout occurs.							
Option	Description													
<i>session</i>	After session ends.													
<i>timeout</i>	After timeout occurs.													

### config quota

Parameter	Description	Type	Size	Default
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
type	Quota type.	option	-	time



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>time</i></td> <td>Use a time-based quota.</td> </tr> <tr> <td><i>traffic</i></td> <td>Use a traffic-based quota.</td> </tr> </tbody> </table>	Option	Description	<i>time</i>	Use a time-based quota.	<i>traffic</i>	Use a traffic-based quota.							
Option	Description													
<i>time</i>	Use a time-based quota.													
<i>traffic</i>	Use a traffic-based quota.													
unit	Traffic quota unit of measurement.	option	-	MB										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>B</i></td> <td>Quota in bytes.</td> </tr> <tr> <td><i>KB</i></td> <td>Quota in kilobytes.</td> </tr> <tr> <td><i>MB</i></td> <td>Quota in megabytes.</td> </tr> <tr> <td><i>GB</i></td> <td>Quota in gigabytes.</td> </tr> </tbody> </table>	Option	Description	<i>B</i>	Quota in bytes.	<i>KB</i>	Quota in kilobytes.	<i>MB</i>	Quota in megabytes.	<i>GB</i>	Quota in gigabytes.			
Option	Description													
<i>B</i>	Quota in bytes.													
<i>KB</i>	Quota in kilobytes.													
<i>MB</i>	Quota in megabytes.													
<i>GB</i>	Quota in gigabytes.													
value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295	1024										
duration	Duration of quota.	user	Not Specified	5m										
override-replacemsg	Override replacement message.	string	Maximum length: 28											

## config antiphish

Parameter	Description	Type	Size	Default								
status	Toggle AntiPhishing functionality.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AntiPhishing functionality.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AntiPhishing functionality.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AntiPhishing functionality.	<i>disable</i>	Disable AntiPhishing functionality.					
Option	Description											
<i>enable</i>	Enable AntiPhishing functionality.											
<i>disable</i>	Disable AntiPhishing functionality.											
domain-controller	Domain for which to verify received credentials against.	string	Maximum length: 63									
default-action	Action to be taken when there is no matching rule.	option	-	exempt								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exempt</i></td> <td>Exempt requests from matching.</td> </tr> <tr> <td><i>log</i></td> <td>Log all matched requests.</td> </tr> <tr> <td><i>block</i></td> <td>Block all matched requests.</td> </tr> </tbody> </table>	Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.			
Option	Description											
<i>exempt</i>	Exempt requests from matching.											
<i>log</i>	Log all matched requests.											
<i>block</i>	Block all matched requests.											

Parameter	Description	Type	Size	Default						
check-uri	Enable/disable checking of GET URI parameters for known credentials.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable checking of GET URI for username and password fields.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable checking of GET URI for username and password fields.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable checking of GET URI for username and password fields.	<i>disable</i>	Disable checking of GET URI for username and password fields.			
Option	Description									
<i>enable</i>	Enable checking of GET URI for username and password fields.									
<i>disable</i>	Disable checking of GET URI for username and password fields.									
check-basic-auth	Enable/disable checking of HTTP Basic Auth field for known credentials.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable checking of HTTP Basic Auth field for known credentials.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable checking of HTTP Basic Auth field for known credentials.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.	<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.			
Option	Description									
<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.									
<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.									
check-username-only	Enable/disable acting only on valid username credentials. Action will be taken for valid usernames regardless of password validity.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable acting only on valid username credentials.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable acting only on valid username credentials.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable acting only on valid username credentials.	<i>disable</i>	Disable acting only on valid username credentials.			
Option	Description									
<i>enable</i>	Enable acting only on valid username credentials.									
<i>disable</i>	Disable acting only on valid username credentials.									
max-body-len	Maximum size of a POST body to check for credentials.	integer	Minimum value: 0 Maximum value: 4294967295	65536						

### config inspection-entries

Parameter	Description	Type	Size	Default								
fortiguard-category	FortiGuard category to match.	user	Not Specified	g21								
action	Action to be taken upon an AntiPhishing match.	option	-	exempt								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>exempt</i></td> <td>Exempt requests from matching.</td> </tr> <tr> <td><i>log</i></td> <td>Log all matched requests.</td> </tr> <tr> <td><i>block</i></td> <td>Block all matched requests.</td> </tr> </tbody> </table>	Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.			
Option	Description											
<i>exempt</i>	Exempt requests from matching.											
<i>log</i>	Log all matched requests.											
<i>block</i>	Block all matched requests.											

## config custom-patterns

Parameter	Description	Type	Size	Default						
category	Category that the pattern matches.	option	-	username						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>username</i></td><td>Pattern matches username fields.</td></tr><tr><td><i>password</i></td><td>Pattern matches password fields.</td></tr></tbody></table>	Option	Description	<i>username</i>	Pattern matches username fields.	<i>password</i>	Pattern matches password fields.			
Option	Description									
<i>username</i>	Pattern matches username fields.									
<i>password</i>	Pattern matches password fields.									

## config webfilter fortiguard

Configure FortiGuard Web Filter service.

```
config webfilter fortiguard
  Description: Configure FortiGuard Web Filter service.
  set cache-mode [ttl|db-ver]
  set cache-prefix-match [enable|disable]
  set cache-mem-percent {integer}
  set ovr-auth-port-http {integer}
  set ovr-auth-port-https {integer}
  set ovr-auth-port-https-flow {integer}
  set ovr-auth-port-warning {integer}
  set ovr-auth-https [enable|disable]
  set warn-auth-https [enable|disable]
  set close-ports [enable|disable]
  set request-packet-size-limit {integer}
end
```

## config webfilter fortiguard

Parameter	Description	Type	Size	Default						
cache-mode	Cache entry expiration mode.	option	-	ttl						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>ttl</i></td><td>Expire cache items by time-to-live.</td></tr><tr><td><i>db-ver</i></td><td>Expire cache items when the server DB version changes.</td></tr></tbody></table>	Option	Description	<i>ttl</i>	Expire cache items by time-to-live.	<i>db-ver</i>	Expire cache items when the server DB version changes.			
Option	Description									
<i>ttl</i>	Expire cache items by time-to-live.									
<i>db-ver</i>	Expire cache items when the server DB version changes.									
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
cache-mem-percent	Maximum percentage of available memory allocated to caching .	integer	Minimum value: 1 Maximum value: 15	1 **						
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication	integer	Minimum value: 0 Maximum value: 65535	8008						
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010						
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015						
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020						
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server .	integer	Minimum value: 576 Maximum value: 10000	0						

\*\* Values may differ between models.

## config webfilter categories

List the FortiGuard Web Filter category descriptions.

```
config webfilter categories
  Description: List the FortiGuard Web Filter category descriptions.
end
```

## config webfilter override

Configure FortiGuard Web Filter administrative overrides.

```
config webfilter override
  Description: Configure FortiGuard Web Filter administrative overrides.
  edit <id>
    set status [enable|disable]
    set scope [user|user-group|...]
    set ip {ipv4-address}
    set user {string}
    set user-group {string}
    set old-profile {string}
    set new-profile {string}
    set ip6 {ipv6-address}
    set expires {user}
    set initiator {string}
  next
end
```

## config webfilter override

Parameter	Description	Type	Size	Default
status	Enable/disable override rule.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable override rule.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable override rule.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable override rule.	<i>disable</i>	Disable override rule.							
Option	Description													
<i>enable</i>	Enable override rule.													
<i>disable</i>	Disable override rule.													
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-	user										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>user</i></td> <td>Override the specified user.</td> </tr> <tr> <td><i>user-group</i></td> <td>Override the specified user group.</td> </tr> <tr> <td><i>ip</i></td> <td>Override the specified IP address.</td> </tr> <tr> <td><i>ip6</i></td> <td>Override the specified IPv6 address.</td> </tr> </tbody> </table>	Option	Description	<i>user</i>	Override the specified user.	<i>user-group</i>	Override the specified user group.	<i>ip</i>	Override the specified IP address.	<i>ip6</i>	Override the specified IPv6 address.			
Option	Description													
<i>user</i>	Override the specified user.													
<i>user-group</i>	Override the specified user group.													
<i>ip</i>	Override the specified IP address.													
<i>ip6</i>	Override the specified IPv6 address.													
ip	IPv4 address which the override applies.	ipv4-address	Not Specified	0.0.0.0										
user	Name of the user which the override applies.	string	Maximum length: 64											
user-group	Specify the user group for which the override applies.	string	Maximum length: 63											
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 35											
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 35											
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified	::										
expires	Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).	user	Not Specified	1969/12/31 17:00:00										
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64											

## config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

```

config webfilter ftgd-local-rating
  Description: Configure local FortiGuard Web Filter local ratings.
  edit <url>
    set status [enable|disable]
    set comment {var-string}
    set rating {user}
  next
end

```

## config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default						
status	Enable/disable local rating.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable local rating.</td></tr><tr><td><i>disable</i></td><td>Disable local rating.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable local rating.	<i>disable</i>	Disable local rating.			
Option	Description									
<i>enable</i>	Enable local rating.									
<i>disable</i>	Disable local rating.									
comment	Comment.	var-string	Maximum length: 255							
rating	Local rating.	user	Not Specified							

## config webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
  Description: Configure web filter search engines.
  edit <name>
    set hostname {string}
    set url {string}
    set query {string}
    set safesearch [disable|url|...]
    set charset [utf-8|gb2312]
    set safesearch-str {string}
  next
end
```

## config webfilter search-engine

Parameter	Description	Type	Size	Default
hostname	Hostname (regular expression).	string	Maximum length: 127	
url	URL (regular expression).	string	Maximum length: 127	
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15	
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Site does not support safe search.</td> </tr> <tr> <td><i>url</i></td> <td>Safe search selected with a parameter in the URL.</td> </tr> <tr> <td><i>header</i></td> <td>Safe search selected by search header (i.e. youtube.edu).</td> </tr> <tr> <td><i>translate</i></td> <td>Perform URL FortiGuard check on HTTP requests parameter.</td> </tr> <tr> <td><i>yt-pattern</i></td> <td>Pattern to match YouTube channel ID.</td> </tr> <tr> <td><i>yt-scan</i></td> <td>Perform IPS scan.</td> </tr> <tr> <td><i>yt-video</i></td> <td>Pattern to match YouTube video name.</td> </tr> <tr> <td><i>yt-channel</i></td> <td>Pattern to match YouTube channel name.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Site does not support safe search.	<i>url</i>	Safe search selected with a parameter in the URL.	<i>header</i>	Safe search selected by search header (i.e. youtube.edu).	<i>translate</i>	Perform URL FortiGuard check on HTTP requests parameter.	<i>yt-pattern</i>	Pattern to match YouTube channel ID.	<i>yt-scan</i>	Perform IPS scan.	<i>yt-video</i>	Pattern to match YouTube video name.	<i>yt-channel</i>	Pattern to match YouTube channel name.			
Option	Description																					
<i>disable</i>	Site does not support safe search.																					
<i>url</i>	Safe search selected with a parameter in the URL.																					
<i>header</i>	Safe search selected by search header (i.e. youtube.edu).																					
<i>translate</i>	Perform URL FortiGuard check on HTTP requests parameter.																					
<i>yt-pattern</i>	Pattern to match YouTube channel ID.																					
<i>yt-scan</i>	Perform IPS scan.																					
<i>yt-video</i>	Pattern to match YouTube video name.																					
<i>yt-channel</i>	Pattern to match YouTube channel name.																					
charset	Search engine charset.	option	-	utf-8																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>utf-8</i></td> <td>UTF-8 encoding.</td> </tr> <tr> <td><i>gb2312</i></td> <td>GB2312 encoding.</td> </tr> </tbody> </table>	Option	Description	<i>utf-8</i>	UTF-8 encoding.	<i>gb2312</i>	GB2312 encoding.															
Option	Description																					
<i>utf-8</i>	UTF-8 encoding.																					
<i>gb2312</i>	GB2312 encoding.																					
safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79																			

## config webfilter ftgd-statistics

Display rating cache and daemon statistics.

```
config webfilter ftgd-statistics
  Description: Display rating cache and daemon statistics.
end
```

## config webfilter status

Display rating info.

```
config webfilter status
  Description: Display rating info.
  set <refresh-rate> {string}
end
```

## config webfilter status

Parameter	Description	Type	Size	Default
<refresh-rate>	Frequency to refresh the server list (sec).	string	Maximum length: -1	



---

## config webfilter override-usr

Display list of user overrides.

```
config webfilter override-usr
  Description: Display list of user overrides.
end
```

## wireless-controller

This section includes syntax for the following commands:

- [config wireless-controller status on page 1595](#)
- [config wireless-controller access-control-list on page 1592](#)
- [config wireless-controller addrgrp on page 1586](#)
- [config wireless-controller vap on page 1445](#)
- [config wireless-controller wtp-status on page 1596](#)
- [config wireless-controller wtp-profile on page 1500](#)
- [config wireless-controller client-info on page 1596](#)
- [config wireless-controller address on page 1586](#)
- [config wireless-controller snmp on page 1587](#)
- [config wireless-controller wtp on page 1556](#)
- [config wireless-controller hotspot20 icon on page 1434](#)
- [config wireless-controller wids-profile on page 1491](#)
- [config wireless-controller hotspot20 h2qp-osu-provider on page 1435](#)
- [config wireless-controller bonjour-profile on page 1486](#)
- [config wireless-controller log on page 1480](#)
- [config wireless-controller apcfg-profile on page 1484](#)
- [config wireless-controller hotspot20 qos-map on page 1437](#)
- [config wireless-controller setting on page 1471](#)
- [config wireless-controller vap-group on page 1491](#)
- [config wireless-controller wag-profile on page 1583](#)
- [config wireless-controller ap-status on page 1594](#)
- [config wireless-controller vap-status on page 1596](#)
- [config wireless-controller hotspot20 h2qp-conn-capability on page 1432](#)
- [config wireless-controller wtp-group on page 1577](#)
- [config wireless-controller region on page 1490](#)
- [config wireless-controller hotspot20 hs-profile on page 1438](#)
- [config wireless-controller hotspot20 anqp-roaming-consortium on page 1424](#)
- [config wireless-controller timers on page 1469](#)
- [config wireless-controller spectral-info on page 1597](#)
- [config wireless-controller hotspot20 anqp-nai-realm on page 1425](#)
- [config wireless-controller rf-analysis on page 1597](#)
- [config wireless-controller hotspot20 anqp-ip-address-type on page 1429](#)
- [config wireless-controller scan on page 1594](#)
- [config wireless-controller hotspot20 h2qp-wan-metric on page 1430](#)
- [config wireless-controller ble-profile on page 1498](#)
- [config wireless-controller wlchanlistlic on page 1595](#)
- [config wireless-controller arrp-profile on page 1487](#)
- [config wireless-controller hotspot20 h2qp-operator-name on page 1430](#)
- [config wireless-controller qos-profile on page 1580](#)

- [config wireless-controller mpsk-profile on page 1590](#)
- [config wireless-controller hotspot20 anqp-venue-name on page 1423](#)
- [config wireless-controller hotspot20 anqp-3gpp-cellular on page 1428](#)
- [config wireless-controller global on page 1420](#)
- [config wireless-controller hotspot20 anqp-network-auth-type on page 1424](#)
- [config wireless-controller utm-profile on page 1585](#)
- [config wireless-controller inter-controller on page 1419](#)

## config wireless-controller inter-controller

Configure inter wireless controller operation.

```
config wireless-controller inter-controller
  Description: Configure inter wireless controller operation.
  set inter-controller-mode [disable|l2-roaming|...]
  set inter-controller-key {password}
  set inter-controller-pri [primary|secondary]
  set fast-failover-max {integer}
  set fast-failover-wait {integer}
  config inter-controller-peer
    Description: Fast failover peer wireless controller list.
    edit <id>
      set peer-ip {ipv4-address}
      set peer-port {integer}
      set peer-priority [primary|secondary]
    next
  end
end
```

## config wireless-controller inter-controller

Parameter	Description	Type	Size	Default								
inter-controller-mode	Configure inter-controller mode .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable inter-controller mode.</td> </tr> <tr> <td><i>l2-roaming</i></td> <td>Enable layer 2 roaming support between inter-controllers.</td> </tr> <tr> <td><i>1+1</i></td> <td>Enable 1+1 fast failover mode.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable inter-controller mode.	<i>l2-roaming</i>	Enable layer 2 roaming support between inter-controllers.	<i>1+1</i>	Enable 1+1 fast failover mode.			
Option	Description											
<i>disable</i>	Disable inter-controller mode.											
<i>l2-roaming</i>	Enable layer 2 roaming support between inter-controllers.											
<i>1+1</i>	Enable 1+1 fast failover mode.											
inter-controller-key	Secret key for inter-controller communications.	password	Not Specified									
inter-controller-pri	Configure inter-controller's priority .	option	-	primary								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>primary</i></td> <td>Primary fast failover mode.</td> </tr> <tr> <td><i>secondary</i></td> <td>Secondary fast failover mode.</td> </tr> </tbody> </table>	Option	Description	<i>primary</i>	Primary fast failover mode.	<i>secondary</i>	Secondary fast failover mode.			
Option	Description									
<i>primary</i>	Primary fast failover mode.									
<i>secondary</i>	Secondary fast failover mode.									
fast-failover-max	Maximum number of retransmissions for fast failover HA messages between peer wireless controllers .	integer	Minimum value: 3 Maximum value: 64	10						
fast-failover-wait	Minimum wait time before an AP transitions from secondary controller to primary controller .	integer	Minimum value: 10 Maximum value: 86400	10						

### config inter-controller-peer

Parameter	Description	Type	Size	Default						
peer-ip	Peer wireless controller's IP address.	ipv4-address	Not Specified	0.0.0.0						
peer-port	Port used by the wireless controller's for inter-controller communications .	integer	Minimum value: 1024 Maximum value: 49150	5246						
peer-priority	Peer wireless controller's priority .	option	-	primary						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>primary</i></td> <td>Primary fast failover mode.</td> </tr> <tr> <td><i>secondary</i></td> <td>Secondary fast failover mode.</td> </tr> </tbody> </table>	Option	Description	<i>primary</i>	Primary fast failover mode.	<i>secondary</i>	Secondary fast failover mode.			
Option	Description									
<i>primary</i>	Primary fast failover mode.									
<i>secondary</i>	Secondary fast failover mode.									

### config wireless-controller global

Configure wireless controller global settings.

```

config wireless-controller global
  Description: Configure wireless controller global settings.
  set name {string}
  set location {string}
  set image-download [enable|disable]
  set max-retransmit {integer}
  set control-message-offload {option1}, {option2}, ...
  set data-ethernet-II [enable|disable]
  set link-aggregation [enable|disable]

```

```

set mesh-eth-type {integer}
set fiapp-eth-type {integer}
set discovery-mc-addr {ipv4-address-multicast}
set max-clients {integer}
set rogue-scan-mac-adjacency {integer}
set ipsec-base-ip {ipv4-address}
set wtp-share [enable|disable]
set ap-log-server [enable|disable]
set ap-log-server-ip {ipv4-address}
set ap-log-server-port {integer}
end

```

## config wireless-controller global

Parameter	Description	Type	Size	Default								
name	Name of the wireless controller.	string	Maximum length: 35									
location	Description of the location of the wireless controller.	string	Maximum length: 35									
image-download	Enable/disable WTP image download at join time.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WTP image download at join time.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WTP image download at join time.</td> </tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable WTP image download at join time.	<i>disable</i>	Disable WTP image download at join time.		
Option	Description											
<i>enable</i>	Enable WTP image download at join time.											
<i>disable</i>	Disable WTP image download at join time.											
max-retransmit	Maximum number of tunnel packet retransmissions .	integer	Minimum value: 0 Maximum value: 64	3								
control-message-offload	Configure CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ebp-frame</i></td> <td>Ekahau blink protocol (EBP) frames.</td> </tr> <tr> <td><i>aeroscout-tag</i></td> <td>AeroScout tag.</td> </tr> <tr> <td><i>ap-list</i></td> <td>Rogue AP list.</td> </tr> </tbody> </table>				Option	Description	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.	<i>aeroscout-tag</i>	AeroScout tag.	<i>ap-list</i>	Rogue AP list.
Option	Description											
<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.											
<i>aeroscout-tag</i>	AeroScout tag.											
<i>ap-list</i>	Rogue AP list.											

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>sta-list</i></td> <td>Rogue STA list.</td> </tr> <tr> <td><i>sta-cap-list</i></td> <td>STA capability list.</td> </tr> <tr> <td><i>stats</i></td> <td>WTP, radio, VAP, and STA statistics.</td> </tr> <tr> <td><i>aeroscout-mu</i></td> <td>AeroScout Mobile Unit (MU) report.</td> </tr> <tr> <td><i>sta-health</i></td> <td>STA health log.</td> </tr> <tr> <td><i>spectral-analysis</i></td> <td>Spectral analysis report.</td> </tr> </tbody> </table>	Option	Description	<i>sta-list</i>	Rogue STA list.	<i>sta-cap-list</i>	STA capability list.	<i>stats</i>	WTP, radio, VAP, and STA statistics.	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	<i>sta-health</i>	STA health log.	<i>spectral-analysis</i>	Spectral analysis report.			
Option	Description																	
<i>sta-list</i>	Rogue STA list.																	
<i>sta-cap-list</i>	STA capability list.																	
<i>stats</i>	WTP, radio, VAP, and STA statistics.																	
<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.																	
<i>sta-health</i>	STA health log.																	
<i>spectral-analysis</i>	Spectral analysis report.																	
data-ethernet-II	Configure the wireless controller to use Ethernet II or 802.3 frames with 802.3 data tunnel mode .	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Use Ethernet II frames with 802.3 data tunnel mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Use 802.3 Ethernet frames with 802.3 data tunnel mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.	<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.											
Option	Description																	
<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.																	
<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.																	
link-aggregation	Enable/disable calculating the CAPWAP transmit hash to load balance sessions to link aggregation nodes .	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable calculating the CAPWAP transmit hash.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable calculating the CAPWAP transmit hash.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable calculating the CAPWAP transmit hash.	<i>disable</i>	Disable calculating the CAPWAP transmit hash.											
Option	Description																	
<i>enable</i>	Enable calculating the CAPWAP transmit hash.																	
<i>disable</i>	Disable calculating the CAPWAP transmit hash.																	
mesh-eth-type	Mesh Ethernet identifier included in backhaul packets .	integer	Minimum value: 0 Maximum value: 65535	8755														
fiapp-eth-type	Ethernet type for Fortinet Inter-Access Point Protocol .	integer	Minimum value: 0 Maximum value: 65535	5252														
discovery-mc-addr	Multicast IP address for AP discovery .	ipv4-address-multicast	Not Specified	224.0.1.140														
max-clients	Maximum number of clients that can connect simultaneously .	integer	Minimum value: 0 Maximum value: 4294967295	0														

Parameter	Description	Type	Size	Default						
rogue-scan-mac-adjacency	Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection .	integer	Minimum value: 0 Maximum value: 31	7						
ipsec-base-ip	Base IP address for IPsec VPN tunnels between the access points and the wireless controller .	ipv4-address	Not Specified	169.254.0.1						
wtp-share	Enable/disable sharing of WTPs between VDOMs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>WTP can be shared between all VDOMs.</td> </tr> <tr> <td><i>disable</i></td> <td>WTP can be used only in its own VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	WTP can be shared between all VDOMs.	<i>disable</i>	WTP can be used only in its own VDOM.			
Option	Description									
<i>enable</i>	WTP can be shared between all VDOMs.									
<i>disable</i>	WTP can be used only in its own VDOM.									
ap-log-server	Enable/disable configuring APs or FortiAPs to send log messages to a syslog server .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AP log server.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AP log server.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AP log server.	<i>disable</i>	Disable AP log server.			
Option	Description									
<i>enable</i>	Enable AP log server.									
<i>disable</i>	Disable AP log server.									
ap-log-server-ip	IP address that APs or FortiAPs send log messages to.	ipv4-address	Not Specified	0.0.0.0						
ap-log-server-port	Port that APs or FortiAPs send log messages to.	integer	Minimum value: 0 Maximum value: 65535	0						

## config wireless-controller hotspot20 anqp-venue-name

Configure venue name duple.

```

config wireless-controller hotspot20 anqp-venue-name
  Description: Configure venue name duple.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end

```

## config value-list

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
value	Venue name value.	string	Maximum length: 252	

## config wireless-controller hotspot20 anqp-network-auth-type

Configure network authentication type.

```
config wireless-controller hotspot20 anqp-network-auth-type
  Description: Configure network authentication type.
  edit <name>
    set auth-type [acceptance-of-terms|online-enrollment|...]
    set url {string}
  next
end
```

## config wireless-controller hotspot20 anqp-network-auth-type

Parameter	Description	Type	Size	Default										
auth-type	Network authentication type.	option	-	acceptance-of-terms										
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>acceptance-of-terms</i></td><td>Acceptance of terms and conditions.</td></tr><tr><td><i>online-enrollment</i></td><td>Online enrollment supported.</td></tr><tr><td><i>http-redirection</i></td><td>HTTP and HTTPS redirection.</td></tr><tr><td><i>dns-redirection</i></td><td>DNS redirection.</td></tr></tbody></table>	Option	Description	<i>acceptance-of-terms</i>	Acceptance of terms and conditions.	<i>online-enrollment</i>	Online enrollment supported.	<i>http-redirection</i>	HTTP and HTTPS redirection.	<i>dns-redirection</i>	DNS redirection.			
Option	Description													
<i>acceptance-of-terms</i>	Acceptance of terms and conditions.													
<i>online-enrollment</i>	Online enrollment supported.													
<i>http-redirection</i>	HTTP and HTTPS redirection.													
<i>dns-redirection</i>	DNS redirection.													
url	Redirect URL.	string	Maximum length: 255											

## config wireless-controller hotspot20 anqp-roaming-consortium

Configure roaming consortium.

```
config wireless-controller hotspot20 anqp-roaming-consortium
  Description: Configure roaming consortium.
  edit <name>
    config oi-list
      Description: Organization identifier list.
      edit <index>
```



```

        set oi {string}
        set comment {string}
    next
end
next
end

```

## config oi-list

Parameter	Description	Type	Size	Default
oi	Organization identifier.	string	Maximum length: 10	
comment	Comment.	string	Maximum length: 35	

## config wireless-controller hotspot20 anqp-nai-realm

Configure network access identifier (NAI) realm.

```

config wireless-controller hotspot20 anqp-nai-realm
  Description: Configure network access identifier (NAI) realm.
  edit <name>
    config nai-list
      Description: NAI list.
      edit <name>
        set encoding [disable|enable]
        set nai-realm {string}
        config eap-method
          Description: EAP Methods.
          edit <index>
            set method [eap-identity|eap-md5|...]
            config auth-param
              Description: EAP auth param.
              edit <index>
                set id [non-eap-inner-auth|inner-auth-eap|...]
                set val [eap-identity|eap-md5|...]
              next
            end
          next
        end
      next
    end
  next
end
next
end
next
end
next
end

```

## config nai-list

Parameter	Description	Type	Size	Default						
encoding	Enable/disable format in accordance with IETF RFC 4282.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Disable format in accordance with IETF RFC 4282.</td></tr><tr><td><i>enable</i></td><td>Enable format in accordance with IETF RFC 4282.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Disable format in accordance with IETF RFC 4282.	<i>enable</i>	Enable format in accordance with IETF RFC 4282.			
Option	Description									
<i>disable</i>	Disable format in accordance with IETF RFC 4282.									
<i>enable</i>	Enable format in accordance with IETF RFC 4282.									
nai-realm	Configure NAI realms (delimited by a semi-colon character).	string	Maximum length: 255							

## config eap-method

Parameter	Description	Type	Size	Default																		
method	EAP method type.	option	-	eap-identity																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>eap-identity</i></td><td>Identity.</td></tr><tr><td><i>eap-md5</i></td><td>MD5.</td></tr><tr><td><i>eap-tls</i></td><td>TLS.</td></tr><tr><td><i>eap-ttls</i></td><td>TTLS.</td></tr><tr><td><i>eap-peap</i></td><td>PEAP.</td></tr><tr><td><i>eap-sim</i></td><td>SIM.</td></tr><tr><td><i>eap-aka</i></td><td>AKA.</td></tr><tr><td><i>eap-aka-prime</i></td><td>AKA'.</td></tr></tbody></table>	Option	Description	<i>eap-identity</i>	Identity.	<i>eap-md5</i>	MD5.	<i>eap-tls</i>	TLS.	<i>eap-ttls</i>	TTLS.	<i>eap-peap</i>	PEAP.	<i>eap-sim</i>	SIM.	<i>eap-aka</i>	AKA.	<i>eap-aka-prime</i>	AKA'.			
Option	Description																					
<i>eap-identity</i>	Identity.																					
<i>eap-md5</i>	MD5.																					
<i>eap-tls</i>	TLS.																					
<i>eap-ttls</i>	TTLS.																					
<i>eap-peap</i>	PEAP.																					
<i>eap-sim</i>	SIM.																					
<i>eap-aka</i>	AKA.																					
<i>eap-aka-prime</i>	AKA'.																					

## config auth-param

Parameter	Description	Type	Size	Default								
id	ID of authentication parameter.	option	-	inner-auth-eap								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>non-eap-inner-auth</i></td><td>Non-EAP inner authentication type.</td></tr><tr><td><i>inner-auth-eap</i></td><td>Inner authentication EAP method type.</td></tr><tr><td><i>credential</i></td><td>Credential type.</td></tr></tbody></table>	Option	Description	<i>non-eap-inner-auth</i>	Non-EAP inner authentication type.	<i>inner-auth-eap</i>	Inner authentication EAP method type.	<i>credential</i>	Credential type.			
Option	Description											
<i>non-eap-inner-auth</i>	Non-EAP inner authentication type.											
<i>inner-auth-eap</i>	Inner authentication EAP method type.											
<i>credential</i>	Credential type.											

Parameter	Description	Type	Size	Default																																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunneled-credential</i></td> <td>Tunneled EAP method credential type.</td> </tr> </tbody> </table>	Option	Description	<i>tunneled-credential</i>	Tunneled EAP method credential type.																																													
Option	Description																																																	
<i>tunneled-credential</i>	Tunneled EAP method credential type.																																																	
val	Value of authentication parameter.	option	-	eap-identity																																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>eap-identity</i></td> <td>EAP Identity.</td> </tr> <tr> <td><i>eap-md5</i></td> <td>EAP MD5.</td> </tr> <tr> <td><i>eap-tls</i></td> <td>EAP TLS.</td> </tr> <tr> <td><i>eap-ttls</i></td> <td>EAP TTLS.</td> </tr> <tr> <td><i>eap-peap</i></td> <td>EAP PEAP.</td> </tr> <tr> <td><i>eap-sim</i></td> <td>EAP SIM.</td> </tr> <tr> <td><i>eap-aka</i></td> <td>EAP AKA.</td> </tr> <tr> <td><i>eap-aka-prime</i></td> <td>EAP AKA'.</td> </tr> <tr> <td><i>non-eap-pap</i></td> <td>Non EAP PAP.</td> </tr> <tr> <td><i>non-eap-chap</i></td> <td>Non EAP CHAP.</td> </tr> <tr> <td><i>non-eap-mschap</i></td> <td>Non EAP MSCHAP.</td> </tr> <tr> <td><i>non-eap-mschapv2</i></td> <td>Non EAP MSCHAPV2.</td> </tr> <tr> <td><i>cred-sim</i></td> <td>Credential SIM.</td> </tr> <tr> <td><i>cred-usim</i></td> <td>Credential USIM.</td> </tr> <tr> <td><i>cred-nfc</i></td> <td>Credential NFC secure element.</td> </tr> <tr> <td><i>cred-hardware-token</i></td> <td>Credential hardware token.</td> </tr> <tr> <td><i>cred-softoken</i></td> <td>Credential softoken.</td> </tr> <tr> <td><i>cred-certificate</i></td> <td>Credential certificate.</td> </tr> <tr> <td><i>cred-user-pwd</i></td> <td>Credential username password.</td> </tr> <tr> <td><i>cred-none</i></td> <td>Credential none.</td> </tr> <tr> <td><i>cred-vendor-specific</i></td> <td>Credential vendor specific.</td> </tr> <tr> <td><i>tun-cred-sim</i></td> <td>Tunneled credential SIM.</td> </tr> </tbody> </table>	Option	Description	<i>eap-identity</i>	EAP Identity.	<i>eap-md5</i>	EAP MD5.	<i>eap-tls</i>	EAP TLS.	<i>eap-ttls</i>	EAP TTLS.	<i>eap-peap</i>	EAP PEAP.	<i>eap-sim</i>	EAP SIM.	<i>eap-aka</i>	EAP AKA.	<i>eap-aka-prime</i>	EAP AKA'.	<i>non-eap-pap</i>	Non EAP PAP.	<i>non-eap-chap</i>	Non EAP CHAP.	<i>non-eap-mschap</i>	Non EAP MSCHAP.	<i>non-eap-mschapv2</i>	Non EAP MSCHAPV2.	<i>cred-sim</i>	Credential SIM.	<i>cred-usim</i>	Credential USIM.	<i>cred-nfc</i>	Credential NFC secure element.	<i>cred-hardware-token</i>	Credential hardware token.	<i>cred-softoken</i>	Credential softoken.	<i>cred-certificate</i>	Credential certificate.	<i>cred-user-pwd</i>	Credential username password.	<i>cred-none</i>	Credential none.	<i>cred-vendor-specific</i>	Credential vendor specific.	<i>tun-cred-sim</i>	Tunneled credential SIM.			
Option	Description																																																	
<i>eap-identity</i>	EAP Identity.																																																	
<i>eap-md5</i>	EAP MD5.																																																	
<i>eap-tls</i>	EAP TLS.																																																	
<i>eap-ttls</i>	EAP TTLS.																																																	
<i>eap-peap</i>	EAP PEAP.																																																	
<i>eap-sim</i>	EAP SIM.																																																	
<i>eap-aka</i>	EAP AKA.																																																	
<i>eap-aka-prime</i>	EAP AKA'.																																																	
<i>non-eap-pap</i>	Non EAP PAP.																																																	
<i>non-eap-chap</i>	Non EAP CHAP.																																																	
<i>non-eap-mschap</i>	Non EAP MSCHAP.																																																	
<i>non-eap-mschapv2</i>	Non EAP MSCHAPV2.																																																	
<i>cred-sim</i>	Credential SIM.																																																	
<i>cred-usim</i>	Credential USIM.																																																	
<i>cred-nfc</i>	Credential NFC secure element.																																																	
<i>cred-hardware-token</i>	Credential hardware token.																																																	
<i>cred-softoken</i>	Credential softoken.																																																	
<i>cred-certificate</i>	Credential certificate.																																																	
<i>cred-user-pwd</i>	Credential username password.																																																	
<i>cred-none</i>	Credential none.																																																	
<i>cred-vendor-specific</i>	Credential vendor specific.																																																	
<i>tun-cred-sim</i>	Tunneled credential SIM.																																																	

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tun-cred-usim</i></td> <td>Tunneled credential USIM.</td> </tr> <tr> <td><i>tun-cred-nfc</i></td> <td>Tunneled credential NFC secure element.</td> </tr> <tr> <td><i>tun-cred-hardware-token</i></td> <td>Tunneled credential hardware token.</td> </tr> <tr> <td><i>tun-cred-softoken</i></td> <td>Tunneled credential softoken.</td> </tr> <tr> <td><i>tun-cred-certificate</i></td> <td>Tunneled credential certificate.</td> </tr> <tr> <td><i>tun-cred-user-pwd</i></td> <td>Tunneled credential username password.</td> </tr> <tr> <td><i>tun-cred-anonymous</i></td> <td>Tunneled credential anonymous.</td> </tr> <tr> <td><i>tun-cred-vendor-specific</i></td> <td>Tunneled credential vendor specific.</td> </tr> </tbody> </table>	Option	Description	<i>tun-cred-usim</i>	Tunneled credential USIM.	<i>tun-cred-nfc</i>	Tunneled credential NFC secure element.	<i>tun-cred-hardware-token</i>	Tunneled credential hardware token.	<i>tun-cred-softoken</i>	Tunneled credential softoken.	<i>tun-cred-certificate</i>	Tunneled credential certificate.	<i>tun-cred-user-pwd</i>	Tunneled credential username password.	<i>tun-cred-anonymous</i>	Tunneled credential anonymous.	<i>tun-cred-vendor-specific</i>	Tunneled credential vendor specific.			
Option	Description																					
<i>tun-cred-usim</i>	Tunneled credential USIM.																					
<i>tun-cred-nfc</i>	Tunneled credential NFC secure element.																					
<i>tun-cred-hardware-token</i>	Tunneled credential hardware token.																					
<i>tun-cred-softoken</i>	Tunneled credential softoken.																					
<i>tun-cred-certificate</i>	Tunneled credential certificate.																					
<i>tun-cred-user-pwd</i>	Tunneled credential username password.																					
<i>tun-cred-anonymous</i>	Tunneled credential anonymous.																					
<i>tun-cred-vendor-specific</i>	Tunneled credential vendor specific.																					

## config wireless-controller hotspot20 anqp-3gpp-cellular

Configure 3GPP public land mobile network (PLMN).

```
config wireless-controller hotspot20 anqp-3gpp-cellular
  Description: Configure 3GPP public land mobile network (PLMN).
  edit <name>
    config mcc-mnc-list
      Description: Mobile Country Code and Mobile Network Code configuration.
      edit <id>
        set mcc {string}
        set mnc {string}
      next
    end
  next
end
```

### config mcc-mnc-list

Parameter	Description	Type	Size	Default
mcc	Mobile country code.	string	Maximum length: 3	
mnc	Mobile network code.	string	Maximum length: 3	

## config wireless-controller hotspot20 anqp-ip-address-type

Configure IP address type availability.

```
config wireless-controller hotspot20 anqp-ip-address-type
  Description: Configure IP address type availability.
  edit <name>
    set ipv6-address-type [not-available|available|...]
    set ipv4-address-type [not-available|public|...]
  next
end
```

## config wireless-controller hotspot20 anqp-ip-address-type

Parameter	Description	Type	Size	Default																		
ipv6-address-type	IPv6 address type.	option	-	not-available																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>not-available</i></td><td>Address type not available.</td></tr><tr><td><i>available</i></td><td>Address type available.</td></tr><tr><td><i>not-known</i></td><td>Availability of the address type not known.</td></tr></tbody></table>	Option	Description	<i>not-available</i>	Address type not available.	<i>available</i>	Address type available.	<i>not-known</i>	Availability of the address type not known.													
Option	Description																					
<i>not-available</i>	Address type not available.																					
<i>available</i>	Address type available.																					
<i>not-known</i>	Availability of the address type not known.																					
ipv4-address-type	IPv4 address type.	option	-	not-available																		
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>not-available</i></td><td>Address type not available.</td></tr><tr><td><i>public</i></td><td>Public IPv4 address available.</td></tr><tr><td><i>port-restricted</i></td><td>Port-restricted IPv4 address available.</td></tr><tr><td><i>single-NATed-private</i></td><td>Single NATed private IPv4 address available.</td></tr><tr><td><i>double-NATed-private</i></td><td>Double NATed private IPv4 address available.</td></tr><tr><td><i>port-restricted-and-single-NATed</i></td><td>Port-restricted IPv4 address and single NATed IPv4 address available.</td></tr><tr><td><i>port-restricted-and-double-NATed</i></td><td>Port-restricted IPv4 address and double NATed IPv4 address available.</td></tr><tr><td><i>not-known</i></td><td>Availability of the address type is not known.</td></tr></tbody></table>	Option	Description	<i>not-available</i>	Address type not available.	<i>public</i>	Public IPv4 address available.	<i>port-restricted</i>	Port-restricted IPv4 address available.	<i>single-NATed-private</i>	Single NATed private IPv4 address available.	<i>double-NATed-private</i>	Double NATed private IPv4 address available.	<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.	<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.	<i>not-known</i>	Availability of the address type is not known.			
Option	Description																					
<i>not-available</i>	Address type not available.																					
<i>public</i>	Public IPv4 address available.																					
<i>port-restricted</i>	Port-restricted IPv4 address available.																					
<i>single-NATed-private</i>	Single NATed private IPv4 address available.																					
<i>double-NATed-private</i>	Double NATed private IPv4 address available.																					
<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.																					
<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.																					
<i>not-known</i>	Availability of the address type is not known.																					

## config wireless-controller hotspot20 h2qp-operator-name

Configure operator friendly name.

```
config wireless-controller hotspot20 h2qp-operator-name
  Description: Configure operator friendly name.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end
```

### config value-list

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
value	Friendly name value.	string	Maximum length: 252	

## config wireless-controller hotspot20 h2qp-wan-metric

Configure WAN metrics.

```
config wireless-controller hotspot20 h2qp-wan-metric
  Description: Configure WAN metrics.
  edit <name>
    set link-status [up|down|...]
    set symmetric-wan-link [symmetric|asymmetric]
    set link-at-capacity [enable|disable]
    set uplink-speed {integer}
    set downlink-speed {integer}
    set uplink-load {integer}
    set downlink-load {integer}
    set load-measurement-duration {integer}
  next
end
```

### config wireless-controller hotspot20 h2qp-wan-metric

Parameter	Description	Type	Size	Default
link-status	Link status.	option	-	up

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>up</i></td> <td>Link up.</td> </tr> <tr> <td><i>down</i></td> <td>Link down.</td> </tr> <tr> <td><i>in-test</i></td> <td>Link in test state.</td> </tr> </tbody> </table>	Option	Description	<i>up</i>	Link up.	<i>down</i>	Link down.	<i>in-test</i>	Link in test state.			
Option	Description											
<i>up</i>	Link up.											
<i>down</i>	Link down.											
<i>in-test</i>	Link in test state.											
symmetric-wan-link	WAN link symmetry.	option	-	asymmetric								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>symmetric</i></td> <td>Symmetric WAN link (uplink and downlink speeds are the same).</td> </tr> <tr> <td><i>asymmetric</i></td> <td>Asymmetric WAN link (uplink and downlink speeds are not the same).</td> </tr> </tbody> </table>	Option	Description	<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).	<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).					
Option	Description											
<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).											
<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).											
link-at-capacity	Link at capacity.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Link at capacity (not allow additional mobile devices to associate).</td> </tr> <tr> <td><i>disable</i></td> <td>Link not at capacity (allow additional mobile devices to associate).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).	<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).					
Option	Description											
<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).											
<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).											
uplink-speed	Uplink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295	2400								
downlink-speed	Downlink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295	2400								
uplink-load	Uplink load.	integer	Minimum value: 0 Maximum value: 255	0								
downlink-load	Downlink load.	integer	Minimum value: 0 Maximum value: 255	0								
load-measurement-duration	Load measurement duration (in tenths of a second).	integer	Minimum value: 0 Maximum value: 65535	0								

## config wireless-controller hotspot20 h2qp-conn-capability

Configure connection capability.

```
config wireless-controller hotspot20 h2qp-conn-capability
  Description: Configure connection capability.
  edit <name>
    set icmp-port [closed|open|...]
    set ftp-port [closed|open|...]
    set ssh-port [closed|open|...]
    set http-port [closed|open|...]
    set tls-port [closed|open|...]
    set pptp-vpn-port [closed|open|...]
    set voip-tcp-port [closed|open|...]
    set voip-udp-port [closed|open|...]
    set ikev2-port [closed|open|...]
    set ikev2-xx-port [closed|open|...]
    set esp-port [closed|open|...]
  next
end
```

## config wireless-controller hotspot20 h2qp-conn-capability

Parameter	Description	Type	Size	Default								
icmp-port	Set ICMP port service status.	option	-	unknown								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></tbody></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ftp-port	Set FTP port service status.	option	-	unknown								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></tbody></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ssh-port	Set SSH port service status.	option	-	unknown								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></tbody></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											



Parameter	Description	Type	Size	Default								
http-port	Set HTTP port service status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
tls-port	Set TLS VPN (HTTPS) port service status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
pptp-vpn-port	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
voip-tcp-port	Set VoIP TCP port service status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
voip-udp-port	Set VoIP UDP port service status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ikev2-port	Set IKEv2 port service for IPsec VPN status.	option	-	unknown								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ikev2-xx-port	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
esp-port	Set ESP port service (used by IPsec VPNs) status.	option	-	unknown								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>closed</i></td> <td>The port is not open for communication.</td> </tr> <tr> <td><i>open</i></td> <td>The port is open for communication.</td> </tr> <tr> <td><i>unknown</i></td> <td>The port may or may not be open for communication.</td> </tr> </tbody> </table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											

## config wireless-controller hotspot20 icon

Configure OSU provider icon.

```

config wireless-controller hotspot20 icon
  Description: Configure OSU provider icon.
  edit <name>
    config icon-list
      Description: Icon list.
      edit <name>
        set lang {string}
        set file {string}
        set type [bmp|gif|...]
        set width {integer}
        set height {integer}
      next
    end
  next
end

```

## config icon-list

Parameter	Description	Type	Size	Default												
lang	Language code.	string	Maximum length: 3	eng												
file	Icon file.	string	Maximum length: 255													
type	Icon type.	option	-	png												
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>bmp</i></td><td>BMP image.</td></tr><tr><td><i>gif</i></td><td>GIF image.</td></tr><tr><td><i>jpeg</i></td><td>JPEG image.</td></tr><tr><td><i>png</i></td><td>PNG image.</td></tr><tr><td><i>tiff</i></td><td>TIFF image.</td></tr></tbody></table>	Option	Description	<i>bmp</i>	BMP image.	<i>gif</i>	GIF image.	<i>jpeg</i>	JPEG image.	<i>png</i>	PNG image.	<i>tiff</i>	TIFF image.			
Option	Description															
<i>bmp</i>	BMP image.															
<i>gif</i>	GIF image.															
<i>jpeg</i>	JPEG image.															
<i>png</i>	PNG image.															
<i>tiff</i>	TIFF image.															
width	Icon width.	integer	Minimum value: 1 Maximum value: 65535	0												
height	Icon height.	integer	Minimum value: 1 Maximum value: 65535	0												

## config wireless-controller hotspot20 h2qp-osu-provider

Configure online sign up (OSU) provider list.

```
config wireless-controller hotspot20 h2qp-osu-provider
  Description: Configure online sign up (OSU) provider list.
  edit <name>
    config friendly-name
      Description: OSU provider friendly name.
      edit <index>
        set lang {string}
        set friendly-name {string}
      next
    end
    set server-uri {string}
    set osu-method {option1}, {option2}, ...
    set osu-nai {string}
    config service-description
      Description: OSU service name.
      edit <service-id>
```

```

        set lang {string}
        set service-description {string}
    next
end
set icon {string}
next
end

```

## config wireless-controller hotspot20 h2qp-osu-provider

Parameter	Description	Type	Size	Default								
server-uri	Server URI.	string	Maximum length: 255									
osu-method	OSU method list.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>oma-dm</i></td> <td>OMA DM.</td> </tr> <tr> <td><i>soap-xml-spp</i></td> <td>SOAP XML SPP.</td> </tr> <tr> <td><i>reserved</i></td> <td>Reserved.</td> </tr> </tbody> </table>	Option	Description	<i>oma-dm</i>	OMA DM.	<i>soap-xml-spp</i>	SOAP XML SPP.	<i>reserved</i>	Reserved.			
Option	Description											
<i>oma-dm</i>	OMA DM.											
<i>soap-xml-spp</i>	SOAP XML SPP.											
<i>reserved</i>	Reserved.											
osu-nai	OSU NAI.	string	Maximum length: 255									
icon	OSU provider icon.	string	Maximum length: 35									

## config friendly-name

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
friendly-name	OSU provider friendly name.	string	Maximum length: 252	

## config service-description

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
service-description	Service description.	string	Maximum length: 252	

## config wireless-controller hotspot20 qos-map

Configure QoS map set.

```
config wireless-controller hotspot20 qos-map
  Description: Configure QoS map set.
  edit <name>
    config dscp-except
      Description: Differentiated Services Code Point (DSCP) exceptions.
      edit <index>
        set dscp {integer}
        set up {integer}
      next
    end
    config dscp-range
      Description: Differentiated Services Code Point (DSCP) ranges.
      edit <index>
        set up {integer}
        set low {integer}
        set high {integer}
      next
    end
  next
end
```

### config dscp-except

Parameter	Description	Type	Size	Default
dscp	DSCP value.	integer	Minimum value: 0 Maximum value: 63	0
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0

### config dscp-range

Parameter	Description	Type	Size	Default
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0
low	DSCP low value.	integer	Minimum value: 0 Maximum value: 63	255

Parameter	Description	Type	Size	Default
high	DSCP high value.	integer	Minimum value: 0 Maximum value: 63	255

## config wireless-controller hotspot20 hs-profile

Configure hotspot profile.

```

config wireless-controller hotspot20 hs-profile
  Description: Configure hotspot profile.
  edit <name>
    set access-network-type [private-network|private-network-with-guest-access|...]
    set access-network-internet [enable|disable]
    set access-network-asra [enable|disable]
    set access-network-esr [enable|disable]
    set access-network-uesa [enable|disable]
    set venue-group [unspecified|assembly|...]
    set venue-type [unspecified|arena|...]
    set hessid {mac-address}
    set proxy-arp [enable|disable]
    set l2tif [enable|disable]
    set pame-bi [disable|enable]
    set anqp-domain-id {integer}
    set domain-name {string}
    set osu-ssid {string}
    set gas-comeback-delay {integer}
    set gas-fragmentation-limit {integer}
    set dgaf [enable|disable]
    set deauth-request-timeout {integer}
    set wnm-sleep-mode [enable|disable]
    set bss-transition [enable|disable]
    set venue-name {string}
    set roaming-consortium {string}
    set nai-realm {string}
    set oper-friendly-name {string}
    set osu-provider <name1>, <name2>, ...
    set wan-metrics {string}
    set network-auth {string}
    set 3gpp-plmn {string}
    set conn-cap {string}
    set qos-map {string}
    set ip-addr-type {string}
  next
end

```

## config wireless-controller hotspot20 hs-profile

Parameter	Description	Type	Size	Default																		
access-network-type	Access network type.	option	-	private-network																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>private-network</i></td> <td>Private network.</td> </tr> <tr> <td><i>private-network-with-guest-access</i></td> <td>Private network with guest access.</td> </tr> <tr> <td><i>chargeable-public-network</i></td> <td>Chargeable public network.</td> </tr> <tr> <td><i>free-public-network</i></td> <td>Free public network.</td> </tr> <tr> <td><i>personal-device-network</i></td> <td>Personal devices network.</td> </tr> <tr> <td><i>emergency-services-only-network</i></td> <td>Emergency services only network.</td> </tr> <tr> <td><i>test-or-experimental</i></td> <td>Test or experimental.</td> </tr> <tr> <td><i>wildcard</i></td> <td>Wildcard.</td> </tr> </tbody> </table>	Option	Description	<i>private-network</i>	Private network.	<i>private-network-with-guest-access</i>	Private network with guest access.	<i>chargeable-public-network</i>	Chargeable public network.	<i>free-public-network</i>	Free public network.	<i>personal-device-network</i>	Personal devices network.	<i>emergency-services-only-network</i>	Emergency services only network.	<i>test-or-experimental</i>	Test or experimental.	<i>wildcard</i>	Wildcard.			
Option	Description																					
<i>private-network</i>	Private network.																					
<i>private-network-with-guest-access</i>	Private network with guest access.																					
<i>chargeable-public-network</i>	Chargeable public network.																					
<i>free-public-network</i>	Free public network.																					
<i>personal-device-network</i>	Personal devices network.																					
<i>emergency-services-only-network</i>	Emergency services only network.																					
<i>test-or-experimental</i>	Test or experimental.																					
<i>wildcard</i>	Wildcard.																					
access-network-internet	Enable/disable connectivity to the Internet.	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable connectivity to the Internet.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable connectivity to the Internet.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable connectivity to the Internet.	<i>disable</i>	Disable connectivity to the Internet.															
Option	Description																					
<i>enable</i>	Enable connectivity to the Internet.																					
<i>disable</i>	Disable connectivity to the Internet.																					
access-network-asra	Enable/disable additional step required for access (ASRA).	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable additional step required for access (ASRA).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable additional step required for access (ASRA).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable additional step required for access (ASRA).	<i>disable</i>	Disable additional step required for access (ASRA).															
Option	Description																					
<i>enable</i>	Enable additional step required for access (ASRA).																					
<i>disable</i>	Disable additional step required for access (ASRA).																					
access-network-esr	Enable/disable emergency services reachable (ESR).	option	-	disable																		

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable emergency services reachable (ESR).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable emergency services reachable (ESR).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable emergency services reachable (ESR).	<i>disable</i>	Disable emergency services reachable (ESR).																							
Option	Description																													
<i>enable</i>	Enable emergency services reachable (ESR).																													
<i>disable</i>	Disable emergency services reachable (ESR).																													
access-network-uesa	Enable/disable unauthenticated emergency service accessible (UESA).	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable unauthenticated emergency service accessible (UESA).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable unauthenticated emergency service accessible (UESA).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).	<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).																							
Option	Description																													
<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).																													
<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).																													
venue-group	Venue group.	option	-	unspecified																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>unspecified</i></td> <td>Unspecified.</td> </tr> <tr> <td><i>assembly</i></td> <td>Assembly.</td> </tr> <tr> <td><i>business</i></td> <td>Business.</td> </tr> <tr> <td><i>educational</i></td> <td>Educational.</td> </tr> <tr> <td><i>factory</i></td> <td>Factory and industrial.</td> </tr> <tr> <td><i>institutional</i></td> <td>Institutional.</td> </tr> <tr> <td><i>mercantile</i></td> <td>Mercantile.</td> </tr> <tr> <td><i>residential</i></td> <td>Residential.</td> </tr> <tr> <td><i>storage</i></td> <td>Storage.</td> </tr> <tr> <td><i>utility</i></td> <td>Utility and miscellaneous.</td> </tr> <tr> <td><i>vehicular</i></td> <td>Vehicular.</td> </tr> <tr> <td><i>outdoor</i></td> <td>Outdoor.</td> </tr> </tbody> </table>	Option	Description	<i>unspecified</i>	Unspecified.	<i>assembly</i>	Assembly.	<i>business</i>	Business.	<i>educational</i>	Educational.	<i>factory</i>	Factory and industrial.	<i>institutional</i>	Institutional.	<i>mercantile</i>	Mercantile.	<i>residential</i>	Residential.	<i>storage</i>	Storage.	<i>utility</i>	Utility and miscellaneous.	<i>vehicular</i>	Vehicular.	<i>outdoor</i>	Outdoor.			
Option	Description																													
<i>unspecified</i>	Unspecified.																													
<i>assembly</i>	Assembly.																													
<i>business</i>	Business.																													
<i>educational</i>	Educational.																													
<i>factory</i>	Factory and industrial.																													
<i>institutional</i>	Institutional.																													
<i>mercantile</i>	Mercantile.																													
<i>residential</i>	Residential.																													
<i>storage</i>	Storage.																													
<i>utility</i>	Utility and miscellaneous.																													
<i>vehicular</i>	Vehicular.																													
<i>outdoor</i>	Outdoor.																													
venue-type	Venue type.	option	-	unspecified																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>unspecified</i></td> <td>Unspecified.</td> </tr> <tr> <td><i>arena</i></td> <td>Arena.</td> </tr> <tr> <td><i>stadium</i></td> <td>Stadium.</td> </tr> <tr> <td><i>passenger-terminal</i></td> <td>Passenger terminal.</td> </tr> </tbody> </table>	Option	Description	<i>unspecified</i>	Unspecified.	<i>arena</i>	Arena.	<i>stadium</i>	Stadium.	<i>passenger-terminal</i>	Passenger terminal.																			
Option	Description																													
<i>unspecified</i>	Unspecified.																													
<i>arena</i>	Arena.																													
<i>stadium</i>	Stadium.																													
<i>passenger-terminal</i>	Passenger terminal.																													



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>amphitheater</i>	Amphitheater.		
	<i>amusement-park</i>	Amusement park.		
	<i>place-of-worship</i>	Place of worship.		
	<i>convention-center</i>	Convention center.		
	<i>library</i>	Library.		
	<i>museum</i>	Museum.		
	<i>restaurant</i>	Restaurant.		
	<i>theater</i>	Theater.		
	<i>bar</i>	Bar.		
	<i>coffee-shop</i>	Coffee shop.		
	<i>zoo-or-aquarium</i>	Zoo or aquarium.		
	<i>emergency-center</i>	Emergency coordination center.		
	<i>doctor-office</i>	Doctor or dentist office.		
	<i>bank</i>	Bank.		
	<i>fire-station</i>	Fire station.		
	<i>police-station</i>	Police station.		
	<i>post-office</i>	Post office.		
	<i>professional-office</i>	Professional office.		
	<i>research-facility</i>	Research and development facility.		
	<i>attorney-office</i>	Attorney office.		
	<i>primary-school</i>	Primary school.		
	<i>secondary-school</i>	Secondary school.		
	<i>university-or-college</i>	University or college.		
	<i>factory</i>	Factory.		
	<i>hospital</i>	Hospital.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>long-term-care-facility</i>	Long term care facility.		
	<i>rehab-center</i>	Alcohol and drug rehabilitation center.		
	<i>group-home</i>	Group home.		
	<i>prison-or-jail</i>	Prison or jail.		
	<i>retail-store</i>	Retail store.		
	<i>grocery-market</i>	Grocery market.		
	<i>auto-service-station</i>	Auto service station.		
	<i>shopping-mall</i>	Shopping mall.		
	<i>gas-station</i>	Gas station.		
	<i>private</i>	Private residence.		
	<i>hotel-or-motel</i>	Hotel or motel.		
	<i>dormitory</i>	Dormitory.		
	<i>boarding-house</i>	Boarding house.		
	<i>automobile</i>	Automobile or truck.		
	<i>airplane</i>	Airplane.		
	<i>bus</i>	Bus.		
	<i>ferry</i>	Ferry.		
	<i>ship-or-boat</i>	Ship or boat.		
	<i>train</i>	Train.		
	<i>motor-bike</i>	Motor bike.		
	<i>muni-mesh-network</i>	Muni mesh network.		
	<i>city-park</i>	City park.		
	<i>rest-area</i>	Rest area.		
	<i>traffic-control</i>	Traffic control.		
	<i>bus-stop</i>	Bus stop.		
	<i>kiosk</i>	Kiosk.		

Parameter	Description	Type	Size	Default						
hessid	Homogeneous extended service set identifier (HESSID).	mac-address	Not Specified	00:00:00:00:00:00						
proxy-arp	Enable/disable Proxy ARP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Proxy ARP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Proxy ARP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Proxy ARP.	<i>disable</i>	Disable Proxy ARP.			
Option	Description									
<i>enable</i>	Enable Proxy ARP.									
<i>disable</i>	Disable Proxy ARP.									
l2tif	Enable/disable Layer 2 traffic inspection and filtering.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Layer 2 traffic inspection and filtering.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Layer 2 traffic inspection and filtering.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Layer 2 traffic inspection and filtering.	<i>disable</i>	Disable Layer 2 traffic inspection and filtering.			
Option	Description									
<i>enable</i>	Enable Layer 2 traffic inspection and filtering.									
<i>disable</i>	Disable Layer 2 traffic inspection and filtering.									
pame-bi	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).			
Option	Description									
<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).									
<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).									
anqp-domain-id	ANQP Domain ID .	integer	Minimum value: 0 Maximum value: 65535	0						
domain-name	Domain name.	string	Maximum length: 255							
osu-ssid	Online sign up (OSU) SSID.	string	Maximum length: 255							
gas-comeback-delay	GAS comeback delay .	integer	Minimum value: 100 Maximum value: 4000	500						
gas-fragmentation-limit	GAS fragmentation limit .	integer	Minimum value: 512 Maximum value: 4096	1024						

Parameter	Description	Type	Size	Default						
dgaf	Enable/disable downstream group-addressed forwarding (DGAF).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable downstream group-addressed forwarding (DGAF).</td> </tr> <tr> <td><i>disable</i></td> <td>Disable downstream group-addressed forwarding (DGAF).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable downstream group-addressed forwarding (DGAF).	<i>disable</i>	Disable downstream group-addressed forwarding (DGAF).			
Option	Description									
<i>enable</i>	Enable downstream group-addressed forwarding (DGAF).									
<i>disable</i>	Disable downstream group-addressed forwarding (DGAF).									
deauth-request-timeout	Deauthentication request timeout (in seconds).	integer	Minimum value: 30 Maximum value: 120	60						
wnm-sleep-mode	Enable/disable wireless network management (WNM) sleep mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable wireless network management (WNM) sleep mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable wireless network management (WNM) sleep mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable wireless network management (WNM) sleep mode.	<i>disable</i>	Disable wireless network management (WNM) sleep mode.			
Option	Description									
<i>enable</i>	Enable wireless network management (WNM) sleep mode.									
<i>disable</i>	Disable wireless network management (WNM) sleep mode.									
bss-transition	Enable/disable basic service set (BSS) transition Support.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable basic service set (BSS) transition support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable basic service set (BSS) transition support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable basic service set (BSS) transition support.	<i>disable</i>	Disable basic service set (BSS) transition support.			
Option	Description									
<i>enable</i>	Enable basic service set (BSS) transition support.									
<i>disable</i>	Disable basic service set (BSS) transition support.									
venue-name	Venue name.	string	Maximum length: 35							
roaming-consortium	Roaming consortium list name.	string	Maximum length: 35							
nai-realm	NAI realm list name.	string	Maximum length: 35							
oper-friendly-name	Operator friendly name.	string	Maximum length: 35							
osu-provider <name>	Manually selected list of OSU provider(s). OSU provider name.	string	Maximum length: 35							
wan-metrics	WAN metric name.	string	Maximum length: 35							
network-auth	Network authentication name.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
3gpp-plmn	3GPP PLMN name.	string	Maximum length: 35	
conn-cap	Connection capability name.	string	Maximum length: 35	
qos-map	QoS MAP set ID.	string	Maximum length: 35	
ip-addr-type	IP address type name.	string	Maximum length: 35	

## config wireless-controller vap

Configure Virtual Access Points (VAPs).

```

config wireless-controller vap
  Description: Configure Virtual Access Points (VAPs).
  edit <name>
    set fast-roaming [enable|disable]
    set external-fast-roaming [enable|disable]
    set mesh-backhaul [enable|disable]
    set atf-weight {integer}
    set max-clients {integer}
    set max-clients-ap {integer}
    set ssid {string}
    set broadcast-ssid [enable|disable]
    set security [open|captive-portal|...]
    set pmf [disable|enable|...]
    set pmf-assoc-comeback-timeout {integer}
    set pmf-sa-query-retry-timeout {integer}
    set okc [disable|enable]
    set voice-enterprise [disable|enable]
    set fast-bss-transition [disable|enable]
    set ft-mobility-domain {integer}
    set ft-r0-key-lifetime {integer}
    set ft-over-ds [disable|enable]
    set sae-groups {option1}, {option2}, ...
    set owe-groups {option1}, {option2}, ...
    set owe-transition [disable|enable]
    set owe-transition-ssid {string}
    set eapol-key-retries [disable|enable]
    set tkip-counter-measure [enable|disable]
    set external-web {string}
    set external-web-format [auto-detect|no-query-string|...]
    set external-logout {string}
    set mac-auth-bypass [enable|disable]
    set radius-mac-auth [enable|disable]
    set radius-mac-auth-server {string}
    set radius-mac-auth-usergroups <name1>, <name2>, ...
    set auth [psk|radius|...]
    set encrypt [TKIP|AES|...]
    set keyindex {integer}
    set key {password}
  
```

```

set passphrase {password}
set sae-password {password}
set radius-server {string}
set local-standalone [enable|disable]
set local-standalone-nat [enable|disable]
set ip {ipv4-classnet-host}
set dhcp-lease-time {integer}
set local-bridging [enable|disable]
set local-lan [allow|deny]
set local-authentication [enable|disable]
set usergroup <name1>, <name2>, ...
set portal-message-override-group {string}
config portal-message-overrides
    Description: Individual message overrides.
    set auth-disclaimer-page {string}
    set auth-reject-page {string}
    set auth-login-page {string}
    set auth-login-failed-page {string}
end
set portal-type [auth|auth+disclaimer|...]
set selected-usergroups <name1>, <name2>, ...
set security-exempt-list {string}
set security-redirect-url {string}
set intra-vap-privacy [enable|disable]
set schedule <name1>, <name2>, ...
set ldpc [disable|rx|...]
set high-efficiency [enable|disable]
set target-wake-time [enable|disable]
set port-macauth [disable|radius|...]
set port-macauth-timeout {integer}
set port-macauth-reauth-timeout {integer}
set bss-color-partial [enable|disable]
set mpsk-profile {string}
set split-tunneling [enable|disable]
set vlanid {integer}
set vlan-auto [enable|disable]
set dynamic-vlan [enable|disable]
set captive-portal-ac-name {string}
set captive-portal-auth-timeout {integer}
set multicast-rate [0|6000|...]
set multicast-enhance [enable|disable]
set igmp-snooping [enable|disable]
set broadcast-suppression {option1}, {option2}, ...
set ipv6-rules {option1}, {option2}, ...
set me-disable-thresh {integer}
set mu-mimo [enable|disable]
set probe-resp-suppression [enable|disable]
set probe-resp-threshold {string}
set radio-sensitivity [enable|disable]
set quarantine [enable|disable]
set radio-5g-threshold {string}
set radio-2g-threshold {string}
set vlan-pooling [wtp-group|round-robin|...]
config vlan-pool
    Description: VLAN pool.
    edit <id>
        set wtp-group {string}

```

```

    next
end
set dhcp-option43-insertion [enable|disable]
set dhcp-option82-insertion [enable|disable]
set dhcp-option82-circuit-id-insertion [style-1|style-2|...]
set dhcp-option82-remote-id-insertion [style-1|disable]
set ptk-rekey [enable|disable]
set ptk-rekey-intv {integer}
set gtk-rekey [enable|disable]
set gtk-rekey-intv {integer}
set eap-reauth [enable|disable]
set eap-reauth-intv {integer}
set qos-profile {string}
set hotspot20-profile {string}
set access-control-list {string}
set primary-wag-profile {string}
set secondary-wag-profile {string}
set tunnel-echo-interval {integer}
set tunnel-fallback-interval {integer}
set rates-11a {option1}, {option2}, ...
set rates-11bg {option1}, {option2}, ...
set rates-11n-ss12 {option1}, {option2}, ...
set rates-11n-ss34 {option1}, {option2}, ...
set rates-11ac-ss12 {option1}, {option2}, ...
set rates-11ac-ss34 {option1}, {option2}, ...
set utm-profile {string}
set address-group {string}
set mac-filter [enable|disable]
set mac-filter-policy-other [allow|deny]
config mac-filter-list
    Description: Create a list of MAC addresses for MAC address filtering.
    edit <id>
        set mac {mac-address}
        set mac-filter-policy [allow|deny]
    next
end
set sticky-client-remove [enable|disable]
set sticky-client-threshold-5g {string}
set sticky-client-threshold-2g {string}
next
end

```

## config wireless-controller vap

Parameter	Description	Type	Size	Default
fast-roaming	Enable/disable fast-roaming, or pre-authentication, where supported by clients .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable fast-roaming, or pre-authentication.		
	<i>disable</i>	Disable fast-roaming, or pre-authentication.		

Parameter	Description	Type	Size	Default						
external-fast-roaming	Enable/disable fast roaming or pre-authentication with external APs not managed by the FortiGate .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable fast roaming or pre-authentication with external APs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable fast roaming or pre-authentication with external APs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable fast roaming or pre-authentication with external APs.	<i>disable</i>	Disable fast roaming or pre-authentication with external APs.			
Option	Description									
<i>enable</i>	Enable fast roaming or pre-authentication with external APs.									
<i>disable</i>	Disable fast roaming or pre-authentication with external APs.									
mesh-backhaul	Enable/disable using this VAP as a WiFi mesh backhaul . This entry is only available when security is set to a WPA type or open.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable mesh backhaul.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable mesh backhaul.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable mesh backhaul.	<i>disable</i>	Disable mesh backhaul.			
Option	Description									
<i>enable</i>	Enable mesh backhaul.									
<i>disable</i>	Disable mesh backhaul.									
aff-weight	Airtime weight in percentage .	integer	Minimum value: 0 Maximum value: 100	20						
max-clients	Maximum number of clients that can connect simultaneously to the VAP .	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-clients-ap	Maximum number of clients that can connect simultaneously to the VAP per AP radio .	integer	Minimum value: 0 Maximum value: 4294967295	0						
ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string	Maximum length: 32	fortinet						
broadcast-ssid	Enable/disable broadcasting the SSID .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable broadcasting the SSID.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable broadcasting the SSID.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable broadcasting the SSID.	<i>disable</i>	Disable broadcasting the SSID.			
Option	Description									
<i>enable</i>	Enable broadcasting the SSID.									
<i>disable</i>	Disable broadcasting the SSID.									
security	Security mode for the wireless interface .	option	-	wpa2-only-personal						



Parameter	Description	Type	Size	Default																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>open</i></td> <td>Open.</td> </tr> <tr> <td><i>captive-portal</i></td> <td>Captive portal.</td> </tr> <tr> <td><i>wep64</i></td> <td>WEP 64-bit.</td> </tr> <tr> <td><i>wep128</i></td> <td>WEP 128-bit.</td> </tr> <tr> <td><i>wpa-personal</i></td> <td>WPA/WPA2 personal.</td> </tr> <tr> <td><i>wpa-personal+captive-portal</i></td> <td>WPA/WPA2 personal with captive portal.</td> </tr> <tr> <td><i>wpa-enterprise</i></td> <td>WPA/WPA2 enterprise.</td> </tr> <tr> <td><i>wpa-only-personal</i></td> <td>WPA personal.</td> </tr> <tr> <td><i>wpa-only-personal+captive-portal</i></td> <td>WPA personal with captive portal.</td> </tr> <tr> <td><i>wpa-only-enterprise</i></td> <td>WPA enterprise.</td> </tr> <tr> <td><i>wpa2-only-personal</i></td> <td>WPA2 personal.</td> </tr> <tr> <td><i>wpa2-only-personal+captive-portal</i></td> <td>WPA2 personal with captive portal.</td> </tr> <tr> <td><i>wpa2-only-enterprise</i></td> <td>WPA2 enterprise.</td> </tr> <tr> <td><i>wpa3-enterprise</i></td> <td>WPA3 enterprise.</td> </tr> <tr> <td><i>wpa3-sae</i></td> <td>WPA3 SAE.</td> </tr> <tr> <td><i>wpa3-sae-transition</i></td> <td>WPA3 SAE transition.</td> </tr> <tr> <td><i>owe</i></td> <td>Opportunistic wireless encryption.</td> </tr> <tr> <td><i>osen</i></td> <td>OSEN.</td> </tr> </tbody> </table>	Option	Description	<i>open</i>	Open.	<i>captive-portal</i>	Captive portal.	<i>wep64</i>	WEP 64-bit.	<i>wep128</i>	WEP 128-bit.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.	<i>wpa-only-personal</i>	WPA personal.	<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.	<i>wpa-only-enterprise</i>	WPA enterprise.	<i>wpa2-only-personal</i>	WPA2 personal.	<i>wpa2-only-personal+captive-portal</i>	WPA2 personal with captive portal.	<i>wpa2-only-enterprise</i>	WPA2 enterprise.	<i>wpa3-enterprise</i>	WPA3 enterprise.	<i>wpa3-sae</i>	WPA3 SAE.	<i>wpa3-sae-transition</i>	WPA3 SAE transition.	<i>owe</i>	Opportunistic wireless encryption.	<i>osen</i>	OSEN.			
Option	Description																																									
<i>open</i>	Open.																																									
<i>captive-portal</i>	Captive portal.																																									
<i>wep64</i>	WEP 64-bit.																																									
<i>wep128</i>	WEP 128-bit.																																									
<i>wpa-personal</i>	WPA/WPA2 personal.																																									
<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.																																									
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.																																									
<i>wpa-only-personal</i>	WPA personal.																																									
<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.																																									
<i>wpa-only-enterprise</i>	WPA enterprise.																																									
<i>wpa2-only-personal</i>	WPA2 personal.																																									
<i>wpa2-only-personal+captive-portal</i>	WPA2 personal with captive portal.																																									
<i>wpa2-only-enterprise</i>	WPA2 enterprise.																																									
<i>wpa3-enterprise</i>	WPA3 enterprise.																																									
<i>wpa3-sae</i>	WPA3 SAE.																																									
<i>wpa3-sae-transition</i>	WPA3 SAE transition.																																									
<i>owe</i>	Opportunistic wireless encryption.																																									
<i>osen</i>	OSEN.																																									
pmf	Protected Management Frames .	option	-	disable																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable PMF completely.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable PMF but deny clients without PMF.</td> </tr> <tr> <td><i>optional</i></td> <td>Enable PMF and allow clients without PMF.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable PMF completely.	<i>enable</i>	Enable PMF but deny clients without PMF.	<i>optional</i>	Enable PMF and allow clients without PMF.																																	
Option	Description																																									
<i>disable</i>	Disable PMF completely.																																									
<i>enable</i>	Enable PMF but deny clients without PMF.																																									
<i>optional</i>	Enable PMF and allow clients without PMF.																																									

Parameter	Description	Type	Size	Default
pmf-assoc-comeback-timeout	Protected Management Frames .	integer	Minimum value: 1 Maximum value: 20	1
pmf-sa-query-retry-timeout	Protected Management Frames .	integer	Minimum value: 1 Maximum value: 5	2
okc	Enable/disable Opportunistic Key Caching .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Opportunistic Key Caching (OKC).		
	<i>enable</i>	Enable Opportunistic Key Caching (OKC).		
voice-enterprise	Enable/disable 802.11k and 802.11v assisted Voice-Enterprise roaming .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.		
	<i>enable</i>	Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.		
fast-bss-transition	Enable/disable 802.11r Fast BSS Transition .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable 802.11r Fast BSS Transition (FT).		
	<i>enable</i>	Enable 802.11r Fast BSS Transition (FT).		
ft-mobility-domain	Mobility domain identifier in FT .	integer	Minimum value: 1 Maximum value: 65535	1000
ft-r0-key-lifetime	Lifetime of the PMK-R0 key in FT, 1-65535 minutes.	integer	Minimum value: 1 Maximum value: 65535	480
ft-over-ds	Enable/disable FT over the Distribution System (DS).	option	-	enable

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable FT over the Distribution System (DS).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable FT over the Distribution System (DS).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable FT over the Distribution System (DS).	<i>enable</i>	Enable FT over the Distribution System (DS).					
Option	Description											
<i>disable</i>	Disable FT over the Distribution System (DS).											
<i>enable</i>	Enable FT over the Distribution System (DS).											
sae-groups	SAE-Groups.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>19</td> <td>DH Group 19.</td> </tr> <tr> <td>20</td> <td>DH Group 20.</td> </tr> <tr> <td>21</td> <td>DH Group 21.</td> </tr> </tbody> </table>	Option	Description	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.			
Option	Description											
19	DH Group 19.											
20	DH Group 20.											
21	DH Group 21.											
owe-groups	OWE-Groups.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>19</td> <td>DH Group 19.</td> </tr> <tr> <td>20</td> <td>DH Group 20.</td> </tr> <tr> <td>21</td> <td>DH Group 21.</td> </tr> </tbody> </table>	Option	Description	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.			
Option	Description											
19	DH Group 19.											
20	DH Group 20.											
21	DH Group 21.											
owe-transition	Enable/disable OWE transition mode support.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable OWE transition mode support.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable OWE transition mode support.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable OWE transition mode support.	<i>enable</i>	Enable OWE transition mode support.					
Option	Description											
<i>disable</i>	Disable OWE transition mode support.											
<i>enable</i>	Enable OWE transition mode support.											
owe-transition-ssid	OWE transition mode peer SSID.	string	Maximum length: 32									
eapol-key-retries	Enable/disable retransmission of EAPOL-Key frames .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).	<i>enable</i>	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).					
Option	Description											
<i>disable</i>	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).											
<i>enable</i>	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).											
tkip-counter-measure	Enable/disable TKIP counter measure.	option	-	enable								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable TKIP counter measure.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable TKIP counter measure.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable TKIP counter measure.	<i>disable</i>	Disable TKIP counter measure.					
Option	Description											
<i>enable</i>	Enable TKIP counter measure.											
<i>disable</i>	Disable TKIP counter measure.											
external-web	URL of external authentication web server.	string	Maximum length: 127									
external-web-format	URL query parameter detection .	option	-	auto-detect								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto-detect</i></td> <td>Automatically detect if "external-web" URL has any query parameter.</td> </tr> <tr> <td><i>no-query-string</i></td> <td>"external-web" URL does not have any query parameter.</td> </tr> <tr> <td><i>partial-query-string</i></td> <td>"external-web" URL has some query parameters.</td> </tr> </tbody> </table>	Option	Description	<i>auto-detect</i>	Automatically detect if "external-web" URL has any query parameter.	<i>no-query-string</i>	"external-web" URL does not have any query parameter.	<i>partial-query-string</i>	"external-web" URL has some query parameters.			
Option	Description											
<i>auto-detect</i>	Automatically detect if "external-web" URL has any query parameter.											
<i>no-query-string</i>	"external-web" URL does not have any query parameter.											
<i>partial-query-string</i>	"external-web" URL has some query parameters.											
external-logout	URL of external authentication logout server.	string	Maximum length: 127									
mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MAC authentication bypass.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MAC authentication bypass.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MAC authentication bypass.	<i>disable</i>	Disable MAC authentication bypass.					
Option	Description											
<i>enable</i>	Enable MAC authentication bypass.											
<i>disable</i>	Disable MAC authentication bypass.											
radius-mac-auth	Enable/disable RADIUS-based MAC authentication of clients .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable RADIUS-based MAC authentication.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable RADIUS-based MAC authentication.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable RADIUS-based MAC authentication.	<i>disable</i>	Disable RADIUS-based MAC authentication.					
Option	Description											
<i>enable</i>	Enable RADIUS-based MAC authentication.											
<i>disable</i>	Disable RADIUS-based MAC authentication.											
radius-mac-auth-server	RADIUS-based MAC authentication server.	string	Maximum length: 35									
radius-mac-auth-usergroups <name>	Selective user groups that are permitted for RADIUS mac authentication. User group name.	string	Maximum length: 79									
auth	Authentication protocol.	option	-	psk								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>psk</i></td> <td>Use a single Pre-shared Key (PSK) to authenticate all users.</td> </tr> <tr> <td><i>radius</i></td> <td>Use a RADIUS server to authenticate clients.</td> </tr> <tr> <td><i>usergroup</i></td> <td>Use a firewall usergroup to authenticate clients.</td> </tr> </tbody> </table>	Option	Description	<i>psk</i>	Use a single Pre-shared Key (PSK) to authenticate all users.	<i>radius</i>	Use a RADIUS server to authenticate clients.	<i>usergroup</i>	Use a firewall usergroup to authenticate clients.			
Option	Description											
<i>psk</i>	Use a single Pre-shared Key (PSK) to authenticate all users.											
<i>radius</i>	Use a RADIUS server to authenticate clients.											
<i>usergroup</i>	Use a firewall usergroup to authenticate clients.											
encrypt	Encryption protocol to use (only available when security is set to a WPA type).	option	-	AES								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>TKIP</i></td> <td>Use TKIP encryption.</td> </tr> <tr> <td><i>AES</i></td> <td>Use AES encryption.</td> </tr> <tr> <td><i>TKIP-AES</i></td> <td>Use TKIP and AES encryption.</td> </tr> </tbody> </table>	Option	Description	<i>TKIP</i>	Use TKIP encryption.	<i>AES</i>	Use AES encryption.	<i>TKIP-AES</i>	Use TKIP and AES encryption.			
Option	Description											
<i>TKIP</i>	Use TKIP encryption.											
<i>AES</i>	Use AES encryption.											
<i>TKIP-AES</i>	Use TKIP and AES encryption.											
keyindex	WEP key index .	integer	Minimum value: 1 Maximum value: 4	1								
key	WEP Key.	password	Not Specified									
passphrase	WPA pre-shared key (PSK) to be used to authenticate WiFi users.	password	Not Specified									
sae-password	WPA3 SAE password to be used to authenticate WiFi users.	password	Not Specified									
radius-server	RADIUS server to be used to authenticate WiFi users.	string	Maximum length: 35									
local-standalone	Enable/disable AP local standalone .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AP local standalone.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AP local standalone.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AP local standalone.	<i>disable</i>	Disable AP local standalone.					
Option	Description											
<i>enable</i>	Enable AP local standalone.											
<i>disable</i>	Disable AP local standalone.											
local-standalone-nat	Enable/disable AP local standalone NAT mode.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AP local standalone NAT mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AP local standalone NAT mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AP local standalone NAT mode.	<i>disable</i>	Disable AP local standalone NAT mode.					
Option	Description											
<i>enable</i>	Enable AP local standalone NAT mode.											
<i>disable</i>	Disable AP local standalone NAT mode.											
ip	IP address and subnet mask for the local standalone NAT subnet.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								

Parameter	Description	Type	Size	Default
dhcp-lease-time	DHCP lease time in seconds for NAT IP address.	integer	Minimum value: 300 Maximum value: 8640000	2400
local-bridging	Enable/disable bridging of wireless and Ethernet interfaces on the FortiAP .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AP local VAP to Ethernet bridging.		
	<i>disable</i>	Disable AP local VAP to Ethernet bridging.		
local-lan	Allow/deny traffic destined for a Class A, B, or C private IP address .	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow traffic destined for a Class A, B, or C private IP address.		
	<i>deny</i>	Deny traffic destined for a Class A, B, or C private IP address.		
local-authentication	Enable/disable AP local authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AP local authentication.		
	<i>disable</i>	Disable AP local authentication.		
usergroup <name>	Firewall user group to be used to authenticate WiFi users. User group name.	string	Maximum length: 79	
portal-message-override-group	Replacement message group for this VAP (only available when security is set to a captive portal type).	string	Maximum length: 35	
portal-type	Captive portal functionality. Configure how the captive portal authenticates users and whether it includes a disclaimer.	option	-	auth
	<b>Option</b>	<b>Description</b>		
	<i>auth</i>	Portal for authentication.		
	<i>auth+disclaimer</i>	Portal for authentication and disclaimer.		
	<i>disclaimer</i>	Portal for disclaimer.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>email-collect</i></td> <td>Portal for email collection.</td> </tr> <tr> <td><i>cmcc</i></td> <td>Portal for CMCC.</td> </tr> <tr> <td><i>cmcc-macauth</i></td> <td>Portal for CMCC and MAC authentication.</td> </tr> <tr> <td><i>auth-mac</i></td> <td>Portal for authentication and MAC authentication.</td> </tr> <tr> <td><i>external-auth</i></td> <td>Portal for external portal authentication.</td> </tr> </tbody> </table>	Option	Description	<i>email-collect</i>	Portal for email collection.	<i>cmcc</i>	Portal for CMCC.	<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.	<i>auth-mac</i>	Portal for authentication and MAC authentication.	<i>external-auth</i>	Portal for external portal authentication.			
Option	Description															
<i>email-collect</i>	Portal for email collection.															
<i>cmcc</i>	Portal for CMCC.															
<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.															
<i>auth-mac</i>	Portal for authentication and MAC authentication.															
<i>external-auth</i>	Portal for external portal authentication.															
selected-usergroups <name>	Selective user groups that are permitted to authenticate. User group name.	string	Maximum length: 79													
security-exempt-list	Optional security exempt list for captive portal authentication.	string	Maximum length: 35													
security-redirect-url	Optional URL for redirecting users after they pass captive portal authentication.	string	Maximum length: 127													
intra-vap-privacy	Enable/disable blocking communication between clients on the same SSID .	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable intra-SSID privacy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable intra-SSID privacy.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable intra-SSID privacy.	<i>disable</i>	Disable intra-SSID privacy.									
Option	Description															
<i>enable</i>	Enable intra-SSID privacy.															
<i>disable</i>	Disable intra-SSID privacy.															
schedule <name>	Firewall schedules for enabling this VAP on the FortiAP. This VAP will be enabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35													
ldpc	VAP low-density parity-check (LDPC) coding configuration.	option	-	rxtx												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable LDPC.</td> </tr> <tr> <td><i>rx</i></td> <td>Enable LDPC when receiving traffic.</td> </tr> <tr> <td><i>tx</i></td> <td>Enable LDPC when transmitting traffic.</td> </tr> <tr> <td><i>rxtx</i></td> <td>Enable LDPC when both receiving and transmitting traffic.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable LDPC.	<i>rx</i>	Enable LDPC when receiving traffic.	<i>tx</i>	Enable LDPC when transmitting traffic.	<i>rxtx</i>	Enable LDPC when both receiving and transmitting traffic.					
Option	Description															
<i>disable</i>	Disable LDPC.															
<i>rx</i>	Enable LDPC when receiving traffic.															
<i>tx</i>	Enable LDPC when transmitting traffic.															
<i>rxtx</i>	Enable LDPC when both receiving and transmitting traffic.															
high-efficiency	Enable/disable 802.11ax high efficiency .	option	-	enable												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable 802.11ax high efficiency.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11ax high efficiency.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable 802.11ax high efficiency.	<i>disable</i>	Disable 802.11ax high efficiency.					
Option	Description											
<i>enable</i>	Enable 802.11ax high efficiency.											
<i>disable</i>	Disable 802.11ax high efficiency.											
target-wake-time	Enable/disable 802.11ax target wake time .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable 802.11ax target wake time.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11ax target wake time.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable 802.11ax target wake time.	<i>disable</i>	Disable 802.11ax target wake time.					
Option	Description											
<i>enable</i>	Enable 802.11ax target wake time.											
<i>disable</i>	Disable 802.11ax target wake time.											
port-macauth	Enable/disable LAN port MAC authentication .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable LAN port MAC authentication.</td> </tr> <tr> <td><i>radius</i></td> <td>Enable LAN port RADIUS-based MAC authentication.</td> </tr> <tr> <td><i>address-group</i></td> <td>Enable LAN port address-group based MAC authentication.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable LAN port MAC authentication.	<i>radius</i>	Enable LAN port RADIUS-based MAC authentication.	<i>address-group</i>	Enable LAN port address-group based MAC authentication.			
Option	Description											
<i>disable</i>	Disable LAN port MAC authentication.											
<i>radius</i>	Enable LAN port RADIUS-based MAC authentication.											
<i>address-group</i>	Enable LAN port address-group based MAC authentication.											
port-macauth-timeout	LAN port MAC authentication idle timeout value .	integer	Minimum value: 60 Maximum value: 65535	600								
port-macauth-reauth-timeout	LAN port MAC authentication re-authentication timeout value .	integer	Minimum value: 120 Maximum value: 65535	7200								
bss-color-partial	Enable/disable 802.11ax partial BSS color .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable 802.11ax partial BSS color.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11ax partial BSS color.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable 802.11ax partial BSS color.	<i>disable</i>	Disable 802.11ax partial BSS color.					
Option	Description											
<i>enable</i>	Enable 802.11ax partial BSS color.											
<i>disable</i>	Disable 802.11ax partial BSS color.											
mpsk-profile	MPSK profile name.	string	Maximum length: 35									
split-tunneling	Enable/disable split tunneling .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable split tunneling.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable split tunneling.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable split tunneling.	<i>disable</i>	Disable split tunneling.					
Option	Description											
<i>enable</i>	Enable split tunneling.											
<i>disable</i>	Disable split tunneling.											



Parameter	Description	Type	Size	Default										
vlanid	Optional VLAN ID.	integer	Minimum value: 0 Maximum value: 4094	0										
vlan-auto	Enable/disable automatic management of SSID VLAN interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic management of SSID VLAN interface.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic management of SSID VLAN interface.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic management of SSID VLAN interface.	<i>disable</i>	Disable automatic management of SSID VLAN interface.							
Option	Description													
<i>enable</i>	Enable automatic management of SSID VLAN interface.													
<i>disable</i>	Disable automatic management of SSID VLAN interface.													
dynamic-vlan	Enable/disable dynamic VLAN assignment.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dynamic VLAN assignment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dynamic VLAN assignment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dynamic VLAN assignment.	<i>disable</i>	Disable dynamic VLAN assignment.							
Option	Description													
<i>enable</i>	Enable dynamic VLAN assignment.													
<i>disable</i>	Disable dynamic VLAN assignment.													
captive-portal-ac-name	Local-bridging captive portal ac-name.	string	Maximum length: 35											
captive-portal-auth-timeout	Hard timeout - AP will always clear the session after timeout regardless of traffic .	integer	Minimum value: 0 Maximum value: 864000	0										
multicast-rate	Multicast rate .	option	-	0										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>0</i></td> <td>Use the default multicast rate.</td> </tr> <tr> <td><i>6000</i></td> <td>6 Mbps.</td> </tr> <tr> <td><i>12000</i></td> <td>12 Mbps.</td> </tr> <tr> <td><i>24000</i></td> <td>24 Mbps.</td> </tr> </tbody> </table>	Option	Description	<i>0</i>	Use the default multicast rate.	<i>6000</i>	6 Mbps.	<i>12000</i>	12 Mbps.	<i>24000</i>	24 Mbps.			
Option	Description													
<i>0</i>	Use the default multicast rate.													
<i>6000</i>	6 Mbps.													
<i>12000</i>	12 Mbps.													
<i>24000</i>	24 Mbps.													
multicast-enhance	Enable/disable converting multicast to unicast to improve performance .	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable multicast enhancement.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable multicast enhancement.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multicast enhancement.	<i>disable</i>	Disable multicast enhancement.							
Option	Description													
<i>enable</i>	Enable multicast enhancement.													
<i>disable</i>	Disable multicast enhancement.													
igmp-snooping	Enable/disable IGMP snooping.	option	-	disable										

Parameter	Description	Type	Size	Default																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable IGMP snooping.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable IGMP snooping.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IGMP snooping.	<i>disable</i>	Disable IGMP snooping.																											
Option	Description																																	
<i>enable</i>	Enable IGMP snooping.																																	
<i>disable</i>	Disable IGMP snooping.																																	
broadcast-suppression	Optional suppression of broadcast messages. For example, you can keep DHCP messages, ARP broadcasts, and so on off of the wireless network.	option	-	dhcp-up dhcp-ucast arp-known																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>dhcp-up</i></td> <td>Suppress broadcast uplink DHCP messages.</td> </tr> <tr> <td><i>dhcp-down</i></td> <td>Suppress broadcast downlink DHCP messages.</td> </tr> <tr> <td><i>dhcp-starvation</i></td> <td>Suppress broadcast DHCP starvation req messages.</td> </tr> <tr> <td><i>dhcp-ucast</i></td> <td>Convert downlink broadcast DHCP messages to unicast messages.</td> </tr> <tr> <td><i>arp-known</i></td> <td>Suppress broadcast ARP for known wireless clients.</td> </tr> <tr> <td><i>arp-unknown</i></td> <td>Suppress broadcast ARP for unknown wireless clients.</td> </tr> <tr> <td><i>arp-reply</i></td> <td>Suppress broadcast ARP reply from wireless clients.</td> </tr> <tr> <td><i>arp-poison</i></td> <td>Suppress ARP poison messages from wireless clients.</td> </tr> <tr> <td><i>arp-proxy</i></td> <td>Reply ARP requests for wireless clients as a proxy.</td> </tr> <tr> <td><i>netbios-ns</i></td> <td>Suppress NetBIOS name services packets with UDP port 137.</td> </tr> <tr> <td><i>netbios-ds</i></td> <td>Suppress NetBIOS datagram services packets with UDP port 138.</td> </tr> <tr> <td><i>ipv6</i></td> <td>Suppress IPv6 packets.</td> </tr> <tr> <td><i>all-other-mc</i></td> <td>Suppress all other multicast messages.</td> </tr> <tr> <td><i>all-other-bc</i></td> <td>Suppress all other broadcast messages.</td> </tr> </tbody> </table>	Option	Description	<i>dhcp-up</i>	Suppress broadcast uplink DHCP messages.	<i>dhcp-down</i>	Suppress broadcast downlink DHCP messages.	<i>dhcp-starvation</i>	Suppress broadcast DHCP starvation req messages.	<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.	<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.	<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.	<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.	<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.	<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.	<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.	<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.	<i>ipv6</i>	Suppress IPv6 packets.	<i>all-other-mc</i>	Suppress all other multicast messages.	<i>all-other-bc</i>	Suppress all other broadcast messages.			
Option	Description																																	
<i>dhcp-up</i>	Suppress broadcast uplink DHCP messages.																																	
<i>dhcp-down</i>	Suppress broadcast downlink DHCP messages.																																	
<i>dhcp-starvation</i>	Suppress broadcast DHCP starvation req messages.																																	
<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.																																	
<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.																																	
<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.																																	
<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.																																	
<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.																																	
<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.																																	
<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.																																	
<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.																																	
<i>ipv6</i>	Suppress IPv6 packets.																																	
<i>all-other-mc</i>	Suppress all other multicast messages.																																	
<i>all-other-bc</i>	Suppress all other broadcast messages.																																	
ipv6-rules	Optional rules of IPv6 packets. For example, you can keep RA, RS and so on off of the wireless network.	option	-	drop-icmp6ra drop-icmp6rs drop-llmnr6 drop-icmp6mld2 drop-dhcp6s drop-dhcp6c ndp-proxy drop-ns-dad																														

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>drop-icmp6ra</i></td> <td>Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.</td> </tr> <tr> <td><i>drop-icmp6rs</i></td> <td>Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.</td> </tr> <tr> <td><i>drop-llmnr6</i></td> <td>Drop Link-Local Multicast Name Resolution (LLMNR) packets</td> </tr> <tr> <td><i>drop-icmp6mld2</i></td> <td>Drop ICMP6 Multicast Listener Report V2 (MLD2) packets</td> </tr> <tr> <td><i>drop-dhcp6s</i></td> <td>Drop DHCP6 server generated packets that originate from wireless clients.</td> </tr> <tr> <td><i>drop-dhcp6c</i></td> <td>Drop DHCP6 client generated packets to be sent to wireless clients.</td> </tr> <tr> <td><i>ndp-proxy</i></td> <td>Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.</td> </tr> <tr> <td><i>drop-ns-dad</i></td> <td>Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.</td> </tr> <tr> <td><i>drop-ns-nondad</i></td> <td>Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.</td> </tr> </tbody> </table>	Option	Description	<i>drop-icmp6ra</i>	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.	<i>drop-icmp6rs</i>	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.	<i>drop-llmnr6</i>	Drop Link-Local Multicast Name Resolution (LLMNR) packets	<i>drop-icmp6mld2</i>	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets	<i>drop-dhcp6s</i>	Drop DHCP6 server generated packets that originate from wireless clients.	<i>drop-dhcp6c</i>	Drop DHCP6 client generated packets to be sent to wireless clients.	<i>ndp-proxy</i>	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.	<i>drop-ns-dad</i>	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.	<i>drop-ns-nondad</i>	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.			
Option	Description																							
<i>drop-icmp6ra</i>	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.																							
<i>drop-icmp6rs</i>	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.																							
<i>drop-llmnr6</i>	Drop Link-Local Multicast Name Resolution (LLMNR) packets																							
<i>drop-icmp6mld2</i>	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets																							
<i>drop-dhcp6s</i>	Drop DHCP6 server generated packets that originate from wireless clients.																							
<i>drop-dhcp6c</i>	Drop DHCP6 client generated packets to be sent to wireless clients.																							
<i>ndp-proxy</i>	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.																							
<i>drop-ns-dad</i>	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.																							
<i>drop-ns-nondad</i>	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.																							
me-disable-thresh	Disable multicast enhancement when this many clients are receiving multicast traffic.	integer	Minimum value: 2 Maximum value: 256	32																				
mu-mimo	Enable/disable Multi-user MIMO .	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Multi-user MIMO.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Multi-user MIMO.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Multi-user MIMO.	<i>disable</i>	Disable Multi-user MIMO.																	
Option	Description																							
<i>enable</i>	Enable Multi-user MIMO.																							
<i>disable</i>	Disable Multi-user MIMO.																							
probe-resp-suppression	Enable/disable probe response suppression .	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable probe response suppression.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable probe response suppression.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable probe response suppression.	<i>disable</i>	Disable probe response suppression.																	
Option	Description																							
<i>enable</i>	Enable probe response suppression.																							
<i>disable</i>	Disable probe response suppression.																							
probe-resp-threshold	Minimum signal level/threshold in dBm required for the AP response to probe requests .	string	Maximum length: 7	-80																				
radio-sensitivity	Enable/disable software radio sensitivity .	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable software radio sensitivity.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable software radio sensitivity.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable software radio sensitivity.	<i>disable</i>	Disable software radio sensitivity.																	
Option	Description																							
<i>enable</i>	Enable software radio sensitivity.																							
<i>disable</i>	Disable software radio sensitivity.																							

Parameter	Description	Type	Size	Default										
quarantine	Enable/disable station quarantine .	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable station quarantine.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable station quarantine.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable station quarantine.	<i>disable</i>	Disable station quarantine.							
Option	Description													
<i>enable</i>	Enable station quarantine.													
<i>disable</i>	Disable station quarantine.													
radio-5g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 5G band.	string	Maximum length: 7	-76										
radio-2g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 2.4G band .	string	Maximum length: 7	-79										
vlan-pooling	Enable/disable VLAN pooling, to allow grouping of multiple wireless controller VLANs into VLAN pools . When set to wtp-group, VLAN pooling occurs with VLAN assignment by wtp-group.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wtp-group</i></td> <td>Enable VLAN pooling with VLAN assignment by wtp-group.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Enable VLAN pooling with round-robin VLAN assignment.</td> </tr> <tr> <td><i>hash</i></td> <td>Enable VLAN pooling with hash-based VLAN assignment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable VLAN pooling.</td> </tr> </tbody> </table>	Option	Description	<i>wtp-group</i>	Enable VLAN pooling with VLAN assignment by wtp-group.	<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.	<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.	<i>disable</i>	Disable VLAN pooling.			
Option	Description													
<i>wtp-group</i>	Enable VLAN pooling with VLAN assignment by wtp-group.													
<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.													
<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.													
<i>disable</i>	Disable VLAN pooling.													
dhcp-option43-insertion	Enable/disable insertion of DHCP option 43 .	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable insertion of DHCP option 43.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable insertion of DHCP option 43.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable insertion of DHCP option 43.	<i>disable</i>	Disable insertion of DHCP option 43.							
Option	Description													
<i>enable</i>	Enable insertion of DHCP option 43.													
<i>disable</i>	Disable insertion of DHCP option 43.													
dhcp-option82-insertion	Enable/disable DHCP option 82 insert .	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable DHCP option 82 insert.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP option 82 insert.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DHCP option 82 insert.	<i>disable</i>	Disable DHCP option 82 insert.							
Option	Description													
<i>enable</i>	Enable DHCP option 82 insert.													
<i>disable</i>	Disable DHCP option 82 insert.													
dhcp-option82-circuit-id-insertion	Enable/disable DHCP option 82 circuit-id insert .	option	-	disable										

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>style-1</i></td> <td>ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".</td> </tr> <tr> <td><i>style-2</i></td> <td>ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".</td> </tr> <tr> <td><i>style-3</i></td> <td>ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP option 82 circuit-id insert.</td> </tr> </tbody> </table>	Option	Description	<i>style-1</i>	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".	<i>style-2</i>	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".	<i>style-3</i>	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".	<i>disable</i>	Disable DHCP option 82 circuit-id insert.			
Option	Description													
<i>style-1</i>	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".													
<i>style-2</i>	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".													
<i>style-3</i>	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".													
<i>disable</i>	Disable DHCP option 82 circuit-id insert.													
dhcp-option82-remote-id-insertion	Enable/disable DHCP option 82 remote-id insert .	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>style-1</i></td> <td>ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable DHCP option 82 remote-id insert.</td> </tr> </tbody> </table>	Option	Description	<i>style-1</i>	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.	<i>disable</i>	Disable DHCP option 82 remote-id insert.							
Option	Description													
<i>style-1</i>	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.													
<i>disable</i>	Disable DHCP option 82 remote-id insert.													
ptk-rekey	Enable/disable PTK rekey for WPA-Enterprise security.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable PTK rekey for WPA-Enterprise security.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable PTK rekey for WPA-Enterprise security.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.	<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.							
Option	Description													
<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.													
<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.													
ptk-rekey-intv	PTK rekey interval .	integer	Minimum value: 1800 Maximum value: 864000	86400										
gtk-rekey	Enable/disable GTK rekey for WPA security.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable GTK rekey for WPA security.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable GTK rekey for WPA security.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable GTK rekey for WPA security.	<i>disable</i>	Disable GTK rekey for WPA security.							
Option	Description													
<i>enable</i>	Enable GTK rekey for WPA security.													
<i>disable</i>	Disable GTK rekey for WPA security.													
gtk-rekey-intv	GTK rekey interval .	integer	Minimum value: 1800 Maximum value: 864000	86400										

Parameter	Description	Type	Size	Default												
eap-reauth	Enable/disable EAP re-authentication for WPA-Enterprise security.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable EAP re-authentication for WPA-Enterprise security.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable EAP re-authentication for WPA-Enterprise security.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.	<i>disable</i>	Disable EAP re-authentication for WPA-Enterprise security.									
Option	Description															
<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.															
<i>disable</i>	Disable EAP re-authentication for WPA-Enterprise security.															
eap-reauth-intv	EAP re-authentication interval .	integer	Minimum value: 1800 Maximum value: 864000	86400												
qos-profile	Quality of service profile name.	string	Maximum length: 35													
hotspot20-profile	Hotspot 2.0 profile name.	string	Maximum length: 35													
access-control-list	access-control-list profile name.	string	Maximum length: 35													
primary-wag-profile	Primary wireless access gateway profile name.	string	Maximum length: 35													
secondary-wag-profile	Secondary wireless access gateway profile name.	string	Maximum length: 35													
tunnel-echo-interval	The time interval to send echo to both primary and secondary tunnel peers .	integer	Minimum value: 1 Maximum value: 65535	300												
tunnel-fallback-interval	The time interval for secondary tunnel to fall back to primary tunnel .	integer	Minimum value: 0 Maximum value: 65535	7200												
rates-11a	Allowed data rates for 802.11a.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>1 Mbps supported rate.</td> </tr> <tr> <td><i>1-basic</i></td> <td>1 Mbps BSS basic rate.</td> </tr> <tr> <td><i>2</i></td> <td>2 Mbps supported rate.</td> </tr> <tr> <td><i>2-basic</i></td> <td>2 Mbps BSS basic rate.</td> </tr> <tr> <td><i>5.5</i></td> <td>5.5 Mbps supported rate.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	1 Mbps supported rate.	<i>1-basic</i>	1 Mbps BSS basic rate.	<i>2</i>	2 Mbps supported rate.	<i>2-basic</i>	2 Mbps BSS basic rate.	<i>5.5</i>	5.5 Mbps supported rate.			
Option	Description															
<i>1</i>	1 Mbps supported rate.															
<i>1-basic</i>	1 Mbps BSS basic rate.															
<i>2</i>	2 Mbps supported rate.															
<i>2-basic</i>	2 Mbps BSS basic rate.															
<i>5.5</i>	5.5 Mbps supported rate.															

Parameter	Description	Type	Size	Default																																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>5.5-basic</i></td> <td>5.5 Mbps BSS basic rate.</td> </tr> <tr> <td><i>11</i></td> <td>11 Mbps supported rate.</td> </tr> <tr> <td><i>11-basic</i></td> <td>11 Mbps BSS basic rate.</td> </tr> <tr> <td><i>6</i></td> <td>6 Mbps supported rate.</td> </tr> <tr> <td><i>6-basic</i></td> <td>6 Mbps BSS basic rate.</td> </tr> <tr> <td><i>9</i></td> <td>9 Mbps supported rate.</td> </tr> <tr> <td><i>9-basic</i></td> <td>9 Mbps BSS basic rate.</td> </tr> <tr> <td><i>12</i></td> <td>12 Mbps supported rate.</td> </tr> <tr> <td><i>12-basic</i></td> <td>12 Mbps BSS basic rate.</td> </tr> <tr> <td><i>18</i></td> <td>18 Mbps supported rate.</td> </tr> <tr> <td><i>18-basic</i></td> <td>18 Mbps BSS basic rate.</td> </tr> <tr> <td><i>24</i></td> <td>24 Mbps supported rate.</td> </tr> <tr> <td><i>24-basic</i></td> <td>24 Mbps BSS basic rate.</td> </tr> <tr> <td><i>36</i></td> <td>36 Mbps supported rate.</td> </tr> <tr> <td><i>36-basic</i></td> <td>36 Mbps BSS basic rate.</td> </tr> <tr> <td><i>48</i></td> <td>48 Mbps supported rate.</td> </tr> <tr> <td><i>48-basic</i></td> <td>48 Mbps BSS basic rate.</td> </tr> <tr> <td><i>54</i></td> <td>54 Mbps supported rate.</td> </tr> <tr> <td><i>54-basic</i></td> <td>54 Mbps BSS basic rate.</td> </tr> </tbody> </table>	Option	Description	<i>5.5-basic</i>	5.5 Mbps BSS basic rate.	<i>11</i>	11 Mbps supported rate.	<i>11-basic</i>	11 Mbps BSS basic rate.	<i>6</i>	6 Mbps supported rate.	<i>6-basic</i>	6 Mbps BSS basic rate.	<i>9</i>	9 Mbps supported rate.	<i>9-basic</i>	9 Mbps BSS basic rate.	<i>12</i>	12 Mbps supported rate.	<i>12-basic</i>	12 Mbps BSS basic rate.	<i>18</i>	18 Mbps supported rate.	<i>18-basic</i>	18 Mbps BSS basic rate.	<i>24</i>	24 Mbps supported rate.	<i>24-basic</i>	24 Mbps BSS basic rate.	<i>36</i>	36 Mbps supported rate.	<i>36-basic</i>	36 Mbps BSS basic rate.	<i>48</i>	48 Mbps supported rate.	<i>48-basic</i>	48 Mbps BSS basic rate.	<i>54</i>	54 Mbps supported rate.	<i>54-basic</i>	54 Mbps BSS basic rate.			
Option	Description																																											
<i>5.5-basic</i>	5.5 Mbps BSS basic rate.																																											
<i>11</i>	11 Mbps supported rate.																																											
<i>11-basic</i>	11 Mbps BSS basic rate.																																											
<i>6</i>	6 Mbps supported rate.																																											
<i>6-basic</i>	6 Mbps BSS basic rate.																																											
<i>9</i>	9 Mbps supported rate.																																											
<i>9-basic</i>	9 Mbps BSS basic rate.																																											
<i>12</i>	12 Mbps supported rate.																																											
<i>12-basic</i>	12 Mbps BSS basic rate.																																											
<i>18</i>	18 Mbps supported rate.																																											
<i>18-basic</i>	18 Mbps BSS basic rate.																																											
<i>24</i>	24 Mbps supported rate.																																											
<i>24-basic</i>	24 Mbps BSS basic rate.																																											
<i>36</i>	36 Mbps supported rate.																																											
<i>36-basic</i>	36 Mbps BSS basic rate.																																											
<i>48</i>	48 Mbps supported rate.																																											
<i>48-basic</i>	48 Mbps BSS basic rate.																																											
<i>54</i>	54 Mbps supported rate.																																											
<i>54-basic</i>	54 Mbps BSS basic rate.																																											
rates-11bg	Allowed data rates for 802.11b/g.	option	-																																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>1</i></td> <td>1 Mbps supported rate.</td> </tr> <tr> <td><i>1-basic</i></td> <td>1 Mbps BSS basic rate.</td> </tr> <tr> <td><i>2</i></td> <td>2 Mbps supported rate.</td> </tr> <tr> <td><i>2-basic</i></td> <td>2 Mbps BSS basic rate.</td> </tr> <tr> <td><i>5.5</i></td> <td>5.5 Mbps supported rate.</td> </tr> <tr> <td><i>5.5-basic</i></td> <td>5.5 Mbps BSS basic rate.</td> </tr> <tr> <td><i>11</i></td> <td>11 Mbps supported rate.</td> </tr> </tbody> </table>	Option	Description	<i>1</i>	1 Mbps supported rate.	<i>1-basic</i>	1 Mbps BSS basic rate.	<i>2</i>	2 Mbps supported rate.	<i>2-basic</i>	2 Mbps BSS basic rate.	<i>5.5</i>	5.5 Mbps supported rate.	<i>5.5-basic</i>	5.5 Mbps BSS basic rate.	<i>11</i>	11 Mbps supported rate.																											
Option	Description																																											
<i>1</i>	1 Mbps supported rate.																																											
<i>1-basic</i>	1 Mbps BSS basic rate.																																											
<i>2</i>	2 Mbps supported rate.																																											
<i>2-basic</i>	2 Mbps BSS basic rate.																																											
<i>5.5</i>	5.5 Mbps supported rate.																																											
<i>5.5-basic</i>	5.5 Mbps BSS basic rate.																																											
<i>11</i>	11 Mbps supported rate.																																											

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>11-basic</i></td> <td>11 Mbps BSS basic rate.</td> </tr> <tr> <td><i>6</i></td> <td>6 Mbps supported rate.</td> </tr> <tr> <td><i>6-basic</i></td> <td>6 Mbps BSS basic rate.</td> </tr> <tr> <td><i>9</i></td> <td>9 Mbps supported rate.</td> </tr> <tr> <td><i>9-basic</i></td> <td>9 Mbps BSS basic rate.</td> </tr> <tr> <td><i>12</i></td> <td>12 Mbps supported rate.</td> </tr> <tr> <td><i>12-basic</i></td> <td>12 Mbps BSS basic rate.</td> </tr> <tr> <td><i>18</i></td> <td>18 Mbps supported rate.</td> </tr> <tr> <td><i>18-basic</i></td> <td>18 Mbps BSS basic rate.</td> </tr> <tr> <td><i>24</i></td> <td>24 Mbps supported rate.</td> </tr> <tr> <td><i>24-basic</i></td> <td>24 Mbps BSS basic rate.</td> </tr> <tr> <td><i>36</i></td> <td>36 Mbps supported rate.</td> </tr> <tr> <td><i>36-basic</i></td> <td>36 Mbps BSS basic rate.</td> </tr> <tr> <td><i>48</i></td> <td>48 Mbps supported rate.</td> </tr> <tr> <td><i>48-basic</i></td> <td>48 Mbps BSS basic rate.</td> </tr> <tr> <td><i>54</i></td> <td>54 Mbps supported rate.</td> </tr> <tr> <td><i>54-basic</i></td> <td>54 Mbps BSS basic rate.</td> </tr> </tbody> </table>	Option	Description	<i>11-basic</i>	11 Mbps BSS basic rate.	<i>6</i>	6 Mbps supported rate.	<i>6-basic</i>	6 Mbps BSS basic rate.	<i>9</i>	9 Mbps supported rate.	<i>9-basic</i>	9 Mbps BSS basic rate.	<i>12</i>	12 Mbps supported rate.	<i>12-basic</i>	12 Mbps BSS basic rate.	<i>18</i>	18 Mbps supported rate.	<i>18-basic</i>	18 Mbps BSS basic rate.	<i>24</i>	24 Mbps supported rate.	<i>24-basic</i>	24 Mbps BSS basic rate.	<i>36</i>	36 Mbps supported rate.	<i>36-basic</i>	36 Mbps BSS basic rate.	<i>48</i>	48 Mbps supported rate.	<i>48-basic</i>	48 Mbps BSS basic rate.	<i>54</i>	54 Mbps supported rate.	<i>54-basic</i>	54 Mbps BSS basic rate.			
Option	Description																																							
<i>11-basic</i>	11 Mbps BSS basic rate.																																							
<i>6</i>	6 Mbps supported rate.																																							
<i>6-basic</i>	6 Mbps BSS basic rate.																																							
<i>9</i>	9 Mbps supported rate.																																							
<i>9-basic</i>	9 Mbps BSS basic rate.																																							
<i>12</i>	12 Mbps supported rate.																																							
<i>12-basic</i>	12 Mbps BSS basic rate.																																							
<i>18</i>	18 Mbps supported rate.																																							
<i>18-basic</i>	18 Mbps BSS basic rate.																																							
<i>24</i>	24 Mbps supported rate.																																							
<i>24-basic</i>	24 Mbps BSS basic rate.																																							
<i>36</i>	36 Mbps supported rate.																																							
<i>36-basic</i>	36 Mbps BSS basic rate.																																							
<i>48</i>	48 Mbps supported rate.																																							
<i>48-basic</i>	48 Mbps BSS basic rate.																																							
<i>54</i>	54 Mbps supported rate.																																							
<i>54-basic</i>	54 Mbps BSS basic rate.																																							
rates-11n-ss12	Allowed data rates for 802.11n with 1 or 2 spatial streams.	option	-																																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mcs0/1</i></td> <td>Data rate for MCS index 0 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs1/1</i></td> <td>Data rate for MCS index 1 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs2/1</i></td> <td>Data rate for MCS index 2 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs3/1</i></td> <td>Data rate for MCS index 3 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs4/1</i></td> <td>Data rate for MCS index 4 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs5/1</i></td> <td>Data rate for MCS index 5 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs6/1</i></td> <td>Data rate for MCS index 6 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs7/1</i></td> <td>Data rate for MCS index 7 with 1 spatial stream.</td> </tr> </tbody> </table>	Option	Description	<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.																					
Option	Description																																							
<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.																																							
<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.																																							
<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.																																							
<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.																																							
<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.																																							
<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.																																							
<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.																																							
<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.																																							



Parameter	Description	Type	Size	Default																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mcs8/2</i></td> <td>Data rate for MCS index 8 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs9/2</i></td> <td>Data rate for MCS index 9 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs10/2</i></td> <td>Data rate for MCS index 10 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs11/2</i></td> <td>Data rate for MCS index 11 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs12/2</i></td> <td>Data rate for MCS index 12 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs13/2</i></td> <td>Data rate for MCS index 13 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs14/2</i></td> <td>Data rate for MCS index 14 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs15/2</i></td> <td>Data rate for MCS index 15 with 2 spatial streams.</td> </tr> </tbody> </table>	Option	Description	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.	<i>mcs12/2</i>	Data rate for MCS index 12 with 2 spatial streams.	<i>mcs13/2</i>	Data rate for MCS index 13 with 2 spatial streams.	<i>mcs14/2</i>	Data rate for MCS index 14 with 2 spatial streams.	<i>mcs15/2</i>	Data rate for MCS index 15 with 2 spatial streams.																			
Option	Description																																					
<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.																																					
<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.																																					
<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.																																					
<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.																																					
<i>mcs12/2</i>	Data rate for MCS index 12 with 2 spatial streams.																																					
<i>mcs13/2</i>	Data rate for MCS index 13 with 2 spatial streams.																																					
<i>mcs14/2</i>	Data rate for MCS index 14 with 2 spatial streams.																																					
<i>mcs15/2</i>	Data rate for MCS index 15 with 2 spatial streams.																																					
rates-11n-ss34	Allowed data rates for 802.11n with 3 or 4 spatial streams.	option	-																																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mcs16/3</i></td> <td>Data rate for MCS index 16 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs17/3</i></td> <td>Data rate for MCS index 17 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs18/3</i></td> <td>Data rate for MCS index 18 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs19/3</i></td> <td>Data rate for MCS index 19 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs20/3</i></td> <td>Data rate for MCS index 20 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs21/3</i></td> <td>Data rate for MCS index 21 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs22/3</i></td> <td>Data rate for MCS index 22 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs23/3</i></td> <td>Data rate for MCS index 23 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs24/4</i></td> <td>Data rate for MCS index 24 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs25/4</i></td> <td>Data rate for MCS index 25 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs26/4</i></td> <td>Data rate for MCS index 26 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs27/4</i></td> <td>Data rate for MCS index 27 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs28/4</i></td> <td>Data rate for MCS index 28 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs29/4</i></td> <td>Data rate for MCS index 29 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs30/4</i></td> <td>Data rate for MCS index 30 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs31/4</i></td> <td>Data rate for MCS index 31 with 4 spatial streams.</td> </tr> </tbody> </table>	Option	Description	<i>mcs16/3</i>	Data rate for MCS index 16 with 3 spatial streams.	<i>mcs17/3</i>	Data rate for MCS index 17 with 3 spatial streams.	<i>mcs18/3</i>	Data rate for MCS index 18 with 3 spatial streams.	<i>mcs19/3</i>	Data rate for MCS index 19 with 3 spatial streams.	<i>mcs20/3</i>	Data rate for MCS index 20 with 3 spatial streams.	<i>mcs21/3</i>	Data rate for MCS index 21 with 3 spatial streams.	<i>mcs22/3</i>	Data rate for MCS index 22 with 3 spatial streams.	<i>mcs23/3</i>	Data rate for MCS index 23 with 3 spatial streams.	<i>mcs24/4</i>	Data rate for MCS index 24 with 4 spatial streams.	<i>mcs25/4</i>	Data rate for MCS index 25 with 4 spatial streams.	<i>mcs26/4</i>	Data rate for MCS index 26 with 4 spatial streams.	<i>mcs27/4</i>	Data rate for MCS index 27 with 4 spatial streams.	<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.	<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.	<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.	<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.			
Option	Description																																					
<i>mcs16/3</i>	Data rate for MCS index 16 with 3 spatial streams.																																					
<i>mcs17/3</i>	Data rate for MCS index 17 with 3 spatial streams.																																					
<i>mcs18/3</i>	Data rate for MCS index 18 with 3 spatial streams.																																					
<i>mcs19/3</i>	Data rate for MCS index 19 with 3 spatial streams.																																					
<i>mcs20/3</i>	Data rate for MCS index 20 with 3 spatial streams.																																					
<i>mcs21/3</i>	Data rate for MCS index 21 with 3 spatial streams.																																					
<i>mcs22/3</i>	Data rate for MCS index 22 with 3 spatial streams.																																					
<i>mcs23/3</i>	Data rate for MCS index 23 with 3 spatial streams.																																					
<i>mcs24/4</i>	Data rate for MCS index 24 with 4 spatial streams.																																					
<i>mcs25/4</i>	Data rate for MCS index 25 with 4 spatial streams.																																					
<i>mcs26/4</i>	Data rate for MCS index 26 with 4 spatial streams.																																					
<i>mcs27/4</i>	Data rate for MCS index 27 with 4 spatial streams.																																					
<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.																																					
<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.																																					
<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.																																					
<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.																																					
rates-11ac-ss12	Allowed data rates for 802.11ac/ax with 1 or 2 spatial streams.	option	-																																			

Parameter	Description	Type	Size	Default																																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mcs0/1</i></td> <td>Data rate for MCS index 0 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs1/1</i></td> <td>Data rate for MCS index 1 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs2/1</i></td> <td>Data rate for MCS index 2 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs3/1</i></td> <td>Data rate for MCS index 3 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs4/1</i></td> <td>Data rate for MCS index 4 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs5/1</i></td> <td>Data rate for MCS index 5 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs6/1</i></td> <td>Data rate for MCS index 6 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs7/1</i></td> <td>Data rate for MCS index 7 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs8/1</i></td> <td>Data rate for MCS index 8 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs9/1</i></td> <td>Data rate for MCS index 9 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs10/1</i></td> <td>Data rate for MCS index 10 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs11/1</i></td> <td>Data rate for MCS index 11 with 1 spatial stream.</td> </tr> <tr> <td><i>mcs0/2</i></td> <td>Data rate for MCS index 0 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs1/2</i></td> <td>Data rate for MCS index 1 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs2/2</i></td> <td>Data rate for MCS index 2 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs3/2</i></td> <td>Data rate for MCS index 3 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs4/2</i></td> <td>Data rate for MCS index 4 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs5/2</i></td> <td>Data rate for MCS index 5 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs6/2</i></td> <td>Data rate for MCS index 6 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs7/2</i></td> <td>Data rate for MCS index 7 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs8/2</i></td> <td>Data rate for MCS index 8 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs9/2</i></td> <td>Data rate for MCS index 9 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs10/2</i></td> <td>Data rate for MCS index 10 with 2 spatial streams.</td> </tr> <tr> <td><i>mcs11/2</i></td> <td>Data rate for MCS index 11 with 2 spatial streams.</td> </tr> </tbody> </table>	Option	Description	<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.			
Option	Description																																																					
<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.																																																					
<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.																																																					
<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.																																																					
<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.																																																					
<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.																																																					
<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.																																																					
<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.																																																					
<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.																																																					
<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.																																																					
<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.																																																					
<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.																																																					
<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.																																																					
<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.																																																					
<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.																																																					
<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.																																																					
<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.																																																					
<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.																																																					
<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.																																																					
<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.																																																					
<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.																																																					
<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.																																																					
<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.																																																					
<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.																																																					
<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.																																																					
rates-11ac-ss34	Allowed data rates for 802.11ac/ax with 3 or 4 spatial streams.	option	-																																																			
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mcs0/3</i></td> <td>Data rate for MCS index 0 with 3 spatial streams.</td> </tr> </tbody> </table>	Option	Description	<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.																																																	
Option	Description																																																					
<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.																																																					

Parameter	Description	Type	Size	Default																																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mcs1/3</i></td> <td>Data rate for MCS index 1 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs2/3</i></td> <td>Data rate for MCS index 2 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs3/3</i></td> <td>Data rate for MCS index 3 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs4/3</i></td> <td>Data rate for MCS index 4 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs5/3</i></td> <td>Data rate for MCS index 5 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs6/3</i></td> <td>Data rate for MCS index 6 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs7/3</i></td> <td>Data rate for MCS index 7 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs8/3</i></td> <td>Data rate for MCS index 8 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs9/3</i></td> <td>Data rate for MCS index 9 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs10/3</i></td> <td>Data rate for MCS index 10 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs11/3</i></td> <td>Data rate for MCS index 11 with 3 spatial streams.</td> </tr> <tr> <td><i>mcs0/4</i></td> <td>Data rate for MCS index 0 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs1/4</i></td> <td>Data rate for MCS index 1 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs2/4</i></td> <td>Data rate for MCS index 2 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs3/4</i></td> <td>Data rate for MCS index 3 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs4/4</i></td> <td>Data rate for MCS index 4 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs5/4</i></td> <td>Data rate for MCS index 5 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs6/4</i></td> <td>Data rate for MCS index 6 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs7/4</i></td> <td>Data rate for MCS index 7 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs8/4</i></td> <td>Data rate for MCS index 8 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs9/4</i></td> <td>Data rate for MCS index 9 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs10/4</i></td> <td>Data rate for MCS index 10 with 4 spatial streams.</td> </tr> <tr> <td><i>mcs11/4</i></td> <td>Data rate for MCS index 11 with 4 spatial streams.</td> </tr> </tbody> </table>	Option	Description	<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.	<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.	<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.	<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.	<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.	<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.	<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.	<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.	<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.	<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.	<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.	<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.	<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.	<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.	<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.	<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.	<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.	<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.	<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.	<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.	<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.	<i>mcs10/4</i>	Data rate for MCS index 10 with 4 spatial streams.	<i>mcs11/4</i>	Data rate for MCS index 11 with 4 spatial streams.			
Option	Description																																																			
<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.																																																			
<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.																																																			
<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.																																																			
<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.																																																			
<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.																																																			
<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.																																																			
<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.																																																			
<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.																																																			
<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.																																																			
<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.																																																			
<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.																																																			
<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.																																																			
<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.																																																			
<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.																																																			
<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.																																																			
<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.																																																			
<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.																																																			
<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.																																																			
<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.																																																			
<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.																																																			
<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.																																																			
<i>mcs10/4</i>	Data rate for MCS index 10 with 4 spatial streams.																																																			
<i>mcs11/4</i>	Data rate for MCS index 11 with 4 spatial streams.																																																			
utm-profile	UTM profile name.	string	Maximum length: 35																																																	
address-group	Address group ID.	string	Maximum length: 35																																																	
mac-filter	Enable/disable MAC filtering to block wireless clients by mac address.	option	-	disable																																																

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable MAC filtering.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable MAC filtering.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable MAC filtering.	<i>disable</i>	Disable MAC filtering.			
Option	Description									
<i>enable</i>	Enable MAC filtering.									
<i>disable</i>	Disable MAC filtering.									
mac-filter-policy-other	Allow or block clients with MAC addresses that are not in the filter list.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>allow</i></td> <td>Allow clients with MAC addresses that are not in the filter list.</td> </tr> <tr> <td><i>deny</i></td> <td>Block clients with MAC addresses that are not in the filter list.</td> </tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.	<i>deny</i>	Block clients with MAC addresses that are not in the filter list.			
Option	Description									
<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.									
<i>deny</i>	Block clients with MAC addresses that are not in the filter list.									
sticky-client-remove	Enable/disable sticky client remove to maintain good signal level clients in SSID. .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Sticky Client Remove.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Sticky Client Remove.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Sticky Client Remove.	<i>disable</i>	Disable Sticky Client Remove.			
Option	Description									
<i>enable</i>	Enable Sticky Client Remove.									
<i>disable</i>	Disable Sticky Client Remove.									
sticky-client-threshold-5g	Minimum signal level/threshold in dBm required for the 5G client to be serviced by the AP .	string	Maximum length: 7	-76						
sticky-client-threshold-2g	Minimum signal level/threshold in dBm required for the 2G client to be serviced by the AP .	string	Maximum length: 7	-79						

### config portal-message-overrides

Parameter	Description	Type	Size	Default
auth-disclaimer-page	Override auth-disclaimer-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-reject-page	Override auth-reject-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-page	Override auth-login-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-failed-page	Override auth-login-failed-page message with message from portal-message-overrides group.	string	Maximum length: 35	

### config vlan-pool

Parameter	Description	Type	Size	Default
wtp-group	WTP group name.	string	Maximum length: 35	

## config mac-filter-list

Parameter	Description	Type	Size	Default						
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00						
mac-filter-policy	Deny or allow the client with this MAC address.	option	-	deny						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>allow</i></td><td>Allow the client with this MAC address.</td></tr><tr><td><i>deny</i></td><td>Block the client with this MAC address.</td></tr></tbody></table>	Option	Description	<i>allow</i>	Allow the client with this MAC address.	<i>deny</i>	Block the client with this MAC address.			
Option	Description									
<i>allow</i>	Allow the client with this MAC address.									
<i>deny</i>	Block the client with this MAC address.									

## config wireless-controller timers

Configure CAPWAP timers.

```
config wireless-controller timers
  Description: Configure CAPWAP timers.
  set echo-interval {integer}
  set discovery-interval {integer}
  set client-idle-timeout {integer}
  set rogue-ap-log {integer}
  set fake-ap-log {integer}
  set sta-stats-interval {integer}
  set vap-stats-interval {integer}
  set radio-stats-interval {integer}
  set sta-capability-interval {integer}
  set sta-locate-timer {integer}
  set ipsec-intf-cleanup {integer}
  set ble-scan-report-intv {integer}
  set drma-interval {integer}
end
```

## config wireless-controller timers

Parameter	Description	Type	Size	Default
echo-interval	Time between echo requests sent by the managed WTP, AP, or FortiAP .	integer	Minimum value: 1 Maximum value: 255	30
discovery-interval	Time between discovery requests .	integer	Minimum value: 2 Maximum value: 180	5

Parameter	Description	Type	Size	Default
client-idle-timeout	Time after which a client is considered idle and times out .	integer	Minimum value: 20 Maximum value: 3600	300
rogue-ap-log	Time between logging rogue AP messages if periodic rogue AP logging is configured .	integer	Minimum value: 0 Maximum value: 1440	0
fake-ap-log	Time between recording logs about fake APs if periodic fake AP logging is configured .	integer	Minimum value: 1 Maximum value: 1440	1
sta-stats-interval	Time between running client .	integer	Minimum value: 1 Maximum value: 255	1
vap-stats-interval	Time between running Virtual Access Point .	integer	Minimum value: 1 Maximum value: 255	15
radio-stats-interval	Time between running radio reports .	integer	Minimum value: 1 Maximum value: 255	15
sta-capability-interval	Time between running station capability reports .	integer	Minimum value: 1 Maximum value: 255	30
sta-locate-timer	Time between running client presence flushes to remove clients that are listed but no longer present .	integer	Minimum value: 0 Maximum value: 86400	1800
ipsec-intf-cleanup	Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected .	integer	Minimum value: 30 Maximum value: 3600	120
ble-scan-report-intv	Time between running Bluetooth Low Energy .	integer	Minimum value: 10 Maximum value: 3600	30

Parameter	Description	Type	Size	Default
drma-interval	Dynamic radio mode assignment .	integer	Minimum value: 1 Maximum value: 1440	60

## config wireless-controller setting

VDOM wireless controller configuration.

```
config wireless-controller setting
  Description: VDOM wireless controller configuration.
  set account-id {string}
  set country [NA|AF|...]
  set duplicate-ssid [enable|disable]
  set fapc-compatibility [enable|disable]
  set wfa-compatibility [enable|disable]
  set phishing-ssid-detect [enable|disable]
  set fake-ssid-action {option1}, {option2}, ...
  config offending-ssid
    Description: Configure offending SSID.
    edit <id>
      set ssid-pattern {string}
      set action {option1}, {option2}, ...
    next
  end
  set device-weight {integer}
  set device-holdoff {integer}
  set device-idle {integer}
  set darrp-optimize {integer}
  set darrp-optimize-schedules <name1>, <name2>, ...
end
```

## config wireless-controller setting

Parameter	Description	Type	Size	Default						
account-id	FortiCloud customer account ID.	string	Maximum length: 63							
country	Country or region in which the FortiGate is located. The country determines the 802.11 bands and channels that are available.	option	-	US						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>NA</td> <td>NO_COUNTRY_SET</td> </tr> <tr> <td>AF</td> <td>AFGHANISTAN</td> </tr> </tbody> </table>	Option	Description	NA	NO_COUNTRY_SET	AF	AFGHANISTAN			
Option	Description									
NA	NO_COUNTRY_SET									
AF	AFGHANISTAN									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>AL</i>	ALBANIA		
	<i>DZ</i>	ALGERIA		
	<i>AS</i>	AMERICAN SAMOA		
	<i>AO</i>	ANGOLA		
	<i>AR</i>	ARGENTINA		
	<i>AM</i>	ARMENIA		
	<i>AU</i>	AUSTRALIA		
	<i>AT</i>	AUSTRIA		
	<i>AZ</i>	AZERBAIJAN		
	<i>BS</i>	BAHAMAS		
	<i>BH</i>	BAHRAIN		
	<i>BD</i>	BANGLADESH		
	<i>BB</i>	BARBADOS		
	<i>BY</i>	BELARUS		
	<i>BE</i>	BELGIUM		
	<i>BZ</i>	BELIZE		
	<i>BJ</i>	BENIN		
	<i>BM</i>	BERMUDA		
	<i>BT</i>	BHUTAN		
	<i>BO</i>	BOLIVIA		
	<i>BA</i>	BOSNIA AND HERZEGOVINA		
	<i>BW</i>	BOTSWANA		
	<i>BR</i>	BRAZIL		
	<i>BN</i>	BRUNEI DARUSSALAM		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GE</i>	GEORGIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		
	<i>CI</i>	COTE_D_IVOIRE		
	<i>JM</i>	JAMAICA		
	<i>JO</i>	JORDAN		
	<i>KZ</i>	KAZAKHSTAN		
	<i>KE</i>	KENYA		
	<i>KR</i>	KOREA REPUBLIC		
	<i>KW</i>	KUWAIT		
	<i>LA</i>	LAOS		
	<i>LV</i>	LATVIA		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>LB</i>	LEBANON		
	<i>LS</i>	LESOTHO		
	<i>LY</i>	LIBYA		
	<i>LI</i>	LIECHTENSTEIN		
	<i>LT</i>	LITHUANIA		
	<i>LU</i>	LUXEMBOURG		
	<i>MO</i>	MACAU SAR		
	<i>MK</i>	MACEDONIA, FYRO		
	<i>MG</i>	MADAGASCAR		
	<i>MW</i>	MALAWI		
	<i>MY</i>	MALAYSIA		
	<i>MV</i>	MALDIVES		
	<i>ML</i>	MALI		
	<i>MT</i>	MALTA		
	<i>MH</i>	MARSHALL ISLANDS		
	<i>MQ</i>	MARTINIQUE		
	<i>MR</i>	MAURITANIA		
	<i>MU</i>	MAURITIUS		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		
	<i>MC</i>	MONACO		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NO</i>	NORWAY		
	<i>MP</i>	NORTHERN MARIANA ISLANDS		
	<i>OM</i>	OMAN		
	<i>PK</i>	PAKISTAN		
	<i>PW</i>	PALAU		
	<i>PA</i>	PANAMA		
	<i>PG</i>	PAPUA NEW GUINEA		
	<i>PY</i>	PARAGUAY		
	<i>PE</i>	PERU		
	<i>PH</i>	PHILIPPINES		
	<i>PL</i>	POLAND		
	<i>PT</i>	PORTUGAL		
	<i>PR</i>	PUERTO RICO		
	<i>QA</i>	QATAR		
	<i>RE</i>	REUNION		
	<i>RO</i>	ROMANIA		
	<i>RU</i>	RUSSIA		
	<i>RW</i>	RWANDA		
	<i>BL</i>	SAINT BARTHELEMY		
	<i>KN</i>	SAINT KITTS AND NEVIS		
	<i>LC</i>	SAINT LUCIA		
	<i>MF</i>	SAINT MARTIN		
	<i>PM</i>	SAINT PIERRE AND MIQUELON		
	<i>VC</i>	SAINT VINCENT AND GRENADIENS		
	<i>SA</i>	SAUDI ARABIA		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>SN</i>	SENEGAL		
	<i>RS</i>	REPUBLIC OF SERBIA		
	<i>ME</i>	MONTENEGRO		
	<i>SL</i>	SIERRA LEONE		
	<i>SG</i>	SINGAPORE		
	<i>SK</i>	SLOVAKIA		
	<i>SI</i>	SLOVENIA		
	<i>ZA</i>	SOUTH AFRICA		
	<i>ES</i>	SPAIN		
	<i>LK</i>	SRI LANKA		
	<i>SE</i>	SWEDEN		
	<i>SR</i>	SURINAME		
	<i>CH</i>	SWITZERLAND		
	<i>TW</i>	TAIWAN		
	<i>TZ</i>	TANZANIA		
	<i>TH</i>	THAILAND		
	<i>TG</i>	TOGO		
	<i>TT</i>	TRINIDAD AND TOBAGO		
	<i>TN</i>	TUNISIA		
	<i>TR</i>	TURKEY		
	<i>TM</i>	TURKMENISTAN		
	<i>AE</i>	UNITED ARAB EMIRATES		
	<i>TC</i>	TURKS AND CAICOS		
	<i>UG</i>	UGANDA		
	<i>UA</i>	UKRAINE		
	<i>GB</i>	UNITED KINGDOM		
	<i>US</i>	UNITED STATES2		
	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)		
	<i>UY</i>	URUGUAY		

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>UZ</i></td> <td>UZBEKISTAN</td> </tr> <tr> <td><i>VU</i></td> <td>VANUATU</td> </tr> <tr> <td><i>VE</i></td> <td>VENEZUELA</td> </tr> <tr> <td><i>VN</i></td> <td>VIET NAM</td> </tr> <tr> <td><i>VI</i></td> <td>VIRGIN ISLANDS</td> </tr> <tr> <td><i>WF</i></td> <td>WALLIS AND FUTUNA</td> </tr> <tr> <td><i>YE</i></td> <td>YEMEN</td> </tr> <tr> <td><i>ZM</i></td> <td>ZAMBIA</td> </tr> <tr> <td><i>ZW</i></td> <td>ZIMBABWE</td> </tr> <tr> <td><i>JP</i></td> <td>JAPAN14</td> </tr> <tr> <td><i>CA</i></td> <td>CANADA2</td> </tr> </tbody> </table>	Option	Description	<i>UZ</i>	UZBEKISTAN	<i>VU</i>	VANUATU	<i>VE</i>	VENEZUELA	<i>VN</i>	VIET NAM	<i>VI</i>	VIRGIN ISLANDS	<i>WF</i>	WALLIS AND FUTUNA	<i>YE</i>	YEMEN	<i>ZM</i>	ZAMBIA	<i>ZW</i>	ZIMBABWE	<i>JP</i>	JAPAN14	<i>CA</i>	CANADA2			
Option	Description																											
<i>UZ</i>	UZBEKISTAN																											
<i>VU</i>	VANUATU																											
<i>VE</i>	VENEZUELA																											
<i>VN</i>	VIET NAM																											
<i>VI</i>	VIRGIN ISLANDS																											
<i>WF</i>	WALLIS AND FUTUNA																											
<i>YE</i>	YEMEN																											
<i>ZM</i>	ZAMBIA																											
<i>ZW</i>	ZIMBABWE																											
<i>JP</i>	JAPAN14																											
<i>CA</i>	CANADA2																											
duplicate-ssid	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow VAPs to use the same SSID name in the same VDOM.</td> </tr> <tr> <td><i>disable</i></td> <td>Do not allow VAPs to use the same SSID name in the same VDOM.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow VAPs to use the same SSID name in the same VDOM.	<i>disable</i>	Do not allow VAPs to use the same SSID name in the same VDOM.																					
Option	Description																											
<i>enable</i>	Allow VAPs to use the same SSID name in the same VDOM.																											
<i>disable</i>	Do not allow VAPs to use the same SSID name in the same VDOM.																											
fapc-compatibility	Enable/disable FAP-C series compatibility.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FAP-C series compatibility.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FAP-C series compatibility.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FAP-C series compatibility.	<i>disable</i>	Disable FAP-C series compatibility.																					
Option	Description																											
<i>enable</i>	Enable FAP-C series compatibility.																											
<i>disable</i>	Disable FAP-C series compatibility.																											
wfa-compatibility	Enable/disable WFA compatibility.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Wi-Fi Alliance Certification compatibility.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Wi-Fi Alliance Certification compatibility.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.	<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.																					
Option	Description																											
<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.																											
<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.																											
phishing-ssid-detect	Enable/disable phishing SSID detection.	option	-	enable																								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable phishing SSID detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable phishing SSID detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable phishing SSID detection.	<i>disable</i>	Disable phishing SSID detection.			
Option	Description									
<i>enable</i>	Enable phishing SSID detection.									
<i>disable</i>	Disable phishing SSID detection.									
fake-ssid-action	Actions taken for detected fake SSID.	option	-	log						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>log</i></td> <td>Write logs for detected fake SSID.</td> </tr> <tr> <td><i>suppress</i></td> <td>Suppress detected fake SSID.</td> </tr> </tbody> </table>	Option	Description	<i>log</i>	Write logs for detected fake SSID.	<i>suppress</i>	Suppress detected fake SSID.			
Option	Description									
<i>log</i>	Write logs for detected fake SSID.									
<i>suppress</i>	Suppress detected fake SSID.									
device-weight	Upper limit of confidence of device for identification .	integer	Minimum value: 0 Maximum value: 255	1						
device-holdoff	Lower limit of creation time of device for identification in minutes .	integer	Minimum value: 0 Maximum value: 60	5						
device-idle	Upper limit of idle time of device for identification in minutes .	integer	Minimum value: 0 Maximum value: 14400	1440						
darrp-optimize	Time for running Dynamic Automatic Radio Resource Provisioning .	integer	Minimum value: 0 Maximum value: 86400	86400						
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35							

### config offending-ssid

Parameter	Description	Type	Size	Default
ssid-pattern	Define offending SSID pattern (case insensitive), eg: word, word*, *word, wo*rd.	string	Maximum length: 33	
action	Actions taken for detected offending SSID.	option	-	log

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>log</i></td> <td>Generate logs for detected offending SSID.</td> </tr> <tr> <td><i>suppress</i></td> <td>Suppress detected offending SSID.</td> </tr> </tbody> </table>	Option	Description	<i>log</i>	Generate logs for detected offending SSID.	<i>suppress</i>	Suppress detected offending SSID.			
Option	Description									
<i>log</i>	Generate logs for detected offending SSID.									
<i>suppress</i>	Suppress detected offending SSID.									

## config wireless-controller log

Configure wireless controller event log filters.

```

config wireless-controller log
  Description: Configure wireless controller event log filters.
  set status [enable|disable]
  set addrgrp-log [emergency|alert|...]
  set ble-log [emergency|alert|...]
  set clb-log [emergency|alert|...]
  set dhcp-starv-log [emergency|alert|...]
  set led-sched-log [emergency|alert|...]
  set radio-event-log [emergency|alert|...]
  set rogue-event-log [emergency|alert|...]
  set sta-event-log [emergency|alert|...]
  set sta-locate-log [emergency|alert|...]
  set wids-log [emergency|alert|...]
  set wtp-event-log [emergency|alert|...]
end

```

## config wireless-controller log

Parameter	Description	Type	Size	Default										
status	Enable/disable wireless event logging.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable wireless event logging.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable wireless event logging.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable wireless event logging.	<i>disable</i>	Disable wireless event logging.							
Option	Description													
<i>enable</i>	Enable wireless event logging.													
<i>disable</i>	Disable wireless event logging.													
addrgrp-log	Lowest severity level to log address group message.	option	-	notification										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.			
Option	Description													
<i>emergency</i>	Emergency level.													
<i>alert</i>	Alert level.													
<i>critical</i>	Critical level.													
<i>error</i>	Error level.													



Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.											
Option	Description																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
ble-log	Lowest severity level to log BLE detection message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
clb-log	Lowest severity level to log client load balancing message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
dhcp-starv-log	Lowest severity level to log DHCP starvation event message.	option	-	notification																		

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
led-sched-log	Lowest severity level to log LED schedule event message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
radio-event-log	Lowest severity level to log radio event message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.							
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>information</i>	Information level.	<i>debug</i>	Debug level.															
Option	Description																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
rogue-event-log	Lowest severity level to log rogue AP event message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
sta-event-log	Lowest severity level to log station event message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
sta-locate-log	Lowest severity level to log station locate message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.													
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.									
Option	Description																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
wids-log	Lowest severity level to log WIDS message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
wtp-event-log	Lowest severity level to log WTP event message.	option	-	notification																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>emergency</i></td> <td>Emergency level.</td> </tr> <tr> <td><i>alert</i></td> <td>Alert level.</td> </tr> <tr> <td><i>critical</i></td> <td>Critical level.</td> </tr> <tr> <td><i>error</i></td> <td>Error level.</td> </tr> <tr> <td><i>warning</i></td> <td>Warning level.</td> </tr> <tr> <td><i>notification</i></td> <td>Notification level.</td> </tr> <tr> <td><i>information</i></td> <td>Information level.</td> </tr> <tr> <td><i>debug</i></td> <td>Debug level.</td> </tr> </tbody> </table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

## config wireless-controller apcfg-profile

Configure AP local configuration profiles.

```
config wireless-controller apcfg-profile
  Description: Configure AP local configuration profiles.
```

```

edit <name>
  set ap-family [fap|fap-u|...]
  set comment {var-string}
  set ac-type [default|specify|...]
  set ac-timer {integer}
  set ac-ip {ipv4-address}
  set ac-port {integer}
  config command-list
    Description: AP local configuration command list.
    edit <id>
      set type [non-password|password]
      set name {string}
      set value {string}
      set passwd-value {password}
    next
  end
next
end

```

## config wireless-controller apcfg-profile

Parameter	Description	Type	Size	Default								
ap-family	FortiAP family type .	option	-	fap								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>fap</i></td> <td>FortiAP Family.</td> </tr> <tr> <td><i>fap-u</i></td> <td>FortiAP-U Family.</td> </tr> <tr> <td><i>fap-c</i></td> <td>FortiAP-C Family.</td> </tr> </tbody> </table>	Option	Description	<i>fap</i>	FortiAP Family.	<i>fap-u</i>	FortiAP-U Family.	<i>fap-c</i>	FortiAP-C Family.			
Option	Description											
<i>fap</i>	FortiAP Family.											
<i>fap-u</i>	FortiAP-U Family.											
<i>fap-c</i>	FortiAP-C Family.											
comment	Comment.	var-string	Maximum length: 255									
ac-type	Validation controller type .	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>This controller is the one and only controller that the AP could join after applying AP local configuration.</td> </tr> <tr> <td><i>specify</i></td> <td>Specified controller is the one and only controller that the AP could join after applying AP local configuration.</td> </tr> <tr> <td><i>apcfg</i></td> <td>Any controller defined by AP local configuration after applying AP local configuration.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	This controller is the one and only controller that the AP could join after applying AP local configuration.	<i>specify</i>	Specified controller is the one and only controller that the AP could join after applying AP local configuration.	<i>apcfg</i>	Any controller defined by AP local configuration after applying AP local configuration.			
Option	Description											
<i>default</i>	This controller is the one and only controller that the AP could join after applying AP local configuration.											
<i>specify</i>	Specified controller is the one and only controller that the AP could join after applying AP local configuration.											
<i>apcfg</i>	Any controller defined by AP local configuration after applying AP local configuration.											
ac-timer	Maximum waiting time for the AP to join the validation controller after applying AP local configuration .	integer	Minimum value: 3 Maximum value: 30	10								

Parameter	Description	Type	Size	Default
ac-ip	IP address of the validation controller that AP must be able to join after applying AP local configuration.	ipv4-address	Not Specified	0.0.0.0
ac-port	Port of the validation controller that AP must be able to join after applying AP local configuration .	integer	Minimum value: 1024 Maximum value: 49150	0

## config command-list

Parameter	Description	Type	Size	Default						
type	The command type .	option	-	non-password						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>non-password</i></td> <td>Non-password command.</td> </tr> <tr> <td><i>password</i></td> <td>Password command.</td> </tr> </tbody> </table>	Option	Description	<i>non-password</i>	Non-password command.	<i>password</i>	Password command.			
Option	Description									
<i>non-password</i>	Non-password command.									
<i>password</i>	Password command.									
name	AP local configuration command name.	string	Maximum length: 63							
value	AP local configuration command value.	string	Maximum length: 127							
passwd-value	AP local configuration command password value.	password	Not Specified							

## config wireless-controller Bonjour-profile

Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour.

```

config wireless-controller Bonjour-profile
  Description: Configure Bonjour profiles. Bonjour is Apple's zero configuration networking
  protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using
  Bonjour.
  edit <name>
    set comment {string}
    config policy-list
      Description: Bonjour policy list.
      edit <policy-id>
        set description {string}
        set from-vlan {string}
        set to-vlan {string}
        set services {option1}, {option2}, ...
      next
    end
  next

```

end

## config wireless-controller Bonjour-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	

## config policy-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
from-vlan	VLAN ID from which the Bonjour service is advertised .	string	Maximum length: 63	0
to-vlan	VLAN ID to which the Bonjour service is made available .	string	Maximum length: 63	all
services	Bonjour services for the VLAN connecting to the Bonjour network.	option	-	all

Option	Description
<i>all</i>	All services.
<i>airplay</i>	AirPlay.
<i>afp</i>	AFP (Apple File Sharing).
<i>bit-torrent</i>	BitTorrent.
<i>ftp</i>	FTP.
<i>ichat</i>	iChat.
<i>itunes</i>	iTunes.
<i>printers</i>	Printers.
<i>samba</i>	Samba.
<i>scanners</i>	Scanners.
<i>ssh</i>	SSH.
<i>chromecast</i>	ChromeCast.

## config wireless-controller arrp-profile

Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.

```
config wireless-controller arrp-profile
```

Description: Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.

```
edit <name>
  set comment {var-string}
  set selection-period {integer}
  set monitor-period {integer}
  set weight-managed-ap {integer}
  set weight-rogue-ap {integer}
  set weight-noise-floor {integer}
  set weight-channel-load {integer}
  set weight-spectral-rssi {integer}
  set weight-weather-channel {integer}
  set weight-dfs-channel {integer}
  set threshold-ap {integer}
  set threshold-noise-floor {string}
  set threshold-channel-load {integer}
  set threshold-spectral-rssi {string}
  set threshold-tx-retries {integer}
  set threshold-rx-errors {integer}
  set include-weather-channel [enable|disable]
  set include-dfs-channel [enable|disable]
next
end
```

## config wireless-controller arrp-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
selection-period	Period in seconds to measure average channel load, noise floor, spectral RSSI .	integer	Minimum value: 0 Maximum value: 65535	3600
monitor-period	Period in seconds to measure average transmit retries and receive errors .	integer	Minimum value: 0 Maximum value: 65535	300
weight-managed-ap	Weight in DARRP channel score calculation for managed APs .	integer	Minimum value: 0 Maximum value: 2000	50
weight-rogue-ap	Weight in DARRP channel score calculation for rogue APs .	integer	Minimum value: 0 Maximum value: 2000	10



Parameter	Description	Type	Size	Default
weight-noise-floor	Weight in DARRP channel score calculation for noise floor .	integer	Minimum value: 0 Maximum value: 2000	40
weight-channel-load	Weight in DARRP channel score calculation for channel load .	integer	Minimum value: 0 Maximum value: 2000	20
weight-spectral-rssi	Weight in DARRP channel score calculation for spectral RSSI .	integer	Minimum value: 0 Maximum value: 2000	40
weight-weather-channel	Weight in DARRP channel score calculation for weather channel .	integer	Minimum value: 0 Maximum value: 2000	1000
weight-dfs-channel	Weight in DARRP channel score calculation for DFS channel .	integer	Minimum value: 0 Maximum value: 2000	500
threshold-ap	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs .	integer	Minimum value: 0 Maximum value: 500	250
threshold-noise-floor	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor .	string	Maximum length: 7	-85
threshold-channel-load	Threshold in percentage to reject channel in DARRP channel selection phase 1 due to channel load .	integer	Minimum value: 0 Maximum value: 100	60
threshold-spectral-rssi	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to spectral RSSI .	string	Maximum length: 7	-65
threshold-tx-retries	Threshold in percentage for transmit retries to trigger channel reselection in DARRP monitor stage .	integer	Minimum value: 0 Maximum value: 1000	300
threshold-rx-errors	Threshold in percentage for receive errors to trigger channel reselection in DARRP monitor stage .	integer	Minimum value: 0 Maximum value: 100	50

Parameter	Description	Type	Size	Default						
include-weather-channel	Enable/disable use of weather channel in DARRP channel selection phase 1 .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Include weather channel in darrp channel selection phase 1.</td> </tr> <tr> <td><i>disable</i></td> <td>Exclude weather channel in darrp channel selection phase 1.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Include weather channel in darrp channel selection phase 1.	<i>disable</i>	Exclude weather channel in darrp channel selection phase 1.			
Option	Description									
<i>enable</i>	Include weather channel in darrp channel selection phase 1.									
<i>disable</i>	Exclude weather channel in darrp channel selection phase 1.									
include-dfs-channel	Enable/disable use of DFS channel in DARRP channel selection phase 1 .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Include DFS channel in darrp channel selection phase 1.</td> </tr> <tr> <td><i>disable</i></td> <td>Exclude DFS channel in darrp channel selection phase 1.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Include DFS channel in darrp channel selection phase 1.	<i>disable</i>	Exclude DFS channel in darrp channel selection phase 1.			
Option	Description									
<i>enable</i>	Include DFS channel in darrp channel selection phase 1.									
<i>disable</i>	Exclude DFS channel in darrp channel selection phase 1.									

## config wireless-controller region

Configure FortiAP regions (for floor plans and maps).

```
config wireless-controller region
  Description: Configure FortiAP regions (for floor plans and maps).
  edit <name>
    set comments {string}
    set grayscale [enable|disable]
    set opacity {integer}
  next
end
```

## config wireless-controller region

Parameter	Description	Type	Size	Default						
comments	Comments.	string	Maximum length: 1027							
grayscale	Region image grayscale.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable region image grayscale.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable region image grayscale.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable region image grayscale.	<i>disable</i>	Disable region image grayscale.			
Option	Description									
<i>enable</i>	Enable region image grayscale.									
<i>disable</i>	Disable region image grayscale.									
opacity	Region image opacity .	integer	Minimum value: 0 Maximum value: 100	100						

## config wireless-controller vap-group

Configure virtual Access Point (VAP) groups.

```
config wireless-controller vap-group
  Description: Configure virtual Access Point (VAP) groups.
  edit <name>
    set comment {var-string}
    set vaps <name1>, <name2>, ...
  next
end
```

## config wireless-controller vap-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
vaps <name>	List of SSIDs to be included in the VAP group. vap name	string	Maximum length: 35	

## config wireless-controller wids-profile

Configure wireless intrusion detection system (WIDS) profiles.

```
config wireless-controller wids-profile
  Description: Configure wireless intrusion detection system (WIDS) profiles.
  edit <name>
    set comment {string}
    set sensor-mode [disable|foreign|...]
    set ap-scan [disable|enable]
    set ap-bgscan-period {integer}
    set ap-bgscan-intv {integer}
    set ap-bgscan-duration {integer}
    set ap-bgscan-idle {integer}
    set ap-bgscan-report-intv {integer}
    set ap-bgscan-disable-schedules <name1>, <name2>, ...
    set ap-fgscan-report-intv {integer}
    set ap-scan-passive [enable|disable]
    set ap-scan-threshold {string}
    set ap-auto-suppress [enable|disable]
    set wireless-bridge [enable|disable]
    set deauth-broadcast [enable|disable]
    set null-ssid-probe-resp [enable|disable]
    set long-duration-attack [enable|disable]
    set long-duration-thresh {integer}
    set invalid-mac-oui [enable|disable]
    set weak-wep-iv [enable|disable]
    set auth-frame-flood [enable|disable]
    set auth-flood-time {integer}
    set auth-flood-thresh {integer}
    set assoc-frame-flood [enable|disable]
    set assoc-flood-time {integer}
```

```

set assoc-flood-thresh {integer}
set spoofed-death [enable|disable]
set asleap-attack [enable|disable]
set eapol-start-flood [enable|disable]
set eapol-start-thresh {integer}
set eapol-start-intv {integer}
set eapol-logoff-flood [enable|disable]
set eapol-logoff-thresh {integer}
set eapol-logoff-intv {integer}
set eapol-succ-flood [enable|disable]
set eapol-succ-thresh {integer}
set eapol-succ-intv {integer}
set eapol-fail-flood [enable|disable]
set eapol-fail-thresh {integer}
set eapol-fail-intv {integer}
set eapol-pre-succ-flood [enable|disable]
set eapol-pre-succ-thresh {integer}
set eapol-pre-succ-intv {integer}
set eapol-pre-fail-flood [enable|disable]
set eapol-pre-fail-thresh {integer}
set eapol-pre-fail-intv {integer}
set death-unknown-src-thresh {integer}
next
end

```

## config wireless-controller wids-profile

Parameter	Description	Type	Size	Default								
comment	Comment.	string	Maximum length: 63									
sensor-mode	Scan nearby WiFi stations .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable the scan.</td> </tr> <tr> <td><i>foreign</i></td> <td>Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.</td> </tr> <tr> <td><i>both</i></td> <td>Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable the scan.	<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.	<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.			
Option	Description											
<i>disable</i>	Disable the scan.											
<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.											
<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.											
ap-scan	Enable/disable rogue AP detection.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable rogue AP detection.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable rogue AP detection.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable rogue AP detection.	<i>enable</i>	Enable rogue AP detection.					
Option	Description											
<i>disable</i>	Disable rogue AP detection.											
<i>enable</i>	Enable rogue AP detection.											



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable on-wire rogue AP auto-suppression.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable on-wire rogue AP auto-suppression.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable on-wire rogue AP auto-suppression.	<i>disable</i>	Disable on-wire rogue AP auto-suppression.			
Option	Description									
<i>enable</i>	Enable on-wire rogue AP auto-suppression.									
<i>disable</i>	Disable on-wire rogue AP auto-suppression.									
wireless-bridge	Enable/disable wireless bridge detection .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable wireless bridge detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable wireless bridge detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable wireless bridge detection.	<i>disable</i>	Disable wireless bridge detection.			
Option	Description									
<i>enable</i>	Enable wireless bridge detection.									
<i>disable</i>	Disable wireless bridge detection.									
deauth-broadcast	Enable/disable broadcasting de-authentication detection .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable broadcast de-authentication detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable broadcast de-authentication detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable broadcast de-authentication detection.	<i>disable</i>	Disable broadcast de-authentication detection.			
Option	Description									
<i>enable</i>	Enable broadcast de-authentication detection.									
<i>disable</i>	Disable broadcast de-authentication detection.									
null-ssid-probe-resp	Enable/disable null SSID probe response detection .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable null SSID probe resp detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable null SSID probe resp detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable null SSID probe resp detection.	<i>disable</i>	Disable null SSID probe resp detection.			
Option	Description									
<i>enable</i>	Enable null SSID probe resp detection.									
<i>disable</i>	Disable null SSID probe resp detection.									
long-duration-attack	Enable/disable long duration attack detection based on user configured threshold .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable long duration attack detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable long duration attack detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable long duration attack detection.	<i>disable</i>	Disable long duration attack detection.			
Option	Description									
<i>enable</i>	Enable long duration attack detection.									
<i>disable</i>	Disable long duration attack detection.									
long-duration-thresh	Threshold value for long duration attack detection .	integer	Minimum value: 1000 Maximum value: 32767	8200						
invalid-mac-oui	Enable/disable invalid MAC OUI detection.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable invalid MAC OUI detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable invalid MAC OUI detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable invalid MAC OUI detection.	<i>disable</i>	Disable invalid MAC OUI detection.			
Option	Description									
<i>enable</i>	Enable invalid MAC OUI detection.									
<i>disable</i>	Disable invalid MAC OUI detection.									
weak-wep-iv	Enable/disable weak WEP IV .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable weak WEP IV detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable weak WEP IV detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable weak WEP IV detection.	<i>disable</i>	Disable weak WEP IV detection.			
Option	Description									
<i>enable</i>	Enable weak WEP IV detection.									
<i>disable</i>	Disable weak WEP IV detection.									
auth-frame-flood	Enable/disable authentication frame flooding detection .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable authentication frame flooding detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable authentication frame flooding detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable authentication frame flooding detection.	<i>disable</i>	Disable authentication frame flooding detection.			
Option	Description									
<i>enable</i>	Enable authentication frame flooding detection.									
<i>disable</i>	Disable authentication frame flooding detection.									
auth-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10						
auth-flood-thresh	The threshold value for authentication frame flooding.	integer	Minimum value: 1 Maximum value: 100	30						
assoc-frame-flood	Enable/disable association frame flooding detection .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable association frame flooding detection.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable association frame flooding detection.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable association frame flooding detection.	<i>disable</i>	Disable association frame flooding detection.			
Option	Description									
<i>enable</i>	Enable association frame flooding detection.									
<i>disable</i>	Disable association frame flooding detection.									
assoc-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10						
assoc-flood-thresh	The threshold value for association frame flooding.	integer	Minimum value: 1 Maximum value: 100	30						

Parameter	Description	Type	Size	Default
spoofed-deauth	Enable/disable spoofed de-authentication attack detection .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable spoofed de-authentication attack detection.		
	<i>disable</i>	Disable spoofed de-authentication attack detection.		
asleep-attack	Enable/disable asleep attack detection .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable asleep attack detection.		
	<i>disable</i>	Disable asleep attack detection.		
eapol-start-flood	Enable/disable EAPOL-Start flooding .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable EAPOL-Start flooding detection.		
	<i>disable</i>	Disable EAPOL-Start flooding detection.		
eapol-start-thresh	The threshold value for EAPOL-Start flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-start-intv	The detection interval for EAPOL-Start flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-logoff-flood	Enable/disable EAPOL-Logoff flooding .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable EAPOL-Logoff flooding detection.		
	<i>disable</i>	Disable EAPOL-Logoff flooding detection.		
eapol-logoff-thresh	The threshold value for EAPOL-Logoff flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10



Parameter	Description	Type	Size	Default
eapol-logoff-intv	The detection interval for EAPOL-Logoff flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-succ-flood	Enable/disable EAPOL-Success flooding .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable EAPOL-Success flooding detection.		
	<i>disable</i>	Disable EAPOL-Success flooding detection.		
eapol-succ-thresh	The threshold value for EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-succ-intv	The detection interval for EAPOL-Success flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-fail-flood	Enable/disable EAPOL-Failure flooding .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable EAPOL-Failure flooding detection.		
	<i>disable</i>	Disable EAPOL-Failure flooding detection.		
eapol-fail-thresh	The threshold value for EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-fail-intv	The detection interval for EAPOL-Failure flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-pre-succ-flood	Enable/disable premature EAPOL-Success flooding .	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable premature EAPOL-Success flooding detection.		
	<i>disable</i>	Disable premature EAPOL-Success flooding detection.		



```

    set ble-scanning [enable|disable]
  next
end

```

## config wireless-controller ble-profile

Parameter	Description	Type	Size	Default								
comment	Comment.	string	Maximum length: 63									
advertising	Advertising type.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ibeacon</i></td> <td>iBeacon advertising.</td> </tr> <tr> <td><i>eddystone-uid</i></td> <td>Eddystone UID advertising.</td> </tr> <tr> <td><i>eddystone-url</i></td> <td>Eddystone URL advertising.</td> </tr> </tbody> </table>	Option	Description	<i>ibeacon</i>	iBeacon advertising.	<i>eddystone-uid</i>	Eddystone UID advertising.	<i>eddystone-url</i>	Eddystone URL advertising.			
Option	Description											
<i>ibeacon</i>	iBeacon advertising.											
<i>eddystone-uid</i>	Eddystone UID advertising.											
<i>eddystone-url</i>	Eddystone URL advertising.											
ibeacon-uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 63	005ea414-cbd1-11e5-9956-625662870761								
major-id	Major ID.	integer	Minimum value: 0 Maximum value: 65535	1000								
minor-id	Minor ID.	integer	Minimum value: 0 Maximum value: 65535	2000								
eddystone-namespace	Eddystone namespace ID.	string	Maximum length: 10	0102030405								
eddystone-instance	Eddystone instance ID.	string	Maximum length: 6	abcdef								
eddystone-url	Eddystone URL.	string	Maximum length: 127	http://www.fortinet.com								
txpower	Transmit power level .	option	-	0								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>0</i></td> <td>Transmit power level 0 (-21 dBm)</td> </tr> <tr> <td><i>1</i></td> <td>Transmit power level 1 (-18 dBm)</td> </tr> </tbody> </table>	Option	Description	<i>0</i>	Transmit power level 0 (-21 dBm)	<i>1</i>	Transmit power level 1 (-18 dBm)					
Option	Description											
<i>0</i>	Transmit power level 0 (-21 dBm)											
<i>1</i>	Transmit power level 1 (-18 dBm)											

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>Transmit power level 2 (-15 dBm)</td> </tr> <tr> <td>3</td> <td>Transmit power level 3 (-12 dBm)</td> </tr> <tr> <td>4</td> <td>Transmit power level 4 (-9 dBm)</td> </tr> <tr> <td>5</td> <td>Transmit power level 5 (-6 dBm)</td> </tr> <tr> <td>6</td> <td>Transmit power level 6 (-3 dBm)</td> </tr> <tr> <td>7</td> <td>Transmit power level 7 (0 dBm)</td> </tr> <tr> <td>8</td> <td>Transmit power level 8 (1 dBm)</td> </tr> <tr> <td>9</td> <td>Transmit power level 9 (2 dBm)</td> </tr> <tr> <td>10</td> <td>Transmit power level 10 (3 dBm)</td> </tr> <tr> <td>11</td> <td>Transmit power level 11 (4 dBm)</td> </tr> <tr> <td>12</td> <td>Transmit power level 12 (5 dBm)</td> </tr> </tbody> </table>	Option	Description	2	Transmit power level 2 (-15 dBm)	3	Transmit power level 3 (-12 dBm)	4	Transmit power level 4 (-9 dBm)	5	Transmit power level 5 (-6 dBm)	6	Transmit power level 6 (-3 dBm)	7	Transmit power level 7 (0 dBm)	8	Transmit power level 8 (1 dBm)	9	Transmit power level 9 (2 dBm)	10	Transmit power level 10 (3 dBm)	11	Transmit power level 11 (4 dBm)	12	Transmit power level 12 (5 dBm)			
Option	Description																											
2	Transmit power level 2 (-15 dBm)																											
3	Transmit power level 3 (-12 dBm)																											
4	Transmit power level 4 (-9 dBm)																											
5	Transmit power level 5 (-6 dBm)																											
6	Transmit power level 6 (-3 dBm)																											
7	Transmit power level 7 (0 dBm)																											
8	Transmit power level 8 (1 dBm)																											
9	Transmit power level 9 (2 dBm)																											
10	Transmit power level 10 (3 dBm)																											
11	Transmit power level 11 (4 dBm)																											
12	Transmit power level 12 (5 dBm)																											
beacon-interval	Beacon interval .	integer	Minimum value: 40 Maximum value: 3500	100																								
ble-scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.	option	-	disable																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable BLE scanning.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable BLE scanning.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable BLE scanning.	<i>disable</i>	Disable BLE scanning.																					
Option	Description																											
<i>enable</i>	Enable BLE scanning.																											
<i>disable</i>	Disable BLE scanning.																											

## config wireless-controller wtp-profile

Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```

config wireless-controller wtp-profile
  Description: Configure WTP profiles or FortiAP profiles that define radio settings for
    manageable FortiAP platforms.
  edit <name>
    set comment {var-string}
    config platform
      Description: WTP, FortiAP, or AP platform.
      set type [AP-11N|220B|...]
      set mode [single-5G|dual-5G]
      set ddscan [enable|disable]
    end
    set control-message-offload {option1}, {option2}, ...
    set apcfg-profile {string}
    set ble-profile {string}
  
```

```

set wan-port-mode [wan-lan|wan-only]
config lan
  Description: WTP LAN port mapping.
  set port-mode [offline|nat-to-wan|...]
  set port-ssid {string}
  set port1-mode [offline|nat-to-wan|...]
  set port1-ssid {string}
  set port2-mode [offline|nat-to-wan|...]
  set port2-ssid {string}
  set port3-mode [offline|nat-to-wan|...]
  set port3-ssid {string}
  set port4-mode [offline|nat-to-wan|...]
  set port4-ssid {string}
  set port5-mode [offline|nat-to-wan|...]
  set port5-ssid {string}
  set port6-mode [offline|nat-to-wan|...]
  set port6-ssid {string}
  set port7-mode [offline|nat-to-wan|...]
  set port7-ssid {string}
  set port8-mode [offline|nat-to-wan|...]
  set port8-ssid {string}
  set port-esl-mode [offline|nat-to-wan|...]
  set port-esl-ssid {string}
end
set energy-efficient-ethernet [enable|disable]
set led-state [enable|disable]
set led-schedules <name1>, <name2>, ...
set dtls-policy {option1}, {option2}, ...
set dtls-in-kernel [enable|disable]
set max-clients {integer}
set handoff-rssi {integer}
set handoff-sta-thresh {integer}
set handoff-roaming [enable|disable]
config deny-mac-list
  Description: List of MAC addresses that are denied access to this WTP, FortiAP, or
  AP.
  edit <id>
    set mac {mac-address}
  next
end
set ap-country [NA|AF|...]
set ip-fragment-preventing {option1}, {option2}, ...
set tun-mtu-uplink {integer}
set tun-mtu-downlink {integer}
set split-tunneling-acl-path [tunnel|local]
set split-tunneling-acl-local-ap-subnet [enable|disable]
config split-tunneling-acl
  Description: Split tunneling ACL filter list.
  edit <id>
    set dest-ip {ipv4-classnet}
  next
end
set allowaccess {option1}, {option2}, ...
set login-passwd-change [yes|default|...]
set login-passwd {password}
set lldp [enable|disable]
set poe-mode [auto|8023af|...]

```

```

set frequency-handoff [enable|disable]
set ap-handoff [enable|disable]
config radio-1
  Description: Configuration options for radio 1.
  set mode [disabled|ap|...]
  set band [802.11a|802.11b|...]
  set band-5g-type [5g-full|5g-high|...]
  set drma [disable|enable]
  set drma-sensitivity [low|medium|...]
  set airtime-fairness [enable|disable]
  set protection-mode [rtscts|ctsonly|...]
  set powersave-optimize {option1}, {option2}, ...
  set transmit-optimize {option1}, {option2}, ...
  set amsdu [enable|disable]
  set coexistence [enable|disable]
  set zero-wait-dfs [enable|disable]
  set bss-color {integer}
  set short-guard-interval [enable|disable]
  set channel-bonding [160MHz|80MHz|...]
  set auto-power-level [enable|disable]
  set auto-power-high {integer}
  set auto-power-low {integer}
  set auto-power-target {string}
  set power-level {integer}
  set dtim {integer}
  set beacon-interval {integer}
  set rts-threshold {integer}
  set frag-threshold {integer}
  set ap-sniffer-bufsize {integer}
  set ap-sniffer-chan {integer}
  set ap-sniffer-addr {mac-address}
  set ap-sniffer-mgmt-beacon [enable|disable]
  set ap-sniffer-mgmt-probe [enable|disable]
  set ap-sniffer-mgmt-other [enable|disable]
  set ap-sniffer-ctl [enable|disable]
  set ap-sniffer-data [enable|disable]
  set channel-utilization [enable|disable]
  set wids-profile {string}
  set darrp [enable|disable]
  set max-clients {integer}
  set max-distance {integer}
  set vap-all [tunnel|bridge|...]
  set vaps <name1>, <name2>, ...
  set channel <chan1>, <chan2>, ...
  set call-admission-control [enable|disable]
  set call-capacity {integer}
  set bandwidth-admission-control [enable|disable]
  set bandwidth-capacity {integer}
end
config radio-2
  Description: Configuration options for radio 2.
  set mode [disabled|ap|...]
  set band [802.11a|802.11b|...]
  set band-5g-type [5g-full|5g-high|...]
  set drma [disable|enable]
  set drma-sensitivity [low|medium|...]
  set airtime-fairness [enable|disable]

```

```

set protection-mode [rtscts|ctsonly|...]
set powersave-optimize {option1}, {option2}, ...
set transmit-optimize {option1}, {option2}, ...
set amsdu [enable|disable]
set coexistence [enable|disable]
set zero-wait-dfs [enable|disable]
set bss-color {integer}
set short-guard-interval [enable|disable]
set channel-bonding [160MHz|80MHz|...]
set auto-power-level [enable|disable]
set auto-power-high {integer}
set auto-power-low {integer}
set auto-power-target {string}
set power-level {integer}
set dtim {integer}
set beacon-interval {integer}
set rts-threshold {integer}
set frag-threshold {integer}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}

```

end

config radio-3

```

Description: Configuration options for radio 3.
set mode [disabled|ap|...]
set band [802.11a|802.11b|...]
set band-5g-type [5g-full|5g-high|...]
set drma [disable|enable]
set drma-sensitivity [low|medium|...]
set airtime-fairness [enable|disable]
set protection-mode [rtscts|ctsonly|...]
set powersave-optimize {option1}, {option2}, ...
set transmit-optimize {option1}, {option2}, ...
set amsdu [enable|disable]
set coexistence [enable|disable]
set zero-wait-dfs [enable|disable]
set bss-color {integer}
set short-guard-interval [enable|disable]
set channel-bonding [160MHz|80MHz|...]
set auto-power-level [enable|disable]

```

```

set auto-power-high {integer}
set auto-power-low {integer}
set auto-power-target {string}
set power-level {integer}
set dtim {integer}
set beacon-interval {integer}
set rts-threshold {integer}
set frag-threshold {integer}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-4
Description: Configuration options for radio 4.
set mode [disabled|ap|...]
set band [802.11a|802.11b|...]
set band-5g-type [5g-full|5g-high|...]
set drma [disable|enable]
set drma-sensitivity [low|medium|...]
set airtime-fairness [enable|disable]
set protection-mode [rtscts|ctsonly|...]
set powersave-optimize {option1}, {option2}, ...
set transmit-optimize {option1}, {option2}, ...
set amsdu [enable|disable]
set coexistence [enable|disable]
set zero-wait-dfs [enable|disable]
set bss-color {integer}
set short-guard-interval [enable|disable]
set channel-bonding [160MHz|80MHz|...]
set auto-power-level [enable|disable]
set auto-power-high {integer}
set auto-power-low {integer}
set auto-power-target {string}
set power-level {integer}
set dtim {integer}
set beacon-interval {integer}
set rts-threshold {integer}
set frag-threshold {integer}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}

```



```

set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config lbs
  Description: Set various location based service (LBS) options.
  set ekahau-blink-mode [enable|disable]
  set ekahau-tag {mac-address}
  set erc-server-ip {ipv4-address-any}
  set erc-server-port {integer}
  set aeroscout [enable|disable]
  set aeroscout-server-ip {ipv4-address-any}
  set aeroscout-server-port {integer}
  set aeroscout-mu [enable|disable]
  set aeroscout-ap-mac [bssid|board-mac]
  set aeroscout-mmu-report [enable|disable]
  set aeroscout-mu-factor {integer}
  set aeroscout-mu-timeout {integer}
  set fortipresence [foreign|both|...]
  set fortipresence-server {ipv4-address-any}
  set fortipresence-port {integer}
  set fortipresence-secret {password}
  set fortipresence-project {string}
  set fortipresence-frequency {integer}
  set fortipresence-rogue [enable|disable]
  set fortipresence-unassoc [enable|disable]
  set fortipresence-ble [enable|disable]
  set station-locate [enable|disable]
end
  set ext-info-enable [enable|disable]
next
end

```

## config wireless-controller wtp-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default																				
control-message-offload	Enable/disable CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ebp-frame</i></td> <td>Ekahau blink protocol (EBP) frames.</td> </tr> <tr> <td><i>aeroscout-tag</i></td> <td>AeroScout tag.</td> </tr> <tr> <td><i>ap-list</i></td> <td>Rogue AP list.</td> </tr> <tr> <td><i>sta-list</i></td> <td>Rogue STA list.</td> </tr> <tr> <td><i>sta-cap-list</i></td> <td>STA capability list.</td> </tr> <tr> <td><i>stats</i></td> <td>WTP, radio, VAP, and STA statistics.</td> </tr> <tr> <td><i>aeroscout-mu</i></td> <td>AeroScout Mobile Unit (MU) report.</td> </tr> <tr> <td><i>sta-health</i></td> <td>STA health log.</td> </tr> <tr> <td><i>spectral-analysis</i></td> <td>Spectral analysis report.</td> </tr> </tbody> </table>	Option	Description	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.	<i>aeroscout-tag</i>	AeroScout tag.	<i>ap-list</i>	Rogue AP list.	<i>sta-list</i>	Rogue STA list.	<i>sta-cap-list</i>	STA capability list.	<i>stats</i>	WTP, radio, VAP, and STA statistics.	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	<i>sta-health</i>	STA health log.	<i>spectral-analysis</i>	Spectral analysis report.			
Option	Description																							
<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.																							
<i>aeroscout-tag</i>	AeroScout tag.																							
<i>ap-list</i>	Rogue AP list.																							
<i>sta-list</i>	Rogue STA list.																							
<i>sta-cap-list</i>	STA capability list.																							
<i>stats</i>	WTP, radio, VAP, and STA statistics.																							
<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.																							
<i>sta-health</i>	STA health log.																							
<i>spectral-analysis</i>	Spectral analysis report.																							
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35																					
ble-profile	Bluetooth Low Energy profile name.	string	Maximum length: 35																					
wan-port-mode	Enable/disable using a WAN port as a LAN port.	option	-	wan-only																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wan-lan</i></td> <td>Enable using a WAN port as a LAN port.</td> </tr> <tr> <td><i>wan-only</i></td> <td>Disable using a WAN port as a LAN port.</td> </tr> </tbody> </table>	Option	Description	<i>wan-lan</i>	Enable using a WAN port as a LAN port.	<i>wan-only</i>	Disable using a WAN port as a LAN port.																	
Option	Description																							
<i>wan-lan</i>	Enable using a WAN port as a LAN port.																							
<i>wan-only</i>	Disable using a WAN port as a LAN port.																							
energy-efficient-ethernet	Enable/disable use of energy efficient Ethernet on WTP.	option	-	disable																				

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of energy efficient Ethernet on WTP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of energy efficient Ethernet on WTP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of energy efficient Ethernet on WTP.	<i>disable</i>	Disable use of energy efficient Ethernet on WTP.					
Option	Description											
<i>enable</i>	Enable use of energy efficient Ethernet on WTP.											
<i>disable</i>	Disable use of energy efficient Ethernet on WTP.											
led-state	Enable/disable use of LEDs on WTP .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable use of LEDs on WTP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable use of LEDs on WTP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of LEDs on WTP.	<i>disable</i>	Disable use of LEDs on WTP.					
Option	Description											
<i>enable</i>	Enable use of LEDs on WTP.											
<i>disable</i>	Disable use of LEDs on WTP.											
led-schedules <name>	Recurring firewall schedules for illuminating LEDs on the FortiAP. If led-state is enabled, LEDs will be visible when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35									
dtls-policy	WTP data channel DTLS policy .	option	-	clear-text								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>clear-text</i></td> <td>Clear Text Data Channel.</td> </tr> <tr> <td><i>dtls-enabled</i></td> <td>DTLS Enabled Data Channel.</td> </tr> <tr> <td><i>ipsec-vpn</i></td> <td>IPsec VPN Data Channel.</td> </tr> </tbody> </table>	Option	Description	<i>clear-text</i>	Clear Text Data Channel.	<i>dtls-enabled</i>	DTLS Enabled Data Channel.	<i>ipsec-vpn</i>	IPsec VPN Data Channel.			
Option	Description											
<i>clear-text</i>	Clear Text Data Channel.											
<i>dtls-enabled</i>	DTLS Enabled Data Channel.											
<i>ipsec-vpn</i>	IPsec VPN Data Channel.											
dtls-in-kernel	Enable/disable data channel DTLS in kernel.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable data channel DTLS in kernel.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable data channel DTLS in kernel.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable data channel DTLS in kernel.	<i>disable</i>	Disable data channel DTLS in kernel.					
Option	Description											
<i>enable</i>	Enable data channel DTLS in kernel.											
<i>disable</i>	Disable data channel DTLS in kernel.											
max-clients	Maximum number of stations .	integer	Minimum value: 0 Maximum value: 4294967295	0								
handoff-rssi	Minimum received signal strength indicator .	integer	Minimum value: 20 Maximum value: 30	25								

Parameter	Description	Type	Size	Default																																						
handoff-sta-thresh	Threshold value for AP handoff.	integer	Minimum value: 0 Maximum value: 4294967295	0																																						
handoff-roaming	Enable/disable client load balancing during roaming to avoid roaming delay .	option	-	enable																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable handoff roaming.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable handoff roaming.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable handoff roaming.	<i>disable</i>	Disable handoff roaming.																																			
Option	Description																																									
<i>enable</i>	Enable handoff roaming.																																									
<i>disable</i>	Disable handoff roaming.																																									
ap-country	Country in which this WTP, FortiAP or AP will operate .	option	-	NA																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>NA</i></td> <td>NO_COUNTRY_SET</td> </tr> <tr> <td><i>AF</i></td> <td>AFGHANISTAN</td> </tr> <tr> <td><i>AL</i></td> <td>ALBANIA</td> </tr> <tr> <td><i>DZ</i></td> <td>ALGERIA</td> </tr> <tr> <td><i>AS</i></td> <td>AMERICAN SAMOA</td> </tr> <tr> <td><i>AO</i></td> <td>ANGOLA</td> </tr> <tr> <td><i>AR</i></td> <td>ARGENTINA</td> </tr> <tr> <td><i>AM</i></td> <td>ARMENIA</td> </tr> <tr> <td><i>AU</i></td> <td>AUSTRALIA</td> </tr> <tr> <td><i>AT</i></td> <td>AUSTRIA</td> </tr> <tr> <td><i>AZ</i></td> <td>AZERBAIJAN</td> </tr> <tr> <td><i>BS</i></td> <td>BAHAMAS</td> </tr> <tr> <td><i>BH</i></td> <td>BAHRAIN</td> </tr> <tr> <td><i>BD</i></td> <td>BANGLADESH</td> </tr> <tr> <td><i>BB</i></td> <td>BARBADOS</td> </tr> <tr> <td><i>BY</i></td> <td>BELARUS</td> </tr> <tr> <td><i>BE</i></td> <td>BELGIUM</td> </tr> <tr> <td><i>BZ</i></td> <td>BELIZE</td> </tr> </tbody> </table>	Option	Description	<i>NA</i>	NO_COUNTRY_SET	<i>AF</i>	AFGHANISTAN	<i>AL</i>	ALBANIA	<i>DZ</i>	ALGERIA	<i>AS</i>	AMERICAN SAMOA	<i>AO</i>	ANGOLA	<i>AR</i>	ARGENTINA	<i>AM</i>	ARMENIA	<i>AU</i>	AUSTRALIA	<i>AT</i>	AUSTRIA	<i>AZ</i>	AZERBAIJAN	<i>BS</i>	BAHAMAS	<i>BH</i>	BAHRAIN	<i>BD</i>	BANGLADESH	<i>BB</i>	BARBADOS	<i>BY</i>	BELARUS	<i>BE</i>	BELGIUM	<i>BZ</i>	BELIZE			
Option	Description																																									
<i>NA</i>	NO_COUNTRY_SET																																									
<i>AF</i>	AFGHANISTAN																																									
<i>AL</i>	ALBANIA																																									
<i>DZ</i>	ALGERIA																																									
<i>AS</i>	AMERICAN SAMOA																																									
<i>AO</i>	ANGOLA																																									
<i>AR</i>	ARGENTINA																																									
<i>AM</i>	ARMENIA																																									
<i>AU</i>	AUSTRALIA																																									
<i>AT</i>	AUSTRIA																																									
<i>AZ</i>	AZERBAIJAN																																									
<i>BS</i>	BAHAMAS																																									
<i>BH</i>	BAHRAIN																																									
<i>BD</i>	BANGLADESH																																									
<i>BB</i>	BARBADOS																																									
<i>BY</i>	BELARUS																																									
<i>BE</i>	BELGIUM																																									
<i>BZ</i>	BELIZE																																									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>BJ</i>	BENIN		
	<i>BM</i>	BERMUDA		
	<i>BT</i>	BHUTAN		
	<i>BO</i>	BOLIVIA		
	<i>BA</i>	BOSNIA AND HERZEGOVINA		
	<i>BW</i>	BOTSWANA		
	<i>BR</i>	BRAZIL		
	<i>BN</i>	BRUNEI DARUSSALAM		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GE</i>	GEORGIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		
	<i>CI</i>	COTE_D_IVOIRE		
	<i>JM</i>	JAMAICA		
	<i>JO</i>	JORDAN		
	<i>KZ</i>	KAZAKHSTAN		
	<i>KE</i>	KENYA		
	<i>KR</i>	KOREA REPUBLIC		
	<i>KW</i>	KUWAIT		
	<i>LA</i>	LAOS		
	<i>LV</i>	LATVIA		
	<i>LB</i>	LEBANON		
	<i>LS</i>	LESOTHO		
	<i>LY</i>	LIBYA		
	<i>LI</i>	LIECHTENSTEIN		
	<i>LT</i>	LITHUANIA		
	<i>LU</i>	LUXEMBOURG		
	<i>MO</i>	MACAU SAR		
	<i>MK</i>	MACEDONIA, FYRO		
	<i>MG</i>	MADAGASCAR		
	<i>MW</i>	MALAWI		
	<i>MY</i>	MALAYSIA		
	<i>MV</i>	MALDIVES		
	<i>ML</i>	MALI		
	<i>MT</i>	MALTA		
	<i>MH</i>	MARSHALL ISLANDS		
	<i>MQ</i>	MARTINIQUE		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>MR</i>	MAURITANIA		
	<i>MU</i>	MAURITIUS		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		
	<i>MC</i>	MONACO		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NO</i>	NORWAY		
	<i>MP</i>	NORTHERN MARIANA ISLANDS		
	<i>OM</i>	OMAN		
	<i>PK</i>	PAKISTAN		
	<i>PW</i>	PALAU		
	<i>PA</i>	PANAMA		
	<i>PG</i>	PAPUA NEW GUINEA		
	<i>PY</i>	PARAGUAY		
	<i>PE</i>	PERU		
	<i>PH</i>	PHILIPPINES		
	<i>PL</i>	POLAND		
	<i>PT</i>	PORTUGAL		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>PR</i>	PUERTO RICO		
	<i>QA</i>	QATAR		
	<i>RE</i>	REUNION		
	<i>RO</i>	ROMANIA		
	<i>RU</i>	RUSSIA		
	<i>RW</i>	RWANDA		
	<i>BL</i>	SAINT BARTHELEMY		
	<i>KN</i>	SAINT KITTS AND NEVIS		
	<i>LC</i>	SAINT LUCIA		
	<i>MF</i>	SAINT MARTIN		
	<i>PM</i>	SAINT PIERRE AND MIQUELON		
	<i>VC</i>	SAINT VINCENT AND GRENADIENS		
	<i>SA</i>	SAUDI ARABIA		
	<i>SN</i>	SENEGAL		
	<i>RS</i>	REPUBLIC OF SERBIA		
	<i>ME</i>	MONTENEGRO		
	<i>SL</i>	SIERRA LEONE		
	<i>SG</i>	SINGAPORE		
	<i>SK</i>	SLOVAKIA		
	<i>SI</i>	SLOVENIA		
	<i>ZA</i>	SOUTH AFRICA		
	<i>ES</i>	SPAIN		
	<i>LK</i>	SRI LANKA		
	<i>SE</i>	SWEDEN		
	<i>SR</i>	SURINAME		
	<i>CH</i>	SWITZERLAND		
	<i>TW</i>	TAIWAN		
	<i>TZ</i>	TANZANIA		
	<i>TH</i>	THAILAND		

Parameter	Description	Type	Size	Default																																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr><td><i>TG</i></td><td>TOGO</td></tr> <tr><td><i>TT</i></td><td>TRINIDAD AND TOBAGO</td></tr> <tr><td><i>TN</i></td><td>TUNISIA</td></tr> <tr><td><i>TR</i></td><td>TURKEY</td></tr> <tr><td><i>TM</i></td><td>TURKMENISTAN</td></tr> <tr><td><i>AE</i></td><td>UNITED ARAB EMIRATES</td></tr> <tr><td><i>TC</i></td><td>TURKS AND CAICOS</td></tr> <tr><td><i>UG</i></td><td>UGANDA</td></tr> <tr><td><i>UA</i></td><td>UKRAINE</td></tr> <tr><td><i>GB</i></td><td>UNITED KINGDOM</td></tr> <tr><td><i>US</i></td><td>UNITED STATES2</td></tr> <tr><td><i>PS</i></td><td>UNITED STATES (PUBLIC SAFETY)</td></tr> <tr><td><i>UY</i></td><td>URUGUAY</td></tr> <tr><td><i>UZ</i></td><td>UZBEKISTAN</td></tr> <tr><td><i>VU</i></td><td>VANUATU</td></tr> <tr><td><i>VE</i></td><td>VENEZUELA</td></tr> <tr><td><i>VN</i></td><td>VIET NAM</td></tr> <tr><td><i>VI</i></td><td>VIRGIN ISLANDS</td></tr> <tr><td><i>WF</i></td><td>WALLIS AND FUTUNA</td></tr> <tr><td><i>YE</i></td><td>YEMEN</td></tr> <tr><td><i>ZM</i></td><td>ZAMBIA</td></tr> <tr><td><i>ZW</i></td><td>ZIMBABWE</td></tr> <tr><td><i>JP</i></td><td>JAPAN14</td></tr> <tr><td><i>CA</i></td><td>CANADA2</td></tr> </tbody> </table>	Option	Description	<i>TG</i>	TOGO	<i>TT</i>	TRINIDAD AND TOBAGO	<i>TN</i>	TUNISIA	<i>TR</i>	TURKEY	<i>TM</i>	TURKMENISTAN	<i>AE</i>	UNITED ARAB EMIRATES	<i>TC</i>	TURKS AND CAICOS	<i>UG</i>	UGANDA	<i>UA</i>	UKRAINE	<i>GB</i>	UNITED KINGDOM	<i>US</i>	UNITED STATES2	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)	<i>UY</i>	URUGUAY	<i>UZ</i>	UZBEKISTAN	<i>VU</i>	VANUATU	<i>VE</i>	VENEZUELA	<i>VN</i>	VIET NAM	<i>VI</i>	VIRGIN ISLANDS	<i>WF</i>	WALLIS AND FUTUNA	<i>YE</i>	YEMEN	<i>ZM</i>	ZAMBIA	<i>ZW</i>	ZIMBABWE	<i>JP</i>	JAPAN14	<i>CA</i>	CANADA2			
Option	Description																																																					
<i>TG</i>	TOGO																																																					
<i>TT</i>	TRINIDAD AND TOBAGO																																																					
<i>TN</i>	TUNISIA																																																					
<i>TR</i>	TURKEY																																																					
<i>TM</i>	TURKMENISTAN																																																					
<i>AE</i>	UNITED ARAB EMIRATES																																																					
<i>TC</i>	TURKS AND CAICOS																																																					
<i>UG</i>	UGANDA																																																					
<i>UA</i>	UKRAINE																																																					
<i>GB</i>	UNITED KINGDOM																																																					
<i>US</i>	UNITED STATES2																																																					
<i>PS</i>	UNITED STATES (PUBLIC SAFETY)																																																					
<i>UY</i>	URUGUAY																																																					
<i>UZ</i>	UZBEKISTAN																																																					
<i>VU</i>	VANUATU																																																					
<i>VE</i>	VENEZUELA																																																					
<i>VN</i>	VIET NAM																																																					
<i>VI</i>	VIRGIN ISLANDS																																																					
<i>WF</i>	WALLIS AND FUTUNA																																																					
<i>YE</i>	YEMEN																																																					
<i>ZM</i>	ZAMBIA																																																					
<i>ZW</i>	ZIMBABWE																																																					
<i>JP</i>	JAPAN14																																																					
<i>CA</i>	CANADA2																																																					
ip-fragment-preventing	Method.	option	-	tcp-mss-adjust																																																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp-mss-adjust</i></td> <td>TCP maximum segment size adjustment.</td> </tr> <tr> <td><i>icmp-unreachable</i></td> <td>Drop packet and send ICMP Destination Unreachable</td> </tr> </tbody> </table>	Option	Description	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable																																															
Option	Description																																																					
<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.																																																					
<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable																																																					

Parameter	Description	Type	Size	Default								
tun-mtu-uplink	The maximum transmission unit .	integer	Minimum value: 576 Maximum value: 1500	0								
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel .	integer	Minimum value: 576 Maximum value: 1500	0								
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Split tunneling ACL list traffic will be tunnel.</td> </tr> <tr> <td><i>local</i></td> <td>Split tunneling ACL list traffic will be local NATed.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.	<i>local</i>	Split tunneling ACL list traffic will be local NATed.					
Option	Description											
<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.											
<i>local</i>	Split tunneling ACL list traffic will be local NATed.											
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.					
Option	Description											
<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.											
<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.											
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> </tbody> </table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description											
<i>https</i>	HTTPS access.											
<i>ssh</i>	SSH access.											
<i>snmp</i>	SNMP access.											
login-password-change	Change or reset the administrator password of a managed WTP, FortiAP or AP .	option	-	no								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>yes</i></td> <td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td> </tr> </tbody> </table>	Option	Description	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.							
Option	Description											
<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.											

Parameter	Description	Type	Size	Default																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td> </tr> <tr> <td><i>no</i></td> <td>Do not change the managed WTP, FortiAP or AP's administrator password.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.													
Option	Description																			
<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.																			
<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.																			
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified																	
lldp	Enable/disable Link Layer Discovery Protocol .	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable LLDP.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable LLDP.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable LLDP.	<i>disable</i>	Disable LLDP.													
Option	Description																			
<i>enable</i>	Enable LLDP.																			
<i>disable</i>	Disable LLDP.																			
poe-mode	Set the WTP, FortiAP, or AP's PoE mode.	option	-	auto																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Automatically detect the PoE mode.</td> </tr> <tr> <td><i>8023af</i></td> <td>Use 802.3af PoE mode.</td> </tr> <tr> <td><i>8023at</i></td> <td>Use 802.3at PoE mode.</td> </tr> <tr> <td><i>power-adapter</i></td> <td>Use the power adapter to control the PoE mode.</td> </tr> <tr> <td><i>full</i></td> <td>Use full power mode.</td> </tr> <tr> <td><i>high</i></td> <td>Use high power mode.</td> </tr> <tr> <td><i>low</i></td> <td>Use low power mode.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Automatically detect the PoE mode.	<i>8023af</i>	Use 802.3af PoE mode.	<i>8023at</i>	Use 802.3at PoE mode.	<i>power-adapter</i>	Use the power adapter to control the PoE mode.	<i>full</i>	Use full power mode.	<i>high</i>	Use high power mode.	<i>low</i>	Use low power mode.			
Option	Description																			
<i>auto</i>	Automatically detect the PoE mode.																			
<i>8023af</i>	Use 802.3af PoE mode.																			
<i>8023at</i>	Use 802.3at PoE mode.																			
<i>power-adapter</i>	Use the power adapter to control the PoE mode.																			
<i>full</i>	Use full power mode.																			
<i>high</i>	Use high power mode.																			
<i>low</i>	Use low power mode.																			
frequency-handoff	Enable/disable frequency handoff of clients to other channels .	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable frequency handoff.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable frequency handoff.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable frequency handoff.	<i>disable</i>	Disable frequency handoff.													
Option	Description																			
<i>enable</i>	Enable frequency handoff.																			
<i>disable</i>	Disable frequency handoff.																			
ap-handoff	Enable/disable AP handoff of clients to other APs .	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AP handoff.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AP handoff.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AP handoff.	<i>disable</i>	Disable AP handoff.													
Option	Description																			
<i>enable</i>	Enable AP handoff.																			
<i>disable</i>	Disable AP handoff.																			

Parameter	Description	Type	Size	Default
ext-info-enable	Enable/disable station/VAP/radio extension information.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable station/VAP/radio extension information.		
	<i>disable</i>	Disable station/VAP/radio extension information.		

## config platform

Parameter	Description	Type	Size	Default
type	WTP, FortiAP or AP platform type. There are built-in WTP profiles for all supported FortiAP models. You can select a built-in profile and customize it or create a new profile.	option	-	221E
	<b>Option</b>	<b>Description</b>		
	<i>AP-11N</i>	Default 11n AP.		
	<i>220B</i>	FAP220B/221B.		
	<i>210B</i>	FAP210B.		
	<i>222B</i>	FAP222B.		
	<i>112B</i>	FAP112B.		
	<i>320B</i>	FAP320B.		
	<i>11C</i>	FAP11C.		
	<i>14C</i>	FAP14C.		
	<i>223B</i>	FAP223B.		
	<i>28C</i>	FAP28C.		
	<i>320C</i>	FAP320C.		
	<i>221C</i>	FAP221C.		
	<i>25D</i>	FAP25D.		
	<i>222C</i>	FAP222C.		
	<i>224D</i>	FAP224D.		
	<i>214B</i>	FK214B.		
	<i>21D</i>	FAP21D.		
	<i>24D</i>	FAP24D.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>112D</i>	FAP112D.		
	<i>223C</i>	FAP223C.		
	<i>321C</i>	FAP321C.		
	<i>C220C</i>	FAPC220C.		
	<i>C225C</i>	FAPC225C.		
	<i>C23JD</i>	FAPC23JD.		
	<i>C24JE</i>	FAPC24JE.		
	<i>S321C</i>	FAPS321C.		
	<i>S322C</i>	FAPS322C.		
	<i>S323C</i>	FAPS323C.		
	<i>S311C</i>	FAPS311C.		
	<i>S313C</i>	FAPS313C.		
	<i>S321CR</i>	FAPS321CR.		
	<i>S322CR</i>	FAPS322CR.		
	<i>S323CR</i>	FAPS323CR.		
	<i>S421E</i>	FAPS421E.		
	<i>S422E</i>	FAPS422E.		
	<i>S423E</i>	FAPS423E.		
	<i>421E</i>	FAP421E.		
	<i>423E</i>	FAP423E.		
	<i>221E</i>	FAP221E.		
	<i>222E</i>	FAP222E.		
	<i>223E</i>	FAP223E.		
	<i>224E</i>	FAP224E.		
	<i>231E</i>	FAP231E.		
	<i>S221E</i>	FAPS221E.		
	<i>S223E</i>	FAPS223E.		
	<i>321E</i>	FAP321E.		
	<i>431F</i>	FAP431F.		

Parameter	Description	Type	Size	Default																																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>432F</i></td> <td>FAP432F.</td> </tr> <tr> <td><i>433F</i></td> <td>FAP433F.</td> </tr> <tr> <td><i>231F</i></td> <td>FAP231F.</td> </tr> <tr> <td><i>234F</i></td> <td>FAP234F.</td> </tr> <tr> <td><i>23JF</i></td> <td>FAP23JF.</td> </tr> <tr> <td><i>831F</i></td> <td>FAP831F.</td> </tr> <tr> <td><i>U421E</i></td> <td>FAPU421EV.</td> </tr> <tr> <td><i>U422EV</i></td> <td>FAPU422EV.</td> </tr> <tr> <td><i>U423E</i></td> <td>FAPU423EV.</td> </tr> <tr> <td><i>U221EV</i></td> <td>FAPU221EV.</td> </tr> <tr> <td><i>U223EV</i></td> <td>FAPU223EV.</td> </tr> <tr> <td><i>U24JEV</i></td> <td>FAPU24JEV.</td> </tr> <tr> <td><i>U321EV</i></td> <td>FAPU321EV.</td> </tr> <tr> <td><i>U323EV</i></td> <td>FAPU323EV.</td> </tr> <tr> <td><i>U431F</i></td> <td>FAPU431F.</td> </tr> <tr> <td><i>U433F</i></td> <td>FAPU433F.</td> </tr> <tr> <td><i>U231F</i></td> <td>FAPU231F.</td> </tr> <tr> <td><i>U234F</i></td> <td>FAPU234F.</td> </tr> <tr> <td><i>U432F</i></td> <td>FAPU432F.</td> </tr> </tbody> </table>	Option	Description	<i>432F</i>	FAP432F.	<i>433F</i>	FAP433F.	<i>231F</i>	FAP231F.	<i>234F</i>	FAP234F.	<i>23JF</i>	FAP23JF.	<i>831F</i>	FAP831F.	<i>U421E</i>	FAPU421EV.	<i>U422EV</i>	FAPU422EV.	<i>U423E</i>	FAPU423EV.	<i>U221EV</i>	FAPU221EV.	<i>U223EV</i>	FAPU223EV.	<i>U24JEV</i>	FAPU24JEV.	<i>U321EV</i>	FAPU321EV.	<i>U323EV</i>	FAPU323EV.	<i>U431F</i>	FAPU431F.	<i>U433F</i>	FAPU433F.	<i>U231F</i>	FAPU231F.	<i>U234F</i>	FAPU234F.	<i>U432F</i>	FAPU432F.			
Option	Description																																											
<i>432F</i>	FAP432F.																																											
<i>433F</i>	FAP433F.																																											
<i>231F</i>	FAP231F.																																											
<i>234F</i>	FAP234F.																																											
<i>23JF</i>	FAP23JF.																																											
<i>831F</i>	FAP831F.																																											
<i>U421E</i>	FAPU421EV.																																											
<i>U422EV</i>	FAPU422EV.																																											
<i>U423E</i>	FAPU423EV.																																											
<i>U221EV</i>	FAPU221EV.																																											
<i>U223EV</i>	FAPU223EV.																																											
<i>U24JEV</i>	FAPU24JEV.																																											
<i>U321EV</i>	FAPU321EV.																																											
<i>U323EV</i>	FAPU323EV.																																											
<i>U431F</i>	FAPU431F.																																											
<i>U433F</i>	FAPU433F.																																											
<i>U231F</i>	FAPU231F.																																											
<i>U234F</i>	FAPU234F.																																											
<i>U432F</i>	FAPU432F.																																											
mode	Configure operation mode of 5G radios .	option	-	single-5G																																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>single-5G</i></td> <td>Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.</td> </tr> <tr> <td><i>dual-5G</i></td> <td>Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.</td> </tr> </tbody> </table>	Option	Description	<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.	<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.																																					
Option	Description																																											
<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.																																											
<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.																																											
ddscan	Enable/disable use of one radio for dedicated dual-band scanning to detect RF characterization and wireless threat management.	option	-	disable																																								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable dedicated dual-band scan mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable dedicated dual-band scan mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable dedicated dual-band scan mode.	<i>disable</i>	Disable dedicated dual-band scan mode.			
Option	Description									
<i>enable</i>	Enable dedicated dual-band scan mode.									
<i>disable</i>	Disable dedicated dual-band scan mode.									

## config lan

Parameter	Description	Type	Size	Default										
port-mode	LAN port mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15											
port1-mode	LAN port 1 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15											
port2-mode	LAN port 2 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15											



Parameter	Description	Type	Size	Default										
port3-mode	LAN port 3 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15											
port4-mode	LAN port 4 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15											
port5-mode	LAN port 5 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15											
port6-mode	LAN port 6 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													

Parameter	Description	Type	Size	Default										
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15											
port7-mode	LAN port 7 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15											
port8-mode	LAN port 8 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15											
port-esl-mode	ESL port mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP ESL port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP ESL port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP ESL port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.													
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15											

### config deny-mac-list

Parameter	Description	Type	Size	Default
mac	A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.	mac-address	Not Specified	00:00:00:00:00:00

## config split-tunneling-acl

Parameter	Description	Type	Size	Default
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config radio-1

Parameter	Description	Type	Size	Default																												
mode	Mode of radio 1. Radio 1 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-	ap																												
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disabled</i></td><td>Radio 1 is disabled.</td></tr><tr><td><i>ap</i></td><td>Radio 1 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td><i>monitor</i></td><td>Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr><tr><td><i>sniffer</i></td><td>Radio 1 operates as a sniffer capturing WiFi frames on air.</td></tr></tbody></table>	Option	Description	<i>disabled</i>	Radio 1 is disabled.	<i>ap</i>	Radio 1 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 1 operates as a sniffer capturing WiFi frames on air.																					
Option	Description																															
<i>disabled</i>	Radio 1 is disabled.																															
<i>ap</i>	Radio 1 operates as an access point that allows WiFi clients to connect to your network.																															
<i>monitor</i>	Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																															
<i>sniffer</i>	Radio 1 operates as a sniffer capturing WiFi frames on air.																															
band	WiFi band that Radio 1 operates on.	option	-																													
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g/b.</td></tr><tr><td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr><tr><td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr><tr><td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr><tr><td><i>802.11g-only</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr><tr><td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr></tbody></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.			
Option	Description																															
<i>802.11a</i>	802.11a.																															
<i>802.11b</i>	802.11b.																															
<i>802.11g</i>	802.11g/b.																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																															
<i>802.11ac</i>	802.11ac/n/a.																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																															
<i>802.11g-only</i>	802.11g.																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																															

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																					
<i>802.11ac,n-only</i>	802.11ac/n.																					
<i>802.11ac-only</i>	802.11ac.																					
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																					
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																					
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																					
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																					
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																					
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																					
band-5g-type	WiFi 5G band type.	option	-	5g-full																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>5g-full</i></td> <td>Full 5G band.</td> </tr> <tr> <td><i>5g-high</i></td> <td>High 5G band.</td> </tr> <tr> <td><i>5g-low</i></td> <td>Low 5G band.</td> </tr> </tbody> </table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.													
Option	Description																					
<i>5g-full</i>	Full 5G band.																					
<i>5g-high</i>	High 5G band.																					
<i>5g-low</i>	Low 5G band.																					
drma	Enable/disable dynamic radio mode assignment .	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dynamic radio mode assignment (DRMA).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dynamic radio mode assignment (DRMA).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).															
Option	Description																					
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).																					
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).																					
drma-sensitivity	Network Coverage Factor .	option	-	low																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Consider a radio as redundant when its NCF is 100%.</td> </tr> <tr> <td><i>medium</i></td> <td>Consider a radio as redundant when its NCF is 95%.</td> </tr> <tr> <td><i>high</i></td> <td>Consider a radio as redundant when its NCF is 90%.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.													
Option	Description																					
<i>low</i>	Consider a radio as redundant when its NCF is 100%.																					
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.																					
<i>high</i>	Consider a radio as redundant when its NCF is 90%.																					
airtime-fairness	Enable/disable airtime fairness .	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable airtime fairness (ATF) support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.																	
Option	Description																					
<i>enable</i>	Enable airtime fairness (ATF) support.																					

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable airtime fairness (ATF) support.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable airtime fairness (ATF) support.											
Option	Description															
<i>disable</i>	Disable airtime fairness (ATF) support.															
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rtscts</i></td> <td>Enable 802.11g protection RTS/CTS mode.</td> </tr> <tr> <td><i>ctsonly</i></td> <td>Enable 802.11g protection CTS only mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11g protection mode.</td> </tr> </tbody> </table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.							
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.															
<i>disable</i>	Disable 802.11g protection mode.															
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tim</i></td> <td>TIM bit for client in power save mode.</td> </tr> <tr> <td><i>ac-vo</i></td> <td>Use AC VO priority to send out packets in the power save queue.</td> </tr> <tr> <td><i>no-obss-scan</i></td> <td>Do not put OBSS scan IE into beacon and probe response frames.</td> </tr> <tr> <td><i>no-11b-rate</i></td> <td>Do not send frame using 11b data rate.</td> </tr> <tr> <td><i>client-rate-follow</i></td> <td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td> </tr> </tbody> </table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet transmission optimization.</td> </tr> <tr> <td><i>power-save</i></td> <td>Tag client as operating in power save mode if excessive transmit retries occur.</td> </tr> <tr> <td><i>aggr-limit</i></td> <td>Set aggregation limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>retry-limit</i></td> <td>Set software retry limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>send-bar</i></td> <td>Limit transmission of BAR frames.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.			
Option	Description															
<i>disable</i>	Disable packet transmission optimization.															
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.															
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.															
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.															
<i>send-bar</i>	Limit transmission of BAR frames.															
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-	enable												

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AMSDU support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AMSDU support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.							
Option	Description													
<i>enable</i>	Enable AMSDU support.													
<i>disable</i>	Disable AMSDU support.													
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support for both HT20 and HT40 on the same radio.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support for both HT20 and HT40 on the same radio.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.							
Option	Description													
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.													
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.													
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable zero wait DFS</td> </tr> <tr> <td><i>disable</i></td> <td>Disable zero wait DFS</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS							
Option	Description													
<i>enable</i>	Enable zero wait DFS													
<i>disable</i>	Disable zero wait DFS													
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0										
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Select the 400 ns short guard interval (Short GI).</td> </tr> <tr> <td><i>disable</i></td> <td>Select the 800 ns long guard interval (Long GI).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>160MHz</i></td> <td>160 MHz channel width.</td> </tr> <tr> <td><i>80MHz</i></td> <td>80 MHz channel width.</td> </tr> <tr> <td><i>40MHz</i></td> <td>40 MHz channel width.</td> </tr> <tr> <td><i>20MHz</i></td> <td>20 MHz channel width.</td> </tr> </tbody> </table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													

Parameter	Description	Type	Size	Default						
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17						
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10						
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70						
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100						
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1						
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346						

Parameter	Description	Type	Size	Default						
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	36						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management beacon frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi management beacon frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management probe frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Enable sniffer on WiFi management probe frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management other frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi management other frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi control frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi control frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi control frame.									
<i>disable</i>	Disable sniffer on WiFi control frame.									
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable						



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi data frame</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi data frame</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi data frame											
<i>disable</i>	Disable sniffer on WiFi data frame											
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable measuring channel utilization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable measuring channel utilization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.					
Option	Description											
<i>enable</i>	Enable measuring channel utilization.											
<i>disable</i>	Disable measuring channel utilization.											
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35									
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable distributed automatic radio resource provisioning.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable distributed automatic radio resource provisioning.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.					
Option	Description											
<i>enable</i>	Enable distributed automatic radio resource provisioning.											
<i>disable</i>	Disable distributed automatic radio resource provisioning.											
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0								
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3							
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM call admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM call admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10						
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM bandwidth admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM bandwidth admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000						

## config radio-2

Parameter	Description	Type	Size	Default						
mode	Mode of radio 2. Radio 2 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-	ap						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Radio 2 is disabled.</td> </tr> <tr> <td><i>ap</i></td> <td>Radio 2 operates as an access point that allows WiFi clients to connect to your network.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Radio 2 is disabled.	<i>ap</i>	Radio 2 operates as an access point that allows WiFi clients to connect to your network.			
Option	Description									
<i>disabled</i>	Radio 2 is disabled.									
<i>ap</i>	Radio 2 operates as an access point that allows WiFi clients to connect to your network.									

Parameter	Description	Type	Size	Default																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>monitor</i></td> <td>Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td> </tr> <tr> <td><i>sniffer</i></td> <td>Radio 2 operates as a sniffer capturing WiFi frames on air.</td> </tr> </tbody> </table>	Option	Description	<i>monitor</i>	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.																																									
Option	Description																																															
<i>monitor</i>	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																																															
<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.																																															
band	WiFi band that Radio 2 operates on.	option	-																																													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																																															
<i>802.11a</i>	802.11a.																																															
<i>802.11b</i>	802.11b.																																															
<i>802.11g</i>	802.11g/b.																																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																															
<i>802.11ac</i>	802.11ac/n/a.																																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																															
<i>802.11g-only</i>	802.11g.																																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																															
<i>802.11ac,n-only</i>	802.11ac/n.																																															
<i>802.11ac-only</i>	802.11ac.																																															
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																															
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																															
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																															
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																															
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																															
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																															
band-5g-type	WiFi 5G band type.	option	-	5g-full																																												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>5g-full</i></td> <td>Full 5G band.</td> </tr> <tr> <td><i>5g-high</i></td> <td>High 5G band.</td> </tr> <tr> <td><i>5g-low</i></td> <td>Low 5G band.</td> </tr> </tbody> </table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.			
Option	Description											
<i>5g-full</i>	Full 5G band.											
<i>5g-high</i>	High 5G band.											
<i>5g-low</i>	Low 5G band.											
drma	Enable/disable dynamic radio mode assignment .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dynamic radio mode assignment (DRMA).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dynamic radio mode assignment (DRMA).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).					
Option	Description											
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).											
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
drma-sensitivity	Network Coverage Factor .	option	-	low								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Consider a radio as redundant when its NCF is 100%.</td> </tr> <tr> <td><i>medium</i></td> <td>Consider a radio as redundant when its NCF is 95%.</td> </tr> <tr> <td><i>high</i></td> <td>Consider a radio as redundant when its NCF is 90%.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.			
Option	Description											
<i>low</i>	Consider a radio as redundant when its NCF is 100%.											
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.											
<i>high</i>	Consider a radio as redundant when its NCF is 90%.											
airtime-fairness	Enable/disable airtime fairness .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable airtime fairness (ATF) support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable airtime fairness (ATF) support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.					
Option	Description											
<i>enable</i>	Enable airtime fairness (ATF) support.											
<i>disable</i>	Disable airtime fairness (ATF) support.											
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rtscts</i></td> <td>Enable 802.11g protection RTS/CTS mode.</td> </tr> <tr> <td><i>ctsonly</i></td> <td>Enable 802.11g protection CTS only mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11g protection mode.</td> </tr> </tbody> </table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.			
Option	Description											
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.											
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.											
<i>disable</i>	Disable 802.11g protection mode.											
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tim</i></td> <td>TIM bit for client in power save mode.</td> </tr> <tr> <td><i>ac-vo</i></td> <td>Use AC VO priority to send out packets in the power save queue.</td> </tr> <tr> <td><i>no-obss-scan</i></td> <td>Do not put OBSS scan IE into beacon and probe response frames.</td> </tr> <tr> <td><i>no-11b-rate</i></td> <td>Do not send frame using 11b data rate.</td> </tr> <tr> <td><i>client-rate-follow</i></td> <td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td> </tr> </tbody> </table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet transmission optimization.</td> </tr> <tr> <td><i>power-save</i></td> <td>Tag client as operating in power save mode if excessive transmit retries occur.</td> </tr> <tr> <td><i>aggr-limit</i></td> <td>Set aggregation limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>retry-limit</i></td> <td>Set software retry limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>send-bar</i></td> <td>Limit transmission of BAR frames.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.			
Option	Description															
<i>disable</i>	Disable packet transmission optimization.															
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.															
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.															
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.															
<i>send-bar</i>	Limit transmission of BAR frames.															
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AMSDU support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AMSDU support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.									
Option	Description															
<i>enable</i>	Enable AMSDU support.															
<i>disable</i>	Disable AMSDU support.															
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support for both HT20 and HT40 on the same radio.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support for both HT20 and HT40 on the same radio.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.									
Option	Description															
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.															
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.															
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable zero wait DFS</td> </tr> <tr> <td><i>disable</i></td> <td>Disable zero wait DFS</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS									
Option	Description															
<i>enable</i>	Enable zero wait DFS															
<i>disable</i>	Disable zero wait DFS															

Parameter	Description	Type	Size	Default										
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0										
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Select the 400 ns short guard interval (Short GI).</td> </tr> <tr> <td><i>disable</i></td> <td>Select the 800 ns long guard interval (Long GI).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>160MHz</i></td> <td>160 MHz channel width.</td> </tr> <tr> <td><i>80MHz</i></td> <td>80 MHz channel width.</td> </tr> <tr> <td><i>40MHz</i></td> <td>40 MHz channel width.</td> </tr> <tr> <td><i>20MHz</i></td> <td>20 MHz channel width.</td> </tr> </tbody> </table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.							
Option	Description													
<i>enable</i>	Enable automatic transmit power adjustment.													
<i>disable</i>	Disable automatic transmit power adjustment.													
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17										
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10										

Parameter	Description	Type	Size	Default						
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70						
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100						
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1						
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346						
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	6						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management beacon frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi management beacon frame.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									

Parameter	Description	Type	Size	Default
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi management probe frame.		
	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi management other frame.		
	<i>disable</i>	Disable sniffer on WiFi management other frame.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable measuring channel utilization.		
	<i>disable</i>	Disable measuring channel utilization.		
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35	
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable distributed automatic radio resource provisioning.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable distributed automatic radio resource provisioning.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.					
Option	Description											
<i>enable</i>	Enable distributed automatic radio resource provisioning.											
<i>disable</i>	Disable distributed automatic radio resource provisioning.											
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0								
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM call admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM call admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.					
Option	Description											
<i>enable</i>	Enable WMM call admission control.											
<i>disable</i>	Disable WMM call admission control.											
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10								

Parameter	Description	Type	Size	Default						
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM bandwidth admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM bandwidth admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000						

### config radio-3

Parameter	Description	Type	Size	Default														
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-	ap														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Radio 3 is disabled.</td> </tr> <tr> <td><i>ap</i></td> <td>Radio 3 operates as an access point that allows WiFi clients to connect to your network.</td> </tr> <tr> <td><i>monitor</i></td> <td>Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td> </tr> <tr> <td><i>sniffer</i></td> <td>Radio 3 operates as a sniffer capturing WiFi frames on air.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Radio 3 is disabled.	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.							
Option	Description																	
<i>disabled</i>	Radio 3 is disabled.																	
<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.																	
<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																	
<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.																	
band	WiFi band that Radio 3 operates on.	option	-															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.			
Option	Description																	
<i>802.11a</i>	802.11a.																	
<i>802.11b</i>	802.11b.																	
<i>802.11g</i>	802.11g/b.																	
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																	
<i>802.11n-5G</i>	802.11n/a at 5GHz.																	
<i>802.11ac</i>	802.11ac/n/a.																	

Parameter	Description	Type	Size	Default																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																																			
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																			
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																			
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																			
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																			
<i>802.11g-only</i>	802.11g.																																			
<i>802.11n-only</i>	802.11n at 2.4GHz.																																			
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																			
<i>802.11ac,n-only</i>	802.11ac/n.																																			
<i>802.11ac-only</i>	802.11ac.																																			
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																			
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																			
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																			
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																			
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																			
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																			
band-5g-type	WiFi 5G band type.	option	-	5g-full																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>5g-full</i></td> <td>Full 5G band.</td> </tr> <tr> <td><i>5g-high</i></td> <td>High 5G band.</td> </tr> <tr> <td><i>5g-low</i></td> <td>Low 5G band.</td> </tr> </tbody> </table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.																											
Option	Description																																			
<i>5g-full</i>	Full 5G band.																																			
<i>5g-high</i>	High 5G band.																																			
<i>5g-low</i>	Low 5G band.																																			
drma	Enable/disable dynamic radio mode assignment .	option	-	disable																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dynamic radio mode assignment (DRMA).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dynamic radio mode assignment (DRMA).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).																													
Option	Description																																			
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).																																			
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).																																			
drma-sensitivity	Network Coverage Factor .	option	-	low																																

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Consider a radio as redundant when its NCF is 100%.</td> </tr> <tr> <td><i>medium</i></td> <td>Consider a radio as redundant when its NCF is 95%.</td> </tr> <tr> <td><i>high</i></td> <td>Consider a radio as redundant when its NCF is 90%.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.							
Option	Description															
<i>low</i>	Consider a radio as redundant when its NCF is 100%.															
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.															
<i>high</i>	Consider a radio as redundant when its NCF is 90%.															
airtime-fairness	Enable/disable airtime fairness .	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable airtime fairness (ATF) support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable airtime fairness (ATF) support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.									
Option	Description															
<i>enable</i>	Enable airtime fairness (ATF) support.															
<i>disable</i>	Disable airtime fairness (ATF) support.															
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rtscts</i></td> <td>Enable 802.11g protection RTS/CTS mode.</td> </tr> <tr> <td><i>ctsonly</i></td> <td>Enable 802.11g protection CTS only mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11g protection mode.</td> </tr> </tbody> </table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.							
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.															
<i>disable</i>	Disable 802.11g protection mode.															
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tim</i></td> <td>TIM bit for client in power save mode.</td> </tr> <tr> <td><i>ac-vo</i></td> <td>Use AC VO priority to send out packets in the power save queue.</td> </tr> <tr> <td><i>no-obss-scan</i></td> <td>Do not put OBSS scan IE into beacon and probe response frames.</td> </tr> <tr> <td><i>no-11b-rate</i></td> <td>Do not send frame using 11b data rate.</td> </tr> <tr> <td><i>client-rate-follow</i></td> <td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td> </tr> </tbody> </table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet transmission optimization.</td> </tr> <tr> <td><i>power-save</i></td> <td>Tag client as operating in power save mode if excessive transmit retries occur.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.									
Option	Description															
<i>disable</i>	Disable packet transmission optimization.															
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.															

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aggr-limit</i></td> <td>Set aggregation limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>retry-limit</i></td> <td>Set software retry limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>send-bar</i></td> <td>Limit transmission of BAR frames.</td> </tr> </tbody> </table>	Option	Description	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.			
Option	Description											
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.											
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.											
<i>send-bar</i>	Limit transmission of BAR frames.											
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AMSDU support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AMSDU support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.					
Option	Description											
<i>enable</i>	Enable AMSDU support.											
<i>disable</i>	Disable AMSDU support.											
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support for both HT20 and HT40 on the same radio.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support for both HT20 and HT40 on the same radio.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.					
Option	Description											
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.											
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.											
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable zero wait DFS</td> </tr> <tr> <td><i>disable</i></td> <td>Disable zero wait DFS</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS					
Option	Description											
<i>enable</i>	Enable zero wait DFS											
<i>disable</i>	Disable zero wait DFS											
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0								
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Select the 400 ns short guard interval (Short GI).</td> </tr> <tr> <td><i>disable</i></td> <td>Select the 800 ns long guard interval (Long GI).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).					
Option	Description											
<i>enable</i>	Select the 400 ns short guard interval (Short GI).											
<i>disable</i>	Select the 800 ns long guard interval (Long GI).											
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz								

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>160MHz</i></td> <td>160 MHz channel width.</td> </tr> <tr> <td><i>80MHz</i></td> <td>80 MHz channel width.</td> </tr> <tr> <td><i>40MHz</i></td> <td>40 MHz channel width.</td> </tr> <tr> <td><i>20MHz</i></td> <td>20 MHz channel width.</td> </tr> </tbody> </table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.							
Option	Description													
<i>enable</i>	Enable automatic transmit power adjustment.													
<i>disable</i>	Disable automatic transmit power adjustment.													
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17										
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10										
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70										
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100										
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1										
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100										

Parameter	Description	Type	Size	Default
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	6
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi management beacon frame.		
	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi management probe frame.		
	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer on WiFi management other frame.		
	<i>disable</i>	Disable sniffer on WiFi management other frame.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi control frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi control frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi control frame.									
<i>disable</i>	Disable sniffer on WiFi control frame.									
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi data frame</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi data frame</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi data frame									
<i>disable</i>	Disable sniffer on WiFi data frame									
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable measuring channel utilization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable measuring channel utilization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.			
Option	Description									
<i>enable</i>	Enable measuring channel utilization.									
<i>disable</i>	Disable measuring channel utilization.									
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable distributed automatic radio resource provisioning.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable distributed automatic radio resource provisioning.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.			
Option	Description									
<i>enable</i>	Enable distributed automatic radio resource provisioning.									
<i>disable</i>	Disable distributed automatic radio resource provisioning.									
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0						
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel						



Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM call admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM call admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.					
Option	Description											
<i>enable</i>	Enable WMM call admission control.											
<i>disable</i>	Disable WMM call admission control.											
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10								
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM bandwidth admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM bandwidth admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.					
Option	Description											
<i>enable</i>	Enable WMM bandwidth admission control.											
<i>disable</i>	Disable WMM bandwidth admission control.											
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000								

## config radio-4

Parameter	Description	Type	Size	Default																																						
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-	ap																																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disabled</i></td> <td>Radio 3 is disabled.</td> </tr> <tr> <td><i>ap</i></td> <td>Radio 3 operates as an access point that allows WiFi clients to connect to your network.</td> </tr> <tr> <td><i>monitor</i></td> <td>Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td> </tr> <tr> <td><i>sniffer</i></td> <td>Radio 3 operates as a sniffer capturing WiFi frames on air.</td> </tr> </tbody> </table>	Option	Description	<i>disabled</i>	Radio 3 is disabled.	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.																															
Option	Description																																									
<i>disabled</i>	Radio 3 is disabled.																																									
<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.																																									
<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																																									
<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.																																									
band	WiFi band that Radio 3 operates on.	option	-																																							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.			
Option	Description																																									
<i>802.11a</i>	802.11a.																																									
<i>802.11b</i>	802.11b.																																									
<i>802.11g</i>	802.11g/b.																																									
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																									
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																									
<i>802.11ac</i>	802.11ac/n/a.																																									
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																									
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																									
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																									
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																									
<i>802.11g-only</i>	802.11g.																																									
<i>802.11n-only</i>	802.11n at 2.4GHz.																																									
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																									
<i>802.11ac,n-only</i>	802.11ac/n.																																									
<i>802.11ac-only</i>	802.11ac.																																									
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																									
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																									
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																									

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description											
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.											
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.											
<i>802.11ax-only</i>	802.11ax at 2.4GHz.											
band-5g-type	WiFi 5G band type.	option	-	5g-full								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>5g-full</i></td> <td>Full 5G band.</td> </tr> <tr> <td><i>5g-high</i></td> <td>High 5G band.</td> </tr> <tr> <td><i>5g-low</i></td> <td>Low 5G band.</td> </tr> </tbody> </table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.			
Option	Description											
<i>5g-full</i>	Full 5G band.											
<i>5g-high</i>	High 5G band.											
<i>5g-low</i>	Low 5G band.											
drma	Enable/disable dynamic radio mode assignment .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable dynamic radio mode assignment (DRMA).</td> </tr> <tr> <td><i>enable</i></td> <td>Enable dynamic radio mode assignment (DRMA).</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).					
Option	Description											
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).											
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
drma-sensitivity	Network Coverage Factor .	option	-	low								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>low</i></td> <td>Consider a radio as redundant when its NCF is 100%.</td> </tr> <tr> <td><i>medium</i></td> <td>Consider a radio as redundant when its NCF is 95%.</td> </tr> <tr> <td><i>high</i></td> <td>Consider a radio as redundant when its NCF is 90%.</td> </tr> </tbody> </table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.			
Option	Description											
<i>low</i>	Consider a radio as redundant when its NCF is 100%.											
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.											
<i>high</i>	Consider a radio as redundant when its NCF is 90%.											
airtime-fairness	Enable/disable airtime fairness .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable airtime fairness (ATF) support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable airtime fairness (ATF) support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.					
Option	Description											
<i>enable</i>	Enable airtime fairness (ATF) support.											
<i>disable</i>	Disable airtime fairness (ATF) support.											
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable								

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rtscts</i></td> <td>Enable 802.11g protection RTS/CTS mode.</td> </tr> <tr> <td><i>ctsonly</i></td> <td>Enable 802.11g protection CTS only mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable 802.11g protection mode.</td> </tr> </tbody> </table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.							
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.															
<i>disable</i>	Disable 802.11g protection mode.															
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tim</i></td> <td>TIM bit for client in power save mode.</td> </tr> <tr> <td><i>ac-vo</i></td> <td>Use AC VO priority to send out packets in the power save queue.</td> </tr> <tr> <td><i>no-obss-scan</i></td> <td>Do not put OBSS scan IE into beacon and probe response frames.</td> </tr> <tr> <td><i>no-11b-rate</i></td> <td>Do not send frame using 11b data rate.</td> </tr> <tr> <td><i>client-rate-follow</i></td> <td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td> </tr> </tbody> </table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable packet transmission optimization.</td> </tr> <tr> <td><i>power-save</i></td> <td>Tag client as operating in power save mode if excessive transmit retries occur.</td> </tr> <tr> <td><i>aggr-limit</i></td> <td>Set aggregation limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>retry-limit</i></td> <td>Set software retry limit to a lower value when data rate is low.</td> </tr> <tr> <td><i>send-bar</i></td> <td>Limit transmission of BAR frames.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.			
Option	Description															
<i>disable</i>	Disable packet transmission optimization.															
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.															
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.															
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.															
<i>send-bar</i>	Limit transmission of BAR frames.															
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AMSDU support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AMSDU support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.									
Option	Description															
<i>enable</i>	Enable AMSDU support.															
<i>disable</i>	Disable AMSDU support.															
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-	enable												

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable support for both HT20 and HT40 on the same radio.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable support for both HT20 and HT40 on the same radio.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.							
Option	Description													
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.													
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.													
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable zero wait DFS</td> </tr> <tr> <td><i>disable</i></td> <td>Disable zero wait DFS</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS							
Option	Description													
<i>enable</i>	Enable zero wait DFS													
<i>disable</i>	Disable zero wait DFS													
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0										
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Select the 400 ns short guard interval (Short GI).</td> </tr> <tr> <td><i>disable</i></td> <td>Select the 800 ns long guard interval (Long GI).</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>160MHz</i></td> <td>160 MHz channel width.</td> </tr> <tr> <td><i>80MHz</i></td> <td>80 MHz channel width.</td> </tr> <tr> <td><i>40MHz</i></td> <td>40 MHz channel width.</td> </tr> <tr> <td><i>20MHz</i></td> <td>20 MHz channel width.</td> </tr> </tbody> </table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.							
Option	Description													
<i>enable</i>	Enable automatic transmit power adjustment.													
<i>disable</i>	Disable automatic transmit power adjustment.													

Parameter	Description	Type	Size	Default
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm .	string	Maximum length: 7	-70
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	6

Parameter	Description	Type	Size	Default						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management beacon frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi management beacon frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management probe frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Enable sniffer on WiFi management probe frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi management other frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi management other frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi control frame.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi control frame.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi control frame.									
<i>disable</i>	Disable sniffer on WiFi control frame.									
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable sniffer on WiFi data frame</td> </tr> <tr> <td><i>disable</i></td> <td>Disable sniffer on WiFi data frame</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi data frame									
<i>disable</i>	Disable sniffer on WiFi data frame									
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable measuring channel utilization.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable measuring channel utilization.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.					
Option	Description											
<i>enable</i>	Enable measuring channel utilization.											
<i>disable</i>	Disable measuring channel utilization.											
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35									
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable distributed automatic radio resource provisioning.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable distributed automatic radio resource provisioning.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.					
Option	Description											
<i>enable</i>	Enable distributed automatic radio resource provisioning.											
<i>disable</i>	Disable distributed automatic radio resource provisioning.											
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0								
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM call admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM call admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10						
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM bandwidth admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM bandwidth admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000						

## config lbs

Parameter	Description	Type	Size	Default						
ekahau-blink-mode	Enable/disable Ekahau blink mode .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Ekahau blink mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Ekahau blink mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Ekahau blink mode.	<i>disable</i>	Disable Ekahau blink mode.			
Option	Description									
<i>enable</i>	Enable Ekahau blink mode.									
<i>disable</i>	Disable Ekahau blink mode.									
ekahau-tag	WiFi frame MAC address or WiFi Tag.	mac-address	Not Specified	01:18:8e:00:00:00						
erc-server-ip	IP address of Ekahau RTLS Controller (ERC).	ipv4-address-any	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
erc-server-port	Ekahau RTLS Controller (ERC) UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	8569						
aeroscout	Enable/disable AeroScout Real Time Location Service .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AeroScout support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AeroScout support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AeroScout support.	<i>disable</i>	Disable AeroScout support.			
Option	Description									
<i>enable</i>	Enable AeroScout support.									
<i>disable</i>	Disable AeroScout support.									
aeroscout-server-ip	IP address of AeroScout server.	ipv4-address-any	Not Specified	0.0.0.0						
aeroscout-server-port	AeroScout server UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	0						
aeroscout-mu	Enable/disable AeroScout Mobile Unit .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable AeroScout MU mode support.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable AeroScout MU mode support.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AeroScout MU mode support.	<i>disable</i>	Disable AeroScout MU mode support.			
Option	Description									
<i>enable</i>	Enable AeroScout MU mode support.									
<i>disable</i>	Disable AeroScout MU mode support.									
aeroscout-ap-mac	Use BSSID or board MAC address as AP MAC address in AeroScout AP messages .	option	-	bssid						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bssid</i></td> <td>Use BSSID as AP MAC address in AeroScout AP messages.</td> </tr> <tr> <td><i>board-mac</i></td> <td>Use board MAC address as AP MAC address in AeroScout AP messages.</td> </tr> </tbody> </table>	Option	Description	<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.	<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.			
Option	Description									
<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.									
<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.									
aeroscout-mmureport	Enable/disable compounded AeroScout tag and MU report .	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable compounded AeroScout tag and MU report.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable compounded AeroScout tag and MU report.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable compounded AeroScout tag and MU report.	<i>disable</i>	Disable compounded AeroScout tag and MU report.			
Option	Description									
<i>enable</i>	Enable compounded AeroScout tag and MU report.									
<i>disable</i>	Disable compounded AeroScout tag and MU report.									

Parameter	Description	Type	Size	Default								
aeroscout-mu-factor	AeroScout MU mode dilution factor .	integer	Minimum value: 0 Maximum value: 4294967295	20								
aeroscout-mu-timeout	AeroScout MU mode timeout .	integer	Minimum value: 0 Maximum value: 65535	5								
fortipresence	Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>foreign</i></td> <td>FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.</td> </tr> <tr> <td><i>both</i></td> <td>Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiPresence.</td> </tr> </tbody> </table>	Option	Description	<i>foreign</i>	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.	<i>both</i>	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.	<i>disable</i>	Disable FortiPresence.			
Option	Description											
<i>foreign</i>	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.											
<i>both</i>	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.											
<i>disable</i>	Disable FortiPresence.											
fortipresence-server	FortiPresence server IP address.	ipv4-address-any	Not Specified	0.0.0.0								
fortipresence-port	FortiPresence server UDP listening port .	integer	Minimum value: 300 Maximum value: 65535	3000								
fortipresence-secret	FortiPresence secret password (max. 16 characters).	password	Not Specified									
fortipresence-project	FortiPresence project name .	string	Maximum length: 16	fortipresence								
fortipresence-frequency	FortiPresence report transmit frequency .	integer	Minimum value: 5 Maximum value: 65535	30								
fortipresence-rogue	Enable/disable FortiPresence finding and reporting rogue APs.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiPresence finding and reporting rogue APs.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiPresence finding and reporting rogue APs.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiPresence finding and reporting rogue APs.	<i>disable</i>	Disable FortiPresence finding and reporting rogue APs.			
Option	Description									
<i>enable</i>	Enable FortiPresence finding and reporting rogue APs.									
<i>disable</i>	Disable FortiPresence finding and reporting rogue APs.									
fortipresence-unassoc	Enable/disable FortiPresence finding and reporting unassociated stations.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiPresence finding and reporting unassociated stations.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiPresence finding and reporting unassociated stations.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiPresence finding and reporting unassociated stations.	<i>disable</i>	Disable FortiPresence finding and reporting unassociated stations.			
Option	Description									
<i>enable</i>	Enable FortiPresence finding and reporting unassociated stations.									
<i>disable</i>	Disable FortiPresence finding and reporting unassociated stations.									
fortipresence-ble	Enable/disable FortiPresence finding and reporting BLE devices.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiPresence finding and reporting BLE devices.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiPresence finding and reporting BLE devices.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable FortiPresence finding and reporting BLE devices.	<i>disable</i>	Disable FortiPresence finding and reporting BLE devices.			
Option	Description									
<i>enable</i>	Enable FortiPresence finding and reporting BLE devices.									
<i>disable</i>	Disable FortiPresence finding and reporting BLE devices.									
station-locate	Enable/disable client station locating services for all clients, whether associated or not .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable station locating service.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable station locating service.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable station locating service.	<i>disable</i>	Disable station locating service.			
Option	Description									
<i>enable</i>	Enable station locating service.									
<i>disable</i>	Disable station locating service.									

## config wireless-controller wtp

Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate.

```

config wireless-controller wtp
  Description: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be
    managed by FortiGate.
  edit <wtp-id>
    set index {integer}
    set uuid {uuid}
    set admin [discovered|disable|...]
    set name {string}
    set location {string}
    set region {string}
    set region-x {string}
    set region-y {string}
    set firmware-provision {string}
    set wtp-profile {string}
    set apcfg-profile {string}
  
```

```

set bonjour-profile {string}
set override-led-state [enable|disable]
set led-state [enable|disable]
set override-wan-port-mode [enable|disable]
set wan-port-mode [wan-lan|wan-only]
set override-ip-fragment [enable|disable]
set ip-fragment-preventing {option1}, {option2}, ...
set tun-mtu-uplink {integer}
set tun-mtu-downlink {integer}
set override-split-tunnel [enable|disable]
set split-tunneling-acl-path [tunnel|local]
set split-tunneling-acl-local-ap-subnet [enable|disable]
config split-tunneling-acl
    Description: Split tunneling ACL filter list.
    edit <id>
        set dest-ip {ipv4-classnet}
    next
end
set override-lan [enable|disable]
config lan
    Description: WTP LAN port mapping.
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
end
set override-allowaccess [enable|disable]
set allowaccess {option1}, {option2}, ...
set override-login-passwd-change [enable|disable]
set login-passwd-change [yes|default|...]
set login-passwd {password}
config radio-1
    Description: Configuration options for radio 1.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-level {integer}

```

```

    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-2
    Description: Configuration options for radio 2.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-level {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-3
    Description: Configuration options for radio 3.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-level {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-4
    Description: Configuration options for radio 4.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-level {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]

```

```

end
set image-download [enable|disable]
set mesh-bridge-enable [default|enable|...]
set coordinate-latitude {string}
set coordinate-longitude {string}
next
end

```

## config wireless-controller wtp

Parameter	Description	Type	Size	Default								
index	Index .	integer	Minimum value: 0 Maximum value: 4294967295	0								
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000								
admin	Configure how the FortiGate operating as a wireless controller discovers and manages this WTP, AP or FortiAP.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>discovered</i></td> <td>FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.</td> </tr> <tr> <td><i>disable</i></td> <td>FortiGate wireless controller is configured to not provide service to this WTP.</td> </tr> <tr> <td><i>enable</i></td> <td>FortiGate wireless controller is configured to provide service to this WTP.</td> </tr> </tbody> </table>	Option	Description	<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.	<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.	<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.			
Option	Description											
<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.											
<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.											
<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.											
name	WTP, AP or FortiAP configuration name.	string	Maximum length: 35									
location	Field for describing the physical location of the WTP, AP or FortiAP.	string	Maximum length: 35									
region	Region name WTP is associated with.	string	Maximum length: 35									
region-x	Relative horizontal region coordinate (between 0 and 1).	string	Maximum length: 15	0								
region-y	Relative vertical region coordinate (between 0 and 1).	string	Maximum length: 15	0								
firmware-provision	Firmware version to provision to this FortiAP on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
wtp-profile	WTP profile name to apply to this WTP, AP or FortiAP.	string	Maximum length: 35							
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35							
bonjour-profile	Bonjour profile name.	string	Maximum length: 35							
override-led-state	Enable to override the profile LED state setting for this FortiAP. You must enable this option to use the led-state command to turn off the FortiAP's LEDs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile LED state.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile LED state.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile LED state.	<i>disable</i>	Use the WTP profile LED state.			
Option	Description									
<i>enable</i>	Override the WTP profile LED state.									
<i>disable</i>	Use the WTP profile LED state.									
led-state	Enable to allow the FortiAPs LEDs to light. Disable to keep the LEDs off. You may want to keep the LEDs off so they are not distracting in low light areas etc.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Allow the LEDs on this FortiAP to light.</td> </tr> <tr> <td><i>disable</i></td> <td>Keep the LEDs on this FortiAP off.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Allow the LEDs on this FortiAP to light.	<i>disable</i>	Keep the LEDs on this FortiAP off.			
Option	Description									
<i>enable</i>	Allow the LEDs on this FortiAP to light.									
<i>disable</i>	Keep the LEDs on this FortiAP off.									
override-wan-port-mode	Enable/disable overriding the wan-port-mode in the WTP profile.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile wan-port-mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the wan-port-mode in the WTP profile.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile wan-port-mode.	<i>disable</i>	Use the wan-port-mode in the WTP profile.			
Option	Description									
<i>enable</i>	Override the WTP profile wan-port-mode.									
<i>disable</i>	Use the wan-port-mode in the WTP profile.									
wan-port-mode	Enable/disable using the FortiAP WAN port as a LAN port.	option	-	wan-only						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>wan-lan</i></td> <td>Use the FortiAP WAN port as a LAN port.</td> </tr> <tr> <td><i>wan-only</i></td> <td>Do not use the WAN port as a LAN port.</td> </tr> </tbody> </table>	Option	Description	<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.	<i>wan-only</i>	Do not use the WAN port as a LAN port.			
Option	Description									
<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.									
<i>wan-only</i>	Do not use the WAN port as a LAN port.									
override-ip-fragment	Enable/disable overriding the WTP profile IP fragment prevention setting.	option	-	disable						



Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile IP fragment prevention setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile IP fragment prevention setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile IP fragment prevention setting.	<i>disable</i>	Use the WTP profile IP fragment prevention setting.			
Option	Description									
<i>enable</i>	Override the WTP profile IP fragment prevention setting.									
<i>disable</i>	Use the WTP profile IP fragment prevention setting.									
ip-fragment-preventing	Method.	option	-	tcp-mss-adjust						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tcp-mss-adjust</i></td> <td>TCP maximum segment size adjustment.</td> </tr> <tr> <td><i>icmp-unreachable</i></td> <td>Drop packet and send ICMP Destination Unreachable</td> </tr> </tbody> </table>	Option	Description	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable			
Option	Description									
<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.									
<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable									
tun-mtu-uplink	The maximum transmission unit .	integer	Minimum value: 576 Maximum value: 1500	0						
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel .	integer	Minimum value: 576 Maximum value: 1500	0						
override-split-tunnel	Enable/disable overriding the WTP profile split tunneling setting.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile split tunneling setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile split tunneling setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile split tunneling setting.	<i>disable</i>	Use the WTP profile split tunneling setting.			
Option	Description									
<i>enable</i>	Override the WTP profile split tunneling setting.									
<i>disable</i>	Use the WTP profile split tunneling setting.									
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Split tunneling ACL list traffic will be tunnel.</td> </tr> <tr> <td><i>local</i></td> <td>Split tunneling ACL list traffic will be local NATed.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.	<i>local</i>	Split tunneling ACL list traffic will be local NATed.			
Option	Description									
<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.									
<i>local</i>	Split tunneling ACL list traffic will be local NATed.									
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL .	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.					
Option	Description											
<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.											
<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.											
override-lan	Enable to override the WTP profile LAN port setting.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile LAN port setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile LAN port setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile LAN port setting.	<i>disable</i>	Use the WTP profile LAN port setting.					
Option	Description											
<i>enable</i>	Override the WTP profile LAN port setting.											
<i>disable</i>	Use the WTP profile LAN port setting.											
override-allowaccess	Enable to override the WTP profile management access configuration.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile management access configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile management access configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile management access configuration.	<i>disable</i>	Use the WTP profile management access configuration.					
Option	Description											
<i>enable</i>	Override the WTP profile management access configuration.											
<i>disable</i>	Use the WTP profile management access configuration.											
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>https</i></td> <td>HTTPS access.</td> </tr> <tr> <td><i>ssh</i></td> <td>SSH access.</td> </tr> <tr> <td><i>snmp</i></td> <td>SNMP access.</td> </tr> </tbody> </table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description											
<i>https</i>	HTTPS access.											
<i>ssh</i>	SSH access.											
<i>snmp</i>	SNMP access.											
override-login-passwd-change	Enable to override the WTP profile login-password (administrator password) setting.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile login-password (administrator password) setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the the WTP profile login-password (administrator password) setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile login-password (administrator password) setting.	<i>disable</i>	Use the the WTP profile login-password (administrator password) setting.					
Option	Description											
<i>enable</i>	Override the WTP profile login-password (administrator password) setting.											
<i>disable</i>	Use the the WTP profile login-password (administrator password) setting.											
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP .	option	-	no								

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>yes</i></td> <td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td> </tr> <tr> <td><i>default</i></td> <td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td> </tr> <tr> <td><i>no</i></td> <td>Do not change the managed WTP, FortiAP or AP's administrator password.</td> </tr> </tbody> </table>	Option	Description	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.	<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.			
Option	Description											
<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.											
<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.											
<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.											
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified									
image-download	Enable/disable WTP image download.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WTP image download at join time.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WTP image download at join time.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WTP image download at join time.	<i>disable</i>	Disable WTP image download at join time.					
Option	Description											
<i>enable</i>	Enable WTP image download at join time.											
<i>disable</i>	Disable WTP image download at join time.											
mesh-bridge-enable	Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Use mesh Ethernet bridge local setting on the WTP.</td> </tr> <tr> <td><i>enable</i></td> <td>Turn on mesh Ethernet bridge on the WTP.</td> </tr> <tr> <td><i>disable</i></td> <td>Turn off mesh Ethernet bridge on the WTP.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Use mesh Ethernet bridge local setting on the WTP.	<i>enable</i>	Turn on mesh Ethernet bridge on the WTP.	<i>disable</i>	Turn off mesh Ethernet bridge on the WTP.			
Option	Description											
<i>default</i>	Use mesh Ethernet bridge local setting on the WTP.											
<i>enable</i>	Turn on mesh Ethernet bridge on the WTP.											
<i>disable</i>	Turn off mesh Ethernet bridge on the WTP.											
coordinate-latitude	WTP latitude coordinate.	string	Maximum length: 19									
coordinate-longitude	WTP longitude coordinate.	string	Maximum length: 19									

### config split-tunneling-acl

Parameter	Description	Type	Size	Default
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

### config lan

Parameter	Description	Type	Size	Default
port-mode	LAN port mode.	option	-	offline

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15											
port1-mode	LAN port 1 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15											
port2-mode	LAN port 2 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15											
port3-mode	LAN port 3 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													

Parameter	Description	Type	Size	Default										
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15											
port4-mode	LAN port 4 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15											
port5-mode	LAN port 5 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15											
port6-mode	LAN port 6 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15											
port7-mode	LAN port 7 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.							
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.							
Option	Description													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15											
port8-mode	LAN port 8 mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP LAN port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP LAN port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15											
port-esl-mode	ESL port mode.	option	-	offline										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>offline</i></td> <td>Offline.</td> </tr> <tr> <td><i>nat-to-wan</i></td> <td>NAT WTP ESL port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-wan</i></td> <td>Bridge WTP ESL port to WTP WAN port.</td> </tr> <tr> <td><i>bridge-to-ssid</i></td> <td>Bridge WTP ESL port to SSID.</td> </tr> </tbody> </table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.			
Option	Description													
<i>offline</i>	Offline.													
<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.													
<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.													
<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.													
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15											

### config radio-1

Parameter	Description	Type	Size	Default						
override-band	Enable to override the WTP profile band setting.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile band setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile band setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile band setting.	<i>disable</i>	Use the WTP profile band setting.			
Option	Description									
<i>enable</i>	Override the WTP profile band setting.									
<i>disable</i>	Use the WTP profile band setting.									
band	WiFi band that Radio 1 operates on.	option	-							

Parameter	Description	Type	Size	Default																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																																															
<i>802.11a</i>	802.11a.																																															
<i>802.11b</i>	802.11b.																																															
<i>802.11g</i>	802.11g/b.																																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																															
<i>802.11ac</i>	802.11ac/n/a.																																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																															
<i>802.11g-only</i>	802.11g.																																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																															
<i>802.11ac,n-only</i>	802.11ac/n.																																															
<i>802.11ac-only</i>	802.11ac.																																															
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																															
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																															
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																															
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																															
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																															
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																															
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile power level configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile power level configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.																																									
Option	Description																																															
<i>enable</i>	Override the WTP profile power level configuration.																																															
<i>disable</i>	Use the WTP profile power level configuration.																																															
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable																																												

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.					
Option	Description											
<i>enable</i>	Enable automatic transmit power adjustment.											
<i>disable</i>	Disable automatic transmit power adjustment.											
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17								
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10								
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70								
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100								
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile VAP settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile VAP settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile VAP settings.	<i>disable</i>	Use WTP profile VAP settings.					
Option	Description											
<i>enable</i>	Override WTP profile VAP settings.											
<i>disable</i>	Use WTP profile VAP settings.											
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
override-channel	Enable to override WTP profile channel settings.	option	-	disable								



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile channel settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile channel settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile channel settings.	<i>disable</i>	Use WTP profile channel settings.							
Option	Description													
<i>enable</i>	Override WTP profile channel settings.													
<i>disable</i>	Use WTP profile channel settings.													
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3											
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ap</i></td> <td>Set the radio to AP mode.</td> </tr> <tr> <td><i>monitor</i></td> <td>Set the radio to monitor mode</td> </tr> <tr> <td><i>ncf</i></td> <td>Select and set the radio mode based on NCF score.</td> </tr> <tr> <td><i>ncf-peek</i></td> <td>Select the radio mode based on NCF score, but do not apply.</td> </tr> </tbody> </table>	Option	Description	<i>ap</i>	Set the radio to AP mode.	<i>monitor</i>	Set the radio to monitor mode	<i>ncf</i>	Select and set the radio mode based on NCF score.	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.			
Option	Description													
<i>ap</i>	Set the radio to AP mode.													
<i>monitor</i>	Set the radio to monitor mode													
<i>ncf</i>	Select and set the radio mode based on NCF score.													
<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.													

## config radio-2

Parameter	Description	Type	Size	Default																				
override-band	Enable to override the WTP profile band setting.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile band setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile band setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile band setting.	<i>disable</i>	Use the WTP profile band setting.																	
Option	Description																							
<i>enable</i>	Override the WTP profile band setting.																							
<i>disable</i>	Use the WTP profile band setting.																							
band	WiFi band that Radio 2 operates on.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.			
Option	Description																							
<i>802.11a</i>	802.11a.																							
<i>802.11b</i>	802.11b.																							
<i>802.11g</i>	802.11g/b.																							
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																							
<i>802.11n-5G</i>	802.11n/a at 5GHz.																							
<i>802.11ac</i>	802.11ac/n/a.																							
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																							
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																							
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																							

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																													
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																													
<i>802.11g-only</i>	802.11g.																													
<i>802.11n-only</i>	802.11n at 2.4GHz.																													
<i>802.11n-5G-only</i>	802.11n at 5GHz.																													
<i>802.11ac,n-only</i>	802.11ac/n.																													
<i>802.11ac-only</i>	802.11ac.																													
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																													
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																													
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																													
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																													
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																													
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																													
override- txpower	Enable to override the WTP profile power level configuration.	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile power level configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile power level configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.																							
Option	Description																													
<i>enable</i>	Override the WTP profile power level configuration.																													
<i>disable</i>	Use the WTP profile power level configuration.																													
auto-power- level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.																							
Option	Description																													
<i>enable</i>	Enable automatic transmit power adjustment.																													
<i>disable</i>	Disable automatic transmit power adjustment.																													
auto-power- high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17																										

Parameter	Description	Type	Size	Default								
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10								
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70								
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100								
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile VAP settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile VAP settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile VAP settings.	<i>disable</i>	Use WTP profile VAP settings.					
Option	Description											
<i>enable</i>	Override WTP profile VAP settings.											
<i>disable</i>	Use WTP profile VAP settings.											
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
override-channel	Enable to override WTP profile channel settings.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile channel settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile channel settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile channel settings.	<i>disable</i>	Use WTP profile channel settings.					
Option	Description											
<i>enable</i>	Override WTP profile channel settings.											
<i>disable</i>	Use WTP profile channel settings.											
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf								

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ap</i></td> <td>Set the radio to AP mode.</td> </tr> <tr> <td><i>monitor</i></td> <td>Set the radio to monitor mode</td> </tr> <tr> <td><i>ncf</i></td> <td>Select and set the radio mode based on NCF score.</td> </tr> <tr> <td><i>ncf-peek</i></td> <td>Select the radio mode based on NCF score, but do not apply.</td> </tr> </tbody> </table>	Option	Description	<i>ap</i>	Set the radio to AP mode.	<i>monitor</i>	Set the radio to monitor mode	<i>ncf</i>	Select and set the radio mode based on NCF score.	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.			
Option	Description													
<i>ap</i>	Set the radio to AP mode.													
<i>monitor</i>	Set the radio to monitor mode													
<i>ncf</i>	Select and set the radio mode based on NCF score.													
<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.													

### config radio-3

Parameter	Description	Type	Size	Default																																
override-band	Enable to override the WTP profile band setting.	option	-	disable																																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile band setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile band setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile band setting.	<i>disable</i>	Use the WTP profile band setting.																													
Option	Description																																			
<i>enable</i>	Override the WTP profile band setting.																																			
<i>disable</i>	Use the WTP profile band setting.																																			
band	WiFi band that Radio 3 operates on.	option	-																																	
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.			
Option	Description																																			
<i>802.11a</i>	802.11a.																																			
<i>802.11b</i>	802.11b.																																			
<i>802.11g</i>	802.11g/b.																																			
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																			
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																			
<i>802.11ac</i>	802.11ac/n/a.																																			
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																			
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																			
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																			
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																			
<i>802.11g-only</i>	802.11g.																																			
<i>802.11n-only</i>	802.11n at 2.4GHz.																																			
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																			
<i>802.11ac,n-only</i>	802.11ac/n.																																			
<i>802.11ac-only</i>	802.11ac.																																			

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																	
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																	
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																	
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																	
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																	
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																	
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																	
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile power level configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile power level configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.											
Option	Description																	
<i>enable</i>	Override the WTP profile power level configuration.																	
<i>disable</i>	Use the WTP profile power level configuration.																	
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.											
Option	Description																	
<i>enable</i>	Enable automatic transmit power adjustment.																	
<i>disable</i>	Disable automatic transmit power adjustment.																	
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17														
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10														
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70														
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100														

Parameter	Description	Type	Size	Default										
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile VAP settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile VAP settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile VAP settings.	<i>disable</i>	Use WTP profile VAP settings.							
Option	Description													
<i>enable</i>	Override WTP profile VAP settings.													
<i>disable</i>	Use WTP profile VAP settings.													
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.					
Option	Description													
<i>tunnel</i>	Automatically select tunnel SSIDs.													
<i>bridge</i>	Automatically select local-bridging SSIDs.													
<i>manual</i>	Manually select SSIDs.													
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35											
override-channel	Enable to override WTP profile channel settings.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile channel settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile channel settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile channel settings.	<i>disable</i>	Use WTP profile channel settings.							
Option	Description													
<i>enable</i>	Override WTP profile channel settings.													
<i>disable</i>	Use WTP profile channel settings.													
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3											
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ap</i></td> <td>Set the radio to AP mode.</td> </tr> <tr> <td><i>monitor</i></td> <td>Set the radio to monitor mode</td> </tr> <tr> <td><i>ncf</i></td> <td>Select and set the radio mode based on NCF score.</td> </tr> <tr> <td><i>ncf-peek</i></td> <td>Select the radio mode based on NCF score, but do not apply.</td> </tr> </tbody> </table>	Option	Description	<i>ap</i>	Set the radio to AP mode.	<i>monitor</i>	Set the radio to monitor mode	<i>ncf</i>	Select and set the radio mode based on NCF score.	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.			
Option	Description													
<i>ap</i>	Set the radio to AP mode.													
<i>monitor</i>	Set the radio to monitor mode													
<i>ncf</i>	Select and set the radio mode based on NCF score.													
<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.													

## config radio-4

Parameter	Description	Type	Size	Default																																												
override-band	Enable to override the WTP profile band setting.	option	-	disable																																												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile band setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile band setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile band setting.	<i>disable</i>	Use the WTP profile band setting.																																									
Option	Description																																															
<i>enable</i>	Override the WTP profile band setting.																																															
<i>disable</i>	Use the WTP profile band setting.																																															
band	WiFi band that Radio 4 operates on.	option	-																																													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>802.11a</i></td> <td>802.11a.</td> </tr> <tr> <td><i>802.11b</i></td> <td>802.11b.</td> </tr> <tr> <td><i>802.11g</i></td> <td>802.11g/b.</td> </tr> <tr> <td><i>802.11n</i></td> <td>802.11n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G</i></td> <td>802.11n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ac</i></td> <td>802.11ac/n/a.</td> </tr> <tr> <td><i>802.11ax-5G</i></td> <td>802.11ax/ac/n/a at 5GHz.</td> </tr> <tr> <td><i>802.11ax</i></td> <td>802.11ax/n/g/b at 2.4GHz.</td> </tr> <tr> <td><i>802.11ac-2G</i></td> <td>802.11ac at 2.4GHz.</td> </tr> <tr> <td><i>802.11n,g-only</i></td> <td>802.11n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11g-only</i></td> <td>802.11g.</td> </tr> <tr> <td><i>802.11n-only</i></td> <td>802.11n at 2.4GHz.</td> </tr> <tr> <td><i>802.11n-5G-only</i></td> <td>802.11n at 5GHz.</td> </tr> <tr> <td><i>802.11ac,n-only</i></td> <td>802.11ac/n.</td> </tr> <tr> <td><i>802.11ac-only</i></td> <td>802.11ac.</td> </tr> <tr> <td><i>802.11ax,ac-only</i></td> <td>802.11ax/ac at 5GHz.</td> </tr> <tr> <td><i>802.11ax,ac,n-only</i></td> <td>802.11ax/ac/n at 5GHz.</td> </tr> <tr> <td><i>802.11ax-5G-only</i></td> <td>802.11ax at 5GHz.</td> </tr> <tr> <td><i>802.11ax,n-only</i></td> <td>802.11ax/n at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax,n,g-only</i></td> <td>802.11ax/n/g at 2.4GHz.</td> </tr> <tr> <td><i>802.11ax-only</i></td> <td>802.11ax at 2.4GHz.</td> </tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																																															
<i>802.11a</i>	802.11a.																																															
<i>802.11b</i>	802.11b.																																															
<i>802.11g</i>	802.11g/b.																																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																															
<i>802.11ac</i>	802.11ac/n/a.																																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																															
<i>802.11g-only</i>	802.11g.																																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																															
<i>802.11ac,n-only</i>	802.11ac/n.																																															
<i>802.11ac-only</i>	802.11ac.																																															
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																															
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																															
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																															
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																															
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																															
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																															
override- txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																												

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override the WTP profile power level configuration.</td> </tr> <tr> <td><i>disable</i></td> <td>Use the WTP profile power level configuration.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.			
Option	Description									
<i>enable</i>	Override the WTP profile power level configuration.									
<i>disable</i>	Use the WTP profile power level configuration.									
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable automatic transmit power adjustment.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable automatic transmit power adjustment.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17						
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10						
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70						
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100	100						
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile VAP settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile VAP settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile VAP settings.	<i>disable</i>	Use WTP profile VAP settings.			
Option	Description									
<i>enable</i>	Override WTP profile VAP settings.									
<i>disable</i>	Use WTP profile VAP settings.									
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>tunnel</i></td> <td>Automatically select tunnel SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.					
Option	Description									
<i>tunnel</i>	Automatically select tunnel SSIDs.									



Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>bridge</i></td> <td>Automatically select local-bridging SSIDs.</td> </tr> <tr> <td><i>manual</i></td> <td>Manually select SSIDs.</td> </tr> </tbody> </table>	Option	Description	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.							
Option	Description													
<i>bridge</i>	Automatically select local-bridging SSIDs.													
<i>manual</i>	Manually select SSIDs.													
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35											
override-channel	Enable to override WTP profile channel settings.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Override WTP profile channel settings.</td> </tr> <tr> <td><i>disable</i></td> <td>Use WTP profile channel settings.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Override WTP profile channel settings.	<i>disable</i>	Use WTP profile channel settings.							
Option	Description													
<i>enable</i>	Override WTP profile channel settings.													
<i>disable</i>	Use WTP profile channel settings.													
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3											
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ap</i></td> <td>Set the radio to AP mode.</td> </tr> <tr> <td><i>monitor</i></td> <td>Set the radio to monitor mode</td> </tr> <tr> <td><i>ncf</i></td> <td>Select and set the radio mode based on NCF score.</td> </tr> <tr> <td><i>ncf-peek</i></td> <td>Select the radio mode based on NCF score, but do not apply.</td> </tr> </tbody> </table>	Option	Description	<i>ap</i>	Set the radio to AP mode.	<i>monitor</i>	Set the radio to monitor mode	<i>ncf</i>	Select and set the radio mode based on NCF score.	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.			
Option	Description													
<i>ap</i>	Set the radio to AP mode.													
<i>monitor</i>	Set the radio to monitor mode													
<i>ncf</i>	Select and set the radio mode based on NCF score.													
<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.													

## config wireless-controller wtp-group

Configure WTP groups.

```
config wireless-controller wtp-group
  Description: Configure WTP groups.
  edit <name>
    set platform-type [AP-11N|220B|...]
    set wtps <wtp-id1>, <wtp-id2>, ...
  next
end
```

## config wireless-controller wtp-group

Parameter	Description	Type	Size	Default																																																								
platform-type	FortiAP models to define the WTP group platform type.	option	-																																																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>AP-11N</i></td> <td>Default 11n AP.</td> </tr> <tr> <td><i>220B</i></td> <td>FAP220B/221B.</td> </tr> <tr> <td><i>210B</i></td> <td>FAP210B.</td> </tr> <tr> <td><i>222B</i></td> <td>FAP222B.</td> </tr> <tr> <td><i>112B</i></td> <td>FAP112B.</td> </tr> <tr> <td><i>320B</i></td> <td>FAP320B.</td> </tr> <tr> <td><i>11C</i></td> <td>FAP11C.</td> </tr> <tr> <td><i>14C</i></td> <td>FAP14C.</td> </tr> <tr> <td><i>223B</i></td> <td>FAP223B.</td> </tr> <tr> <td><i>28C</i></td> <td>FAP28C.</td> </tr> <tr> <td><i>320C</i></td> <td>FAP320C.</td> </tr> <tr> <td><i>221C</i></td> <td>FAP221C.</td> </tr> <tr> <td><i>25D</i></td> <td>FAP25D.</td> </tr> <tr> <td><i>222C</i></td> <td>FAP222C.</td> </tr> <tr> <td><i>224D</i></td> <td>FAP224D.</td> </tr> <tr> <td><i>214B</i></td> <td>FK214B.</td> </tr> <tr> <td><i>21D</i></td> <td>FAP21D.</td> </tr> <tr> <td><i>24D</i></td> <td>FAP24D.</td> </tr> <tr> <td><i>112D</i></td> <td>FAP112D.</td> </tr> <tr> <td><i>223C</i></td> <td>FAP223C.</td> </tr> <tr> <td><i>321C</i></td> <td>FAP321C.</td> </tr> <tr> <td><i>C220C</i></td> <td>FAPC220C.</td> </tr> <tr> <td><i>C225C</i></td> <td>FAPC225C.</td> </tr> <tr> <td><i>C23JD</i></td> <td>FAPC23JD.</td> </tr> <tr> <td><i>C24JE</i></td> <td>FAPC24JE.</td> </tr> <tr> <td><i>S321C</i></td> <td>FAPS321C.</td> </tr> <tr> <td><i>S322C</i></td> <td>FAPS322C.</td> </tr> </tbody> </table>	Option	Description	<i>AP-11N</i>	Default 11n AP.	<i>220B</i>	FAP220B/221B.	<i>210B</i>	FAP210B.	<i>222B</i>	FAP222B.	<i>112B</i>	FAP112B.	<i>320B</i>	FAP320B.	<i>11C</i>	FAP11C.	<i>14C</i>	FAP14C.	<i>223B</i>	FAP223B.	<i>28C</i>	FAP28C.	<i>320C</i>	FAP320C.	<i>221C</i>	FAP221C.	<i>25D</i>	FAP25D.	<i>222C</i>	FAP222C.	<i>224D</i>	FAP224D.	<i>214B</i>	FK214B.	<i>21D</i>	FAP21D.	<i>24D</i>	FAP24D.	<i>112D</i>	FAP112D.	<i>223C</i>	FAP223C.	<i>321C</i>	FAP321C.	<i>C220C</i>	FAPC220C.	<i>C225C</i>	FAPC225C.	<i>C23JD</i>	FAPC23JD.	<i>C24JE</i>	FAPC24JE.	<i>S321C</i>	FAPS321C.	<i>S322C</i>	FAPS322C.			
Option	Description																																																											
<i>AP-11N</i>	Default 11n AP.																																																											
<i>220B</i>	FAP220B/221B.																																																											
<i>210B</i>	FAP210B.																																																											
<i>222B</i>	FAP222B.																																																											
<i>112B</i>	FAP112B.																																																											
<i>320B</i>	FAP320B.																																																											
<i>11C</i>	FAP11C.																																																											
<i>14C</i>	FAP14C.																																																											
<i>223B</i>	FAP223B.																																																											
<i>28C</i>	FAP28C.																																																											
<i>320C</i>	FAP320C.																																																											
<i>221C</i>	FAP221C.																																																											
<i>25D</i>	FAP25D.																																																											
<i>222C</i>	FAP222C.																																																											
<i>224D</i>	FAP224D.																																																											
<i>214B</i>	FK214B.																																																											
<i>21D</i>	FAP21D.																																																											
<i>24D</i>	FAP24D.																																																											
<i>112D</i>	FAP112D.																																																											
<i>223C</i>	FAP223C.																																																											
<i>321C</i>	FAP321C.																																																											
<i>C220C</i>	FAPC220C.																																																											
<i>C225C</i>	FAPC225C.																																																											
<i>C23JD</i>	FAPC23JD.																																																											
<i>C24JE</i>	FAPC24JE.																																																											
<i>S321C</i>	FAPS321C.																																																											
<i>S322C</i>	FAPS322C.																																																											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>S323C</i>	FAPS323C.		
	<i>S311C</i>	FAPS311C.		
	<i>S313C</i>	FAPS313C.		
	<i>S321CR</i>	FAPS321CR.		
	<i>S322CR</i>	FAPS322CR.		
	<i>S323CR</i>	FAPS323CR.		
	<i>S421E</i>	FAPS421E.		
	<i>S422E</i>	FAPS422E.		
	<i>S423E</i>	FAPS423E.		
	<i>421E</i>	FAP421E.		
	<i>423E</i>	FAP423E.		
	<i>221E</i>	FAP221E.		
	<i>222E</i>	FAP222E.		
	<i>223E</i>	FAP223E.		
	<i>224E</i>	FAP224E.		
	<i>231E</i>	FAP231E.		
	<i>S221E</i>	FAPS221E.		
	<i>S223E</i>	FAPS223E.		
	<i>321E</i>	FAP321E.		
	<i>431F</i>	FAP431F.		
	<i>432F</i>	FAP432F.		
	<i>433F</i>	FAP433F.		
	<i>231F</i>	FAP231F.		
	<i>234F</i>	FAP234F.		
	<i>23JF</i>	FAP23JF.		
	<i>831F</i>	FAP831F.		
	<i>U421E</i>	FAPU421EV.		
	<i>U422EV</i>	FAPU422EV.		
	<i>U423E</i>	FAPU423EV.		

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>U221EV</i></td> <td>FAPU221EV.</td> </tr> <tr> <td><i>U223EV</i></td> <td>FAPU223EV.</td> </tr> <tr> <td><i>U24JEV</i></td> <td>FAPU24JEV.</td> </tr> <tr> <td><i>U321EV</i></td> <td>FAPU321EV.</td> </tr> <tr> <td><i>U323EV</i></td> <td>FAPU323EV.</td> </tr> <tr> <td><i>U431F</i></td> <td>FAPU431F.</td> </tr> <tr> <td><i>U433F</i></td> <td>FAPU433F.</td> </tr> <tr> <td><i>U231F</i></td> <td>FAPU231F.</td> </tr> <tr> <td><i>U234F</i></td> <td>FAPU234F.</td> </tr> <tr> <td><i>U432F</i></td> <td>FAPU432F.</td> </tr> </tbody> </table>	Option	Description	<i>U221EV</i>	FAPU221EV.	<i>U223EV</i>	FAPU223EV.	<i>U24JEV</i>	FAPU24JEV.	<i>U321EV</i>	FAPU321EV.	<i>U323EV</i>	FAPU323EV.	<i>U431F</i>	FAPU431F.	<i>U433F</i>	FAPU433F.	<i>U231F</i>	FAPU231F.	<i>U234F</i>	FAPU234F.	<i>U432F</i>	FAPU432F.			
Option	Description																									
<i>U221EV</i>	FAPU221EV.																									
<i>U223EV</i>	FAPU223EV.																									
<i>U24JEV</i>	FAPU24JEV.																									
<i>U321EV</i>	FAPU321EV.																									
<i>U323EV</i>	FAPU323EV.																									
<i>U431F</i>	FAPU431F.																									
<i>U433F</i>	FAPU433F.																									
<i>U231F</i>	FAPU231F.																									
<i>U234F</i>	FAPU234F.																									
<i>U432F</i>	FAPU432F.																									
<code>wtps &lt;wtp-id&gt;</code>	WTP list. WTP ID.	string	Maximum length: 35																							

## config wireless-controller qos-profile

Configure WiFi quality of service (QoS) profiles.

```

config wireless-controller qos-profile
  Description: Configure WiFi quality of service (QoS) profiles.
  edit <name>
    set comment {string}
    set uplink {integer}
    set downlink {integer}
    set uplink-sta {integer}
    set downlink-sta {integer}
    set burst [enable|disable]
    set wmm [enable|disable]
    set wmm-uapsd [enable|disable]
    set call-admission-control [enable|disable]
    set call-capacity {integer}
    set bandwidth-admission-control [enable|disable]
    set bandwidth-capacity {integer}
    set dscp-wmm-mapping [enable|disable]
    set dscp-wmm-vo <id1>, <id2>, ...
    set dscp-wmm-vi <id1>, <id2>, ...
    set dscp-wmm-be <id1>, <id2>, ...
    set dscp-wmm-bk <id1>, <id2>, ...
    set wmm-dscp-marking [enable|disable]
    set wmm-vo-dscp {integer}
    set wmm-vi-dscp {integer}
    set wmm-be-dscp {integer}
    set wmm-bk-dscp {integer}
  next

```

end

## config wireless-controller qos-profile

Parameter	Description	Type	Size	Default						
comment	Comment.	string	Maximum length: 63							
uplink	Maximum uplink bandwidth for Virtual Access Points .	integer	Minimum value: 0 Maximum value: 2097152	0						
downlink	Maximum downlink bandwidth for Virtual Access Points .	integer	Minimum value: 0 Maximum value: 2097152	0						
uplink-sta	Maximum uplink bandwidth for clients .	integer	Minimum value: 0 Maximum value: 2097152	0						
downlink-sta	Maximum downlink bandwidth for clients .	integer	Minimum value: 0 Maximum value: 2097152	0						
burst	Enable/disable client rate burst.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable client rate burst.</td></tr><tr><td><i>disable</i></td><td>Disable client rate burst.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable client rate burst.	<i>disable</i>	Disable client rate burst.			
Option	Description									
<i>enable</i>	Enable client rate burst.									
<i>disable</i>	Disable client rate burst.									
wmm	Enable/disable WiFi multi-media (WMM) control.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable WiFi multi-media (WMM) control.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi multi-media (WMM) control.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable WiFi multi-media (WMM) control.	<i>disable</i>	Disable WiFi multi-media (WMM) control.			
Option	Description									
<i>enable</i>	Enable WiFi multi-media (WMM) control.									
<i>disable</i>	Disable WiFi multi-media (WMM) control.									
wmm-uapsd	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.			
Option	Description									
<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.									
<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.									
call-admission-control	Enable/disable WMM call admission control.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM call admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM call admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10						
bandwidth-admission-control	Enable/disable WMM bandwidth admission control.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM bandwidth admission control.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM bandwidth admission control.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000						
dscp-wmm-mapping	Enable/disable Differentiated Services Code Point (DSCP) mapping.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable Differentiated Services Code Point (DSCP) mapping.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable Differentiated Services Code Point (DSCP) mapping.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable Differentiated Services Code Point (DSCP) mapping.	<i>disable</i>	Disable Differentiated Services Code Point (DSCP) mapping.			
Option	Description									
<i>enable</i>	Enable Differentiated Services Code Point (DSCP) mapping.									
<i>disable</i>	Disable Differentiated Services Code Point (DSCP) mapping.									
dscp-wmm-vo <id>	DSCP mapping for voice access (default = 48 56). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							

Parameter	Description	Type	Size	Default						
dscp-wmm-vi <id>	DSCP mapping for video access (default = 32 40). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-be <id>	DSCP mapping for best effort access (default = 0 24). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-bk <id>	DSCP mapping for background access (default = 8 16). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
wmm-dscp- marking	Enable/disable WMM Differentiated Services Code Point (DSCP) marking.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable WMM Differentiated Services Code Point (DSCP) marking.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable WMM Differentiated Services Code Point (DSCP) marking.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable WMM Differentiated Services Code Point (DSCP) marking.	<i>disable</i>	Disable WMM Differentiated Services Code Point (DSCP) marking.			
Option	Description									
<i>enable</i>	Enable WMM Differentiated Services Code Point (DSCP) marking.									
<i>disable</i>	Disable WMM Differentiated Services Code Point (DSCP) marking.									
wmm-vo-dscp	DSCP marking for voice access .	integer	Minimum value: 0 Maximum value: 63	48						
wmm-vi-dscp	DSCP marking for video access .	integer	Minimum value: 0 Maximum value: 63	32						
wmm-be-dscp	DSCP marking for best effort access .	integer	Minimum value: 0 Maximum value: 63	0						
wmm-bk-dscp	DSCP marking for background access .	integer	Minimum value: 0 Maximum value: 63	8						

## config wireless-controller wag-profile

Configure wireless access gateway (WAG) profiles used for tunnels on AP.

```
config wireless-controller wag-profile
  Description: Configure wireless access gateway (WAG) profiles used for tunnels on AP.
  edit <name>
    set comment {var-string}
```

```

set tunnel-type [l2tpv3|gre]
set wag-ip {ipv4-address}
set wag-port {integer}
set ping-interval {integer}
set ping-number {integer}
set return-packet-timeout {integer}
set dhcp-ip-addr {ipv4-address}
next
end

```

## config wireless-controller wag-profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
tunnel-type	Tunnel type.	option	-	l2tpv3						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>l2tpv3</i></td> <td>L2TPV3 Ethernet Pseudowire.</td> </tr> <tr> <td><i>gre</i></td> <td>GRE Ethernet tunnel.</td> </tr> </tbody> </table>	Option	Description	<i>l2tpv3</i>	L2TPV3 Ethernet Pseudowire.	<i>gre</i>	GRE Ethernet tunnel.			
Option	Description									
<i>l2tpv3</i>	L2TPV3 Ethernet Pseudowire.									
<i>gre</i>	GRE Ethernet tunnel.									
wag-ip	IP Address of the wireless access gateway.	ipv4-address	Not Specified	0.0.0.0						
wag-port	UDP port of the wireless access gateway.	integer	Minimum value: 0 Maximum value: 65535	1701						
ping-interval	Interval between two tunnel monitoring echo packets .	integer	Minimum value: 1 Maximum value: 65535	1						
ping-number	Number of the tunnel mointoring echo packets .	integer	Minimum value: 1 Maximum value: 65535	5						
return-packet-timeout	Window of time for the return packets from the tunnel's remote end .	integer	Minimum value: 1 Maximum value: 65535	160						
dhcp-ip-addr	IP address of the monitoring DHCP request packet sent through the tunnel	ipv4-address	Not Specified	0.0.0.0						



## config wireless-controller utm-profile

Configure UTM (Unified Threat Management) profile.

```
config wireless-controller utm-profile
  Description: Configure UTM (Unified Threat Management) profile.
  edit <name>
    set comment {string}
    set utm-log [enable|disable]
    set ips-sensor {string}
    set application-list {string}
    set antivirus-profile {string}
    set webfilter-profile {string}
    set scan-botnet-connections [disable|monitor|...]
  next
end
```

## config wireless-controller utm-profile

Parameter	Description	Type	Size	Default								
comment	Comment.	string	Maximum length: 63									
utm-log	Enable/disable UTM logging.	option	-	enable								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>enable</i></td><td>Enable UTM logging.</td></tr><tr><td><i>disable</i></td><td>Disable UTM logging.</td></tr></tbody></table>	Option	Description	<i>enable</i>	Enable UTM logging.	<i>disable</i>	Disable UTM logging.					
Option	Description											
<i>enable</i>	Enable UTM logging.											
<i>disable</i>	Disable UTM logging.											
ips-sensor	IPS sensor name.	string	Maximum length: 35									
application-list	Application control list name.	string	Maximum length: 35									
antivirus-profile	AntiVirus profile name.	string	Maximum length: 35									
webfilter-profile	WebFilter profile name.	string	Maximum length: 35									
scan-botnet-connections	Block or monitor connections to Botnet servers or disable Botnet scanning.	option	-	monitor								
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>disable</i></td><td>Do not scan connections to botnet servers.</td></tr><tr><td><i>monitor</i></td><td>Log connections to botnet servers.</td></tr><tr><td><i>block</i></td><td>Block connections to botnet servers.</td></tr></tbody></table>	Option	Description	<i>disable</i>	Do not scan connections to botnet servers.	<i>monitor</i>	Log connections to botnet servers.	<i>block</i>	Block connections to botnet servers.			
Option	Description											
<i>disable</i>	Do not scan connections to botnet servers.											
<i>monitor</i>	Log connections to botnet servers.											
<i>block</i>	Block connections to botnet servers.											

## config wireless-controller address

Configure the client with its MAC address.

```
config wireless-controller address
  Description: Configure the client with its MAC address.
  edit <id>
    set mac {mac-address}
    set policy [allow|deny]
  next
end
```

## config wireless-controller address

Parameter	Description	Type	Size	Default						
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00						
policy	Allow or block the client with this MAC address.	option	-	deny						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>allow</i></td><td>Allow the client with this MAC address.</td></tr><tr><td><i>deny</i></td><td>Block the client with this MAC address.</td></tr></tbody></table>	Option	Description	<i>allow</i>	Allow the client with this MAC address.	<i>deny</i>	Block the client with this MAC address.			
Option	Description									
<i>allow</i>	Allow the client with this MAC address.									
<i>deny</i>	Block the client with this MAC address.									

## config wireless-controller addrgrp

Configure the MAC address group.

```
config wireless-controller addrgrp
  Description: Configure the MAC address group.
  edit <id>
    set default-policy [allow|deny]
    set addresses <id1>, <id2>, ...
  next
end
```

## config wireless-controller addrgrp

Parameter	Description	Type	Size	Default						
default-policy	Allow or block the clients with MAC addresses that are not in the group.	option	-	allow						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>allow</i></td><td>Allow the clients with MAC addresses that are not in the group.</td></tr><tr><td><i>deny</i></td><td>Block the clients with MAC addresses that are not in the group.</td></tr></tbody></table>	Option	Description	<i>allow</i>	Allow the clients with MAC addresses that are not in the group.	<i>deny</i>	Block the clients with MAC addresses that are not in the group.			
Option	Description									
<i>allow</i>	Allow the clients with MAC addresses that are not in the group.									
<i>deny</i>	Block the clients with MAC addresses that are not in the group.									

Parameter	Description	Type	Size	Default
addresses <id>	Manually selected group of addresses. Address ID.	string	Maximum length: 35	

## config wireless-controller snmp

Configure SNMP.

```

config wireless-controller snmp
  Description: Configure SNMP.
  set engine-id {string}
  set contact-info {string}
  set trap-high-cpu-threshold {integer}
  set trap-high-mem-threshold {integer}
  config community
    Description: SNMP Community Configuration.
    edit <id>
      set name {string}
      set status [enable|disable]
      set query-v1-status [enable|disable]
      set query-v2c-status [enable|disable]
      set trap-v1-status [enable|disable]
      set trap-v2c-status [enable|disable]
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ip {user}
      next
    end
  next
end
config user
  Description: SNMP User Configuration.
  edit <name>
    set status [enable|disable]
    set queries [enable|disable]
    set trap-status [enable|disable]
    set security-level [no-auth-no-priv|auth-no-priv|...]
    set auth-proto [md5|sha]
    set auth-pwd {password}
    set priv-proto [aes|des|...]
    set priv-pwd {password}
    set notify-hosts {ipv4-address}
  next
end
end

```

## config wireless-controller snmp

Parameter	Description	Type	Size	Default
engine-id	AC SNMP engineid string (maximum 24 characters).	string	Maximum length: 23	
contact-info	Contact Information.	string	Maximum length: 31	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80
trap-high-mem-threshold	Memory usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80

## config community

Parameter	Description	Type	Size	Default						
name	Community name.	string	Maximum length: 35							
status	Enable/disable this SNMP community.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

### config hosts

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

### config user

Parameter	Description	Type	Size	Default						
status	SNMP User Enable	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
queries	Enable/disable SNMP queries for this user.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-status	Enable/disable traps for this SNMP user.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable setting.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable setting.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default										
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-auth-no-priv</i></td> <td>Message with no authentication and no privacy (encryption).</td> </tr> <tr> <td><i>auth-no-priv</i></td> <td>Message with authentication but no privacy (encryption).</td> </tr> <tr> <td><i>auth-priv</i></td> <td>Message with authentication and privacy (encryption).</td> </tr> </tbody> </table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).					
Option	Description													
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).													
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).													
<i>auth-priv</i>	Message with authentication and privacy (encryption).													
auth-proto	Authentication protocol.	option	-	sha										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>md5</i></td> <td>HMAC-MD5-96 authentication protocol.</td> </tr> <tr> <td><i>sha</i></td> <td>HMAC-SHA-96 authentication protocol.</td> </tr> </tbody> </table>	Option	Description	<i>md5</i>	HMAC-MD5-96 authentication protocol.	<i>sha</i>	HMAC-SHA-96 authentication protocol.							
Option	Description													
<i>md5</i>	HMAC-MD5-96 authentication protocol.													
<i>sha</i>	HMAC-SHA-96 authentication protocol.													
auth-pwd	Password for authentication protocol.	password	Not Specified											
priv-proto	Privacy (encryption) protocol.	option	-	aes										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>aes</i></td> <td>CFB128-AES-128 symmetric encryption protocol.</td> </tr> <tr> <td><i>des</i></td> <td>CBC-DES symmetric encryption protocol.</td> </tr> <tr> <td><i>aes256</i></td> <td>CFB128-AES-256 symmetric encryption protocol.</td> </tr> <tr> <td><i>aes256cisco</i></td> <td>CFB128-AES-256 symmetric encryption protocol compatible with CISCO.</td> </tr> </tbody> </table>	Option	Description	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	<i>des</i>	CBC-DES symmetric encryption protocol.	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.			
Option	Description													
<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.													
<i>des</i>	CBC-DES symmetric encryption protocol.													
<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.													
<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.													
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified											
notify-hosts	Configure SNMP User Notify Hosts.	ipv4-address	Not Specified											

## config wireless-controller mpsk-profile

Configure MPSK profile.

```

config wireless-controller mpsk-profile
  Description: Configure MPSK profile.
  edit <name>
    set mpsk-concurrent-clients {integer}
    config mpsk-group
      Description: List of multiple PSK groups.
      edit <name>
        set vlan-type [no-vlan|fixed-vlan]
        set vlan-id {integer}
      config mpsk-key
        Description: List of multiple PSK entries.
  
```

```

edit <name>
  set mac {mac-address}
  set passphrase {password}
  set concurrent-client-limit-type [default|unlimited|...]
  set concurrent-clients {integer}
  set comment {var-string}
  set mpsk-schedules <name1>, <name2>, ...
next
end
next
end
next
end
end

```

## config wireless-controller mpsk-profile

Parameter	Description	Type	Size	Default
mpsk-concurrent-clients	Maximum number of concurrent clients that connect using the same passphrase in multiple PSK authentication .	integer	Minimum value: 0 Maximum value: 65535	0

## config mpsk-group

Parameter	Description	Type	Size	Default						
vlan-type	MPSK group VLAN options.	option	-	no-vlan						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>no-vlan</i></td> <td>No VLAN.</td> </tr> <tr> <td><i>fixed-vlan</i></td> <td>Fixed VLAN ID.</td> </tr> </tbody> </table>	Option	Description	<i>no-vlan</i>	No VLAN.	<i>fixed-vlan</i>	Fixed VLAN ID.			
Option	Description									
<i>no-vlan</i>	No VLAN.									
<i>fixed-vlan</i>	Fixed VLAN ID.									
vlan-id	Optional VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0						

## config mpsk-key

Parameter	Description	Type	Size	Default
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
passphrase	WPA Pre-shared key.	password	Not Specified	

Parameter	Description	Type	Size	Default								
concurrent-client-limit-type	MPSK client limit type options.	option	-	default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>default</i></td> <td>Using the value in profile configuration.</td> </tr> <tr> <td><i>unlimited</i></td> <td>Unlimited.</td> </tr> <tr> <td><i>specified</i></td> <td>Specified value.</td> </tr> </tbody> </table>	Option	Description	<i>default</i>	Using the value in profile configuration.	<i>unlimited</i>	Unlimited.	<i>specified</i>	Specified value.			
Option	Description											
<i>default</i>	Using the value in profile configuration.											
<i>unlimited</i>	Unlimited.											
<i>specified</i>	Specified value.											
concurrent-clients	Number of clients that can connect using this pre-shared key .	integer	Minimum value: 1 Maximum value: 65535	256								
comment	Comment.	var-string	Maximum length: 255									
mpsk-schedules <name>	Firewall schedule for MPSK passphrase. The passphrase will be effective only when at least one schedule is valid. Schedule name.	string	Maximum length: 35									

## config wireless-controller access-control-list

Configure WiFi bridge access control list.

```

config wireless-controller access-control-list
  Description: Configure WiFi bridge access control list.
  edit <name>
    set comment {string}
    config layer3-ipv4-rules
      Description: AP ACL layer3 ipv4 rule list.
      edit <rule-id>
        set comment {string}
        set srcaddr {user}
        set srcport {integer}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set action [allow|deny]
      next
    end
    config layer3-ipv6-rules
      Description: AP ACL layer3 ipv6 rule list.
      edit <rule-id>
        set comment {string}
        set srcaddr {user}
        set srcport {integer}
        set dstaddr {user}

```



```

        set dstport {integer}
        set protocol {integer}
        set action [allow|deny]
    next
end
next
end

```

## config wireless-controller access-control-list

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	

## config layer3-ipv4-rules

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	
srcaddr	Source IP address .	user	Not Specified	
srcport	Source port .	integer	Minimum value: 0 Maximum value: 65535	0
dstaddr	Destination IP address .	user	Not Specified	
dstport	Destination port .	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	255
action	Policy action (allow   deny).	option	-	

Option	Description
<i>allow</i>	Allows traffic matching the policy.
<i>deny</i>	Blocks traffic matching the policy.

## config layer3-ipv6-rules

Parameter	Description	Type	Size	Default						
comment	Description.	string	Maximum length: 63							
srcaddr	Source IPv6 address (any   local-LAN   IPv6 address [/prefix length]), default = any.	user	Not Specified							
srcport	Source port .	integer	Minimum value: 0 Maximum value: 65535	0						
dstaddr	Destination IPv6 address (any   local-LAN   IPv6 address[/prefix length]), default = any.	user	Not Specified							
dstport	Destination port .	integer	Minimum value: 0 Maximum value: 65535	0						
protocol	Protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	255						
action	Policy action (allow   deny).	option	-							
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>allow</i></td><td>Allows traffic matching the policy.</td></tr><tr><td><i>deny</i></td><td>Blocks traffic matching the policy.</td></tr></tbody></table>	Option	Description	<i>allow</i>	Allows traffic matching the policy.	<i>deny</i>	Blocks traffic matching the policy.			
Option	Description									
<i>allow</i>	Allows traffic matching the policy.									
<i>deny</i>	Blocks traffic matching the policy.									

## config wireless-controller scan

Wireless controller scan result.

```
config wireless-controller scan
  Description: Wireless controller scan result.
end
```

## config wireless-controller ap-status

Configure access point status (rogue | accepted | suppressed).

```
config wireless-controller ap-status
  Description: Configure access point status (rogue | accepted | suppressed) .
  edit <id>
    set bssid {mac-address}
```

```

    set ssid {string}
    set status [rogue|accepted|...]
  next
end

```

## config wireless-controller ap-status

Parameter	Description	Type	Size	Default
bssid	Access Point's (AP's) BSSID.	mac-address	Not Specified	00:00:00:00:00:00
ssid	Access Point's (AP's) SSID.	string	Maximum length: 32	
status	Access Point's (AP's) status: rogue, accepted, or suppressed.	option	-	rogue
	<b>Option</b>	<b>Description</b>		
	<i>rogue</i>	Rogue AP.		
	<i>accepted</i>	Accepted AP.		
	<i>suppressed</i>	Suppressed AP.		

## config wireless-controller wlchanlistlic

Get channel list according to the region code.

```

config wireless-controller wlchanlistlic
  Description: Get channel list according to the region code.
end

```

## config wireless-controller status

Wireless controller status.

```

config wireless-controller status
  Description: Wireless controller status.
  set [1|2] {string}
end

```

## config wireless-controller status

Parameter	Description	Type	Size	Default
[1 2]	verbose	string	Maximum length: -1	

---

## config wireless-controller wtp-status

Wireless controller WTP-status.

```
config wireless-controller wtp-status
  Description: Wireless controller WTP-status.
  set <wtp-id> {string}
end
```

## config wireless-controller wtp-status

Parameter	Description	Type	Size	Default
<wtp-id>	WTP ID.	string	Maximum length: -1	

## config wireless-controller client-info

Wireless controller client-info.

```
config wireless-controller client-info
  Description: Wireless controller client-info.
  set <vfid> {string}
end
```

## config wireless-controller client-info

Parameter	Description	Type	Size	Default
<vfid>	VFID.	string	Maximum length: -1	

## config wireless-controller vap-status

Wireless controller VAP-status.

```
config wireless-controller vap-status
  Description: Wireless controller VAP-status.
  set [1] {string}
end
```

## config wireless-controller vap-status

Parameter	Description	Type	Size	Default
[1]	verbose	string	Maximum length: -1	

---

## config wireless-controller rf-analysis

Wireless controller rf-analysis.

```
config wireless-controller rf-analysis
  Description: Wireless controller rf-analysis.
  set <wtp-id> {string}
end
```

## config wireless-controller rf-analysis

Parameter	Description	Type	Size	Default
<wtp-id>	WTP ID.	string	Maximum length: -1	

## config wireless-controller spectral-info

Wireless controller spectrum analysis.

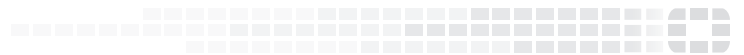
```
config wireless-controller spectral-info
  Description: Wireless controller spectrum analysis.
  set [wtp-id] {string}
end
```

## config wireless-controller spectral-info

Parameter	Description	Type	Size	Default
[wtp-id]	WTP ID.	string	Maximum length: -1	



**FORTINET®**



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.