Cisco Firepower 4100/9300 FXOS Command Reference

First Published: 2021-12-01

Last Modified: 2022-11-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

About the FXOS CLI Command Reference Guide

This guide represents an on-going effort to document the many CLI commands in FXOS, and as such, should be viewed as a work-in-progress. The guide will be republished periodically as new command descriptions are added and existing descriptions updated or corrected.

CLI Overview

Managed Objects

The FXOS uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, chassis, security modules, network modules, ports, and processors are physical entities represented as managed objects, and licenses, user roles, and platform policies are logical entities represented as managed objects.

Managed objects may have one or more associated properties that can be configured.

Command Modes

The CLI is organized into a hierarchy of command modes, with EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use **create**, **enter**, and **scope** commands to move from higher-level modes to modes in the next lower level, and you use the **up** command to move up one level in the mode hierarchy. You can also use the **top** command to move to the top level in the mode hierarchy.

Note Most command modes are associated with managed objects, so you must create an object before you can access the mode associated with that object. You use **create** and **enter** commands to create managed objects for the modes being accessed. The **scope** commands do not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy, and it can be an invaluable tool when you need to navigate through the hierarchy.

The following table lists the main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Table 1: Main Command Modes and Prompts

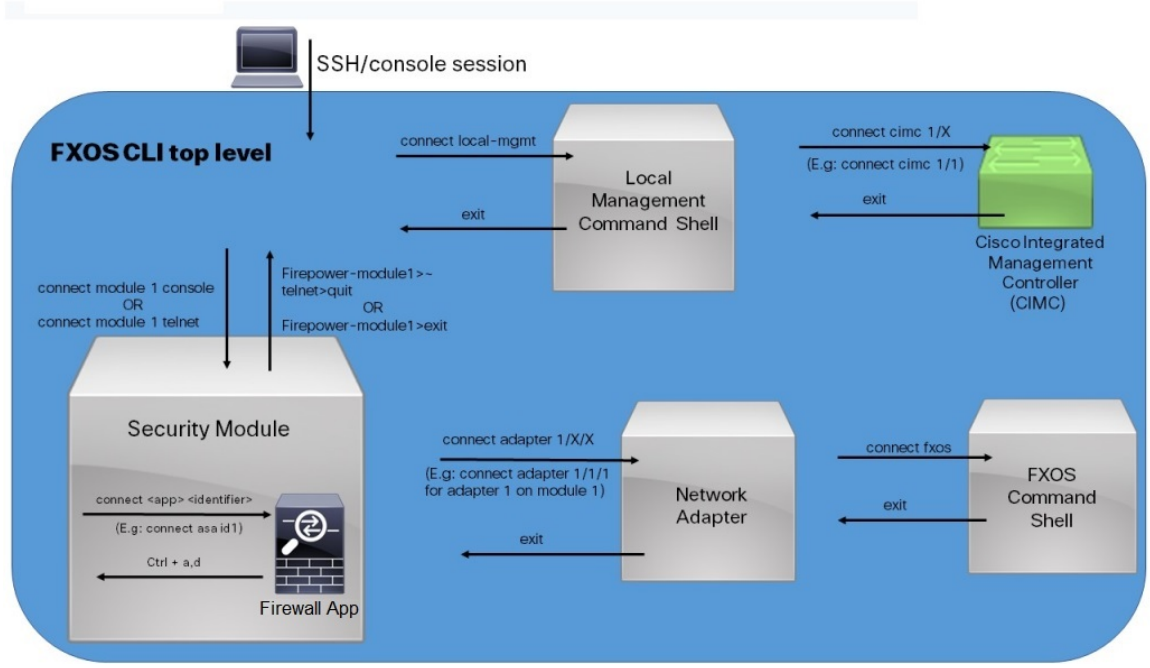
Mode Name	Commands Used to Access	Mode Prompt
EXEC	**top** command from any mode	`#`
Adapter	**scope adapter** command from EXEC mode	`/adapter #`
Cabling	**scope cabling** command from EXEC mode	`/cabling #`
Chassis	**scope chassis** command from EXEC mode	`/chassis #`
Ethernet server domain	**scope eth-server** command from EXEC mode; this command and all subcommands are currently not supported	`/eth-server #`
Ethernet uplink	**scope eth-uplink** command from EXEC mode	`/eth-uplink #`
Fabric interconnect	**scope fabric-interconnect** command from EXEC mode	`/fabric-interconnect #`
Firmware	**scope firmware** command from EXEC mode	`/firmware #`

Mode Name	Commands Used to Access	Mode Prompt
Host Ethernet interface	**scope host-eth-if** command from EXEC mode **Note** This command and all subcommands are not supported at this level; the Host Ethernet interface commands are available in `/adapter #` mode.	`/host-eth-if #`
License	**scope license** command from EXEC mode	`/license #`
Monitoring	**scope monitoring** command from EXEC mode	`/monitoring #`
Organization	**scope org** command from EXEC mode	`/org #`
Packet capture	**scope packet-capture** command from EXEC mode	`/packet-capture #`
Security	**scope security** command from EXEC mode	`/security #`
Server	**scope server** command from EXEC mode	`/server #`
Service profile	**scope service-profile** command from EXEC mode **Note** Do not alter or configure service profiles; that is, do not use the **create**, **set**, or **delete** subcommand sets.	`/service-profile #`
SSA	**scope ssa** command from EXEC mode	`/ssa #`
System	**scope system** command from EXEC mode	`/system #`
Virtual HBA	**scope vhba** command from EXEC mode **Note** This command and all subcommands are currently not supported.	`/vhba #`
Virtual NIC	**scope vnic** command from EXEC mode	`/vnic #`

FXOS CLI Connects Diagram

The following diagram outlines the various commands that can be executed from the FXOS CLI top level to access the FXOS command shell, local management command shell, network adapter, CIMC, and security module CLI.

Figure 1: Firepower 4100/9300 FXOS CLI Connects Diagram



Object Commands

Four general commands are available for object management:

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

You can use the **scope** command with any managed object, whether a permanent object or a user-instantiated object. The other commands allow you to create and manage user-instantiated objects. For every **create** *object* command, a corresponding **delete** *object* and **enter** *object* command exists.

In the management of user-instantiated objects, the behavior of these commands depends on whether the object exists, as described in the following tables:

Table 2: Command Behavior If The Object Does Not Exist

Command	Behavior
create *object*	The object is created and its configuration mode, if applicable, is entered.
delete *object*	An error message is generated.
enter *object*	The object is created and its configuration mode, if applicable, is entered.
scope *object*	An error message is generated.

Table 3: Command Behavior If The Object Exists

Command	Behavior
create *object*	An error message is generated.
delete *object*	The object is deleted.
enter *object*	The configuration mode, if applicable, of the object is entered.
scope *object*	The configuration mode of the object is entered.

Complete a Command

You can use the **Tab** key in any mode to complete a command. Partially typing a command name and pressing **Tab** causes the command to be displayed in full or to the point where you must enter another keyword or an argument value.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the up-arrow or down-arrow keys. The up-arrow key moves to the previous command in the history, and the down-arrow key moves to the next command in the history. When you get to the end of the history, pressing the down-arrow key does nothing.

You can enter any command in the history again by stepping through the history to recall that command and then pressing **Enter**. The command is entered as if you had manually typed it. You can also recall a command and change it before you press **Enter**.

Commit, Discard, and View Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit-buffer** command. Until committed, a configuration command is pending and can be discarded by entering a **discard-buffer** command.

You can accumulate pending changes in multiple command modes and apply them together with a single **commit-buffer** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

Note All pending commands are checked for validity. However, if any queued command fails during commit, the remaining commands are applied; failed commands are reported in an error message.

While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit-buffer** command.

The following example shows how the prompts change during the command entry process:

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # create ntp-server 192.168.200.101
Firepower /system/services* # show configuration pending
 scope services
+    create ntp-server 192.168.200.101
 exit
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

Inline Help for the CLI

At any time, you can enter the **?** character to display the options available at the current state of the command syntax.

If you have not entered anything at the prompt, entering **?** lists all available commands for the mode you are in. With a partially entered command, entering **?** lists all keywords and arguments available at your current position in the command syntax.

CLI Session Limits

FXOS limits the number of CLI sessions that can be active at one time to 32 total sessions. This value is not configurable.

Filter and Save Show Output

Save and Filter Show Command Output

You can save the output of **show** commands by redirecting the output to a text file. You can filter the output of **show** commands by piping the output to filtering commands.

Saving and filtering output are available with all **show** commands but are most useful when dealing with commands that produce a lot of text. For example, you can show all or parts of the configuration by using the **show configuration** command. Copying the configuration output provides a way to backup and restore a configuration.

Note Show commands do not show the secrets (password fields), so if you want to paste a configuration into a new device, you will have to modify the show output to include the actual passwords.

Filter Show Command Output

To filter the output of a **show** command, use the following subcommands. Note that in the following syntax description, the initial vertical bar | after the **show** command is the pipe character and is part of the command, not part of the syntax description. The filtering options are entered after the command's initial | character.

show *command* **|** {**begin** *expression* | **count** | **cut** *expression* | **egrep** *expression* | **end** *expression* | **exclude** *expression* | **grep** *expression* | **head** | **include** *expression* | **last** | **less** | **no-more** | **sort** *expression* | **tr** *expression* | **uniq** *expression* | **wc**}

Filtering Options

These are the filtering subcommands:

- **begin**—Finds the first line that includes the specified pattern, and display that line and all subsequent lines.
- **count**—Counts the number of lines.
- **cut**—Removes ("cut") portions of each line.
- **egrep**—Displays only those lines that match the extended-type pattern.
- **end**—Ends with the line that matches the pattern.
- **exclude**—Excludes all lines that match the pattern and show all other lines.
- **grep**—Displays only those lines that match the pattern.
- **head**—Displays the first lines.
- **include**—Displays only those lines that match the pattern.
- **last**—Displays the last lines.
- **less**—Filters for paging.
- **no-more**—Turns off pagination for command output.
- **sort**—Sorts the lines (stream sorter).

- **tr**—Translates, squeezes, and/or deletes characters.
- **uniq**—Discards all but one of successive identical lines.
- **wc**—Displays a count of lines, words, and characters.

expression

An expression, or pattern, is typically a simple text string. Do not enclose the expression in single or double-quotes—these will be seen as part of the expression. Also, trailing spaces will be included in the expression.

Note Several of these subcommands have additional options that let you further control the filtering. For example, with **show configuration | head** and **show configuration | last**, you can use the **lines** keyword to change the number of lines displayed; the default is 10. As another example, with **show configuration | sort**, you can add the option **-u** to remove duplicate lines from the output. (Complete descriptions of these options is beyond the scope of this document; refer to the FXOS help output for the various commands, and to the appropriate Linux help, for more information.)

Examples

The following example shows how to determine the number of lines currently in the system event log:

```
FP9300-A# show sel 1/1 | count
3008
FP9300-A#
```

The following example shows how to display lines from the system event log that include the string “error”:

```
FP9300-A# show sel 1/1 | include error
968 | 05/15/2016 16:46:25 | CIMC | System Event DDR4_P2_H2_EC
C #0x99 | Upper critical - going high | Asserted | Reading 20
000 >= Threshold 20000 error
FP9300-A#
```

Related Topics

Save Show Command Output, on page 17

Save Show Command Output

You can save the output of **show** commands by redirecting the output to a text file.

show *command* [> { **ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:** }] | [>> { **volatile:** | **workspace:** }]

Syntax Description

> { **ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:** }	Redirects the **show** command output to a specified text file using the selected transport protocol. After you enter the command, you are queried for remote server name or IP address, user name, file path, and so on. If you press **Enter** at this point, the output is saved locally.

>> {**volatile:** | **workspace:**}	Appends the **show** command output to the appropriate text file, which must already exist.

Example

The following example attempts to save the current configuration to the system workspace; a configuration file already exists, which you can choose to overwrite or not.

```
FP9300-A# show configuration > workspace
File already exists, overwrite (y/n)?[n]n
Reissue command with >> if you want to append to existing file

FP9300-A#
```

Related Topics

Filter Show Command Output, on page 16

Unsupported and Restricted Commands

Unsupported Commands

The following commands, while visible in the CLI, are not supported. Entering any of these commands has no effect.

EXEC (Top-level) Commands

restore-check

scope eth-server (and all subcommands)

scope host-eth-if (the **host-eth-if** subcommands are available in `/adapter` mode)

scope nh-test (and all subcommands)

set nh-test

show nh-test

show registry-repository

show ucspe-tech-support

ucspe-copy

vhba (and all subcommands)

Chassis Mode Commands

`/chassis #` **scope iom**

`/chassis #` **show iom**

`/chassis #` **show post**

Fabric Interconnect Mode Commands

`/fabric-interconnect #` **scope fan**

`/fabric-interconnect #` **scope fan-module**

`/fabric-interconnect #` **scope psu**

`/fabric-interconnect #` **scope sw-uplink**

`/fabric-interconnect #` **show fan**

`/fabric-interconnect #` **show fan-module**

`/fabric-interconnect #` **show lan-neighbors**

`/fabric-interconnect #` **show psu**

`/fabric-interconnect #` **show san-neighbors**

`/fabric-interconnect #` **show sw-uplink**

Organization Mode Commands

`/org #` **recommission server**

`/org #` **scope auth-profile**

`/org #` **scope fc-policy**

`/org #` **scope iqn-pool**

`/org #` **scope iscsi-policy**

`/org #` **scope kvm-mgmt-policy**

`/org #` **scope rackserver-disc-policy**

`/org #` **scope rackserver-mgmt-policy**

`/org #` **scope san-connectivity-policy**

`/org #` **scope storage-connection-policy**

`/org #` **scope udld-link-policy**

`/org #` **scope udld-system-settings**

`/org #` **scope uuid-suffix-pool**

`/org #` **scope vhba-beh-policy**

`/org #` **scope vhba-templ**

`/org #` **scope vmq-conn-policy**

`/org #` **scope wwn-pool**

`/org #` **show fc-policy**

`/org #` **show fc-zone**

`/org #` **show iqn-pool**

`/org #` **show rackserver-disc-policy**

`/org #` **show rackserver-mgmt-policy**

`/org #` **show san-connectivity-policy**

`/org #` **show udld-link-policy**

`/org #` **show udld-system-settings**

`/org #` **show uuid-suffix-pool**

`/org #` **show vhba-beh-policy**

`/org #` **show vhba-templ**

`/org #` **show vmq-conn-policy**

`/org #` **show wwn-pool**

Packet Capture Mode Commands

`/packet-capture #` **show nh-test**

Security Mode Commands

`/security #` **create role**

`/security #` **delete role**

Server Mode Commands

`/server #` **show flexflash-controller**

Service Profile Mode Commands

`/service-profile #` **disassociate**

`/service-profile #` **rename-to**

`/service-profile #` **scope dynamic-vnic-conn**

`/service-profile #` **scope ext-pooled-ip**

`/service-profile #` **scope ext-static-ip**

`/service-profile #` **scope fc-zone**

`/service-profile #` **scope iscsi-boot**

`/service-profile #` **scope vhba**

`/service-profile #` **set dynamic-vnic-conn-policy**

`/service-profile #` **set ext-mgmt-ip-pool-name**

`/service-profile #` **set ext-mgmt-ip-state**

`/service-profile #` **set iscsi-identity**

`/service-profile #` **set kvm-mgmt-policy**

`/service-profile #` **set san-connectivity-policy-name**

`/service-profile #` **set src-templ-name**

`/service-profile #` **show dynamic-vnic-conn**

`/service-profile #` **show dynamic-vnic-conn-policy**

`/service-profile #` **show ext-pooled-ip**

`/service-profile #` **show ext-static-ip**

`/service-profile #` **show fc-zone**

`/service-profile #` **show initiator-group**

`/service-profile #` **show iscsi-boot**

`/service-profile #` **show iscsi-identity**

`/service-profile #` **show mgmt-iface**

`/service-profile #` **show vhba**

`/service-profile #` **show vnic-iscsi**

System Mode Commands

`/system #` **scope control-ep**

`/system #` **scope environment-features**

```
/system # scope storage-features
/system # scope vm-mgmt
/system # set virtual-ip
/system # show control-ep
```

Restricted Commands

Use of the following commands is restricted. Do not use any of these commands unless instructed to do so by a member of the Cisco Technical Assistance Center (TAC).

Service Profile Mode Commands

Do not change any service profile configurations; specifically do not use any of the `/service-profile #` **create**, `/service-profile #` **delete** or `/service-profile #` **set** subcommands.

PART I

A – R Commands

A – C Commands

acknowledge fault

To acknowledge a system fault, use the **acknowledge fault** command.

acknowledge fault *id*

Syntax Description

fault *id*	The fault identification number. The range of valid values is 0 to 18446744073709551615.

Command Modes

Multiple modes

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **acknowledge fault** command to acknowledge the existence of a fault.

Example

The following example shows how to acknowledge a fault:

```
firepower # acknowledge fault 11347599
firepower* # commit-buffer
firepower #
```

Related Commands

Command	Description
acknowledge server	Acknowledges a server on the device.
acknowledge slot	Acknowledges the existence of a slot in the device.
show fault	Shows fault policy information.

acknowledge server

To acknowledge a server, use the **acknowledge server** command.

acknowledge server {*id* | *chassis*/*blade_id*}

Syntax Description

server {*id* | *chassis*/*blade_id*}	To use the server identification number to identify the server to acknowledge, provide the *id*. To use the chassis and blade identification numbers to identify the server to acknowledge, enter *chassis*/*blade_id* in n/n format. **Note** The chassis ID number is always **1**.

Command Modes

EXEC

scope chassis/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **acknowledge server** command to verify the existence of a server in your network. For example, you can acknowledge a server that was recently commissioned to ensure that it exists.

In chassis mode, you can use only the *id* variable to identify the server to be acknowledged.

Example

The following example shows how to acknowledge a server in module 2 while in chassis mode:

```
firepower# scope chassis 1
firepower /chassis # acknowledge server 2
firepower /chassis* # commit-buffer
firepower /chassis #
```

Related Commands

Command	Description
acknowledge fault	Acknowledges a system fault.
acknowledge slot	Verifies the existence of a slot that was recently commissioned.
show server	The **show server** commands display a variety of server-related configuration information.

acknowledge slot

To acknowledge a slot, use the **acknowledge slot** command.

acknowledge slot {*id* | *chassis*/*blade_id*}

Syntax Description

	In EXEC mode, use the chassis and blade identification numbers to identify the slot to acknowledge; enter *chassis*/*blade_id* in n/n format. **Note** The chassis ID number is always **1**.

Command Modes

EXEC

scope chassis/

scope fabric-interconnect/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **acknowledge slot** command to verify the existence of a slot that was recently commissioned to ensure that it exists.

In chassis and fabric-interconnect mode, you can use only the *id* variable to identify the slot to be acknowledged.

In EXEC mode, you can use only the chassis and blade identification (*chassis*/*blade_id*) numbers to identify the slot to be acknowledged.

Example

The following example shows how to acknowledge a slot while in chassis mode:

```
firepower# scope chassis 1
firepower /chassis # acknowledge slot 2
firepower /chassis* # commit-buffer
firepower /chassis #
```

Related Commands

Command	Description
acknowledge fault	Acknowledges a system fault.
acknowledge server	Acknowledges the existence of a server in your network.

activate firmware

To activate a firmware package, use the **activate firmware** command.

activate firmware *version*

Syntax Description

version	Use its version number to specify the firmware package to be activated.

Command Modes

scope system/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

As part of the activation process, all CLI sessions will be terminated.

Example

This example shows how to activate a firmware package:

```
firepower# scope system
firepower /system # activate firmware 2.4(1.52)
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)
```

Related Commands

Command	Description
show firmware	Shows system firmware versions and status information.
show server firmware	Shows server firmware versions and status information.

backup sel

To back up the system event log (SEL), use the **backup sel** command.

backup sel {*id* | *chassis*/*blade_id*}

Syntax Description

id	The server ID. On 9300 devices, there may be up to 3 servers.
chassis/*blade_id*	The appliance chassis number and blade number in x/y format. **Note** The chassis ID number is always **1**.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to back up the system event log (SEL) for a server.

In the command mode of a specific server (/chassis/server), you can run this command without any options.

Example

This example shows how to back up the SEL for server 2 in chassis 1:

```
firepower# backup sel 1/2
firepower* # commit-buffer
firepower#
```

Related Commands

Command	Description
clear sel	Clears the system event log (SEL) for a server.

cancel

To cancel a reservation request, use the **cancel** command.

cancel

Syntax Description

This command has no arguments or keywords.

Command Modes

scope license/scope reservation/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you have already generated the authorization code, you must install it.

Example

This example shows how to cancel a reservation request:

```
firepower# scope license
firepower /license # scope reservation
firepower /license/reservation # cancel
Warning : If you have already generated the authorization code from CSSM, please abort the
 cancellation by issuing discard-buffer and then install the authorization code.
firepower /license/reservation* #
```

Related Commands

Command	Description
enable reservation	Enables permanent license reservation.
show license	Shows current license information.

clear lock-status

To clear a user's locked-out status, use the **clear lock-status** command in local user mode.

clear lock-status

Syntax Description

This command has no arguments or keywords.

Command Modes

Local user (/security/local-user)

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If any user (including admin users) exceeds the specified maximum number of login attempts, the user is locked out of the system and must wait the specified amount of time before being allowed to log in, unless you clear the user's locked-out status.

Example

This example shows how to enter local user mode and specify the amount of time that must pass before a locked-out user can log in.

```
FP9300-A # scope security
FP9300-A # scope local-user test_user1
FP9300-A /security/local-user # clear lock-status
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
set max-login-attempts	Specifies the maximum number of failed login attempts before the user is locked out of the system.
set user-account-unlock-time	Specifies the amount of time a user remains locked out of the system after reaching the maximum number of login attempts.

clear message

To clear the current pre-login banner text, use the **clear message** command; the pre-login banner object itself is not deleted.

clear message

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security/scope banner/scope pre-login-banner/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you enter this command, the text in the pre-login banner is cleared; the pre-login banner object itself is not deleted.

Example

This example shows you how to view the current pre-login banner, how to clear it, and then commit and and confirm your change:

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # scope pre-login-banner
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner/pre-login-banner # clear message
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------

firepower /security/banner/pre-login-banner #
```

Related Commands

Command	Description
create pre-login-banner	Creates a banner to be presented prior to the log-in screen; the banner object is initially empty.
set message	Adds or replaces the lines of text presented as the pre-login banner.

clear password-history

To clear the password history for a local user, use the **clear password-history** command.

clear password-history

Syntax Description

This command has no arguments or keywords.

Command Modes

Local user (/security/local-user) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You must be a user with admin or AAA privileges to use this command.

Example

This example shows how to enter local user mode and clear the password history for the user.

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # clear password history
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Command	Description
create local-user	Creates a new local user account.
set password	Specifies the password for a user account.

clear sel

To clear the system event log (SEL) for a server, use the **clear sel** command.

clear sel {*id* | *chassis_id* / *blade_id*}

Syntax Description

id	(Optional) The server ID. The 9300 devices have a maximum of 3 servers.
chassis_id / *blade_id*	(Optional) The chassis number and blade number in n/n format. **Note** The chassis ID number is always **1**.

Command Modes

Any command mode

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

Use this command to clear the system event log (SEL) for a server.

In the command mode for a specific server (/chassis/server), you can run this command without specifying a server.

Example

This example shows how to clear system event logs for server 1 in chassis 1 while in organization mode.

```
FP9300-A # scope org Test
FP9300-A /org # clear sel 1/1
FP9300-A /org* # commit-buffer
FP9300-A /org #
```

Related Commands

Command	Description
backup sel	Backs up the system event log (SEL).

commit-buffer

To save or verify configuration changes, use the **commit-buffer** command.

commit-buffer [**verify-only**]

Syntax Description

verify-only	(Optional) Verifies/validates buffer contents only; the contents are not committed.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to execute or verify all pending configuration changes. While any configuration changes are pending, an asterisk (*) appears before the command prompt. When you enter the **commit-buffer** command, the pending commands are committed and the asterisk disappears.

Example

This example shows how to save configuration changes:

```
FP9300-A# create org 3
FP9300-A /org* # commit-buffer
FP9300-A /org #
```

Related Commands

Command	Description
discard-buffer	Cancels and discards all uncommitted configuration changes.
show configuration pending	Shows all pending configuration changes.

connect adapter

To connect to the adapter command shell, use the **connect** command.

connect adapter {*chassis/server/id* | *rack_server/id*}

Syntax Description

chassis/server/id	Specifies the chassis, server (module) and adapter IDs (entered in n/n/n format). On the Firepower 9300, the module number can be 1, 2, or 3. On the Firepower 4100, it is 1. **Note** The chassis ID number is always **1**.
rack_server/id	Specifies the rack number and module ID (entered in n/n format).

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use **help** to list available mezzanine adapter commands; use **help** *command* to view information about an individual command.

Refer to connect adapter: Command List, on page 690 for additional information.

Note When you connect to an adapter command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to `adapter n/n/n`, where `n/n/n` is the adapter's chassis/server/ID combination you entered to connect.

To exit the adapter mode, type **exit**.

Example

The following example shows how to connect to the adapter command shell, and view available commands:

```
firepower# connect adapter 1/1/1
adapter 1/1/1 # help
Available commands:
  connect             - Connect to remote debug shell
  exit                - Exit from subshell
  help                - List available commands
  history             - Show command history
  show-fwlist         - Show firmware versions on the adapter
  show-identity       - Show adapter identity
  show-phyinfo        - Show adapter phy info
  show-systemstatus   - Show adapter status
adapter 1/1/1 # exit
```

```
firepower#
```

Related Commands

Command	Description
exit	Returns you to the previous CLI mode.

connect asa

To connect to the ASA CLI, use the **connect asa** command.

connect asa [*name*]

Syntax Description

name	(Optional) Specifies the ASA application instance name, which is the same as the logical device name.

Command Modes

connect module/

Command History

Release	Modification
2.4(1)	Added the *name* argument.
1.1(4)	Command added.

Usage Guidelines

See the ASA documentation for commands available from the CLI.

To exit the ASA console, enter **Ctrl-a, d**

Return to the supervisor level of the FXOS CLI:

Exit the console:

Enter **~**, then **quit** to exit the Telnet application.

Example:

```
asa> Ctrl-a, d
Firepower-module1> ~
telnet> quit
firepower#
```

Exit the Telnet session:

Enter **Ctrl-], .**

Example:

```
asa> Ctrl-a, d
Firepower-module1> Ctrl-], .
firepower#
```

Example

This example shows how to connect to the ASA CLI on module 1:

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
```

```
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect asa
asa>
```

Related Commands

Command	Description
connect ftd	Connects to the threat defense CLI.
connect module	Connects to the module CLI.
connect vdp	Connects to the vDP CLI.

connect cimc

To connect to the Cisco Integrated Management Controller (CIMC) command shell, use the **connect cimc** command.

connect cimc {*chassis_id/blade_id* | *rack_id*}

Syntax Description

chassis_id/blade_id	Specifies the chassis and module numbers (entered in n/n format). **Note** The chassis ID number is always **1**.
rack_id	Specifies the rack number.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Enter **help** to list available CIMC firmware debug utility commands; enter **help** *command* to view information about an individual command.

Note When you connect to the CIMC command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to `[ xxx ]`, where `xxx` is the last command you entered; see the following example.

Type **exit** to terminate the utility.

Do not use this utility unless instructed to do so by Cisco TAC. Refer to connect cimc: Command List, on page 694 for additional information.

Example

The following example shows how to connect to CIMC mode and then list the available commands:

```
firepower# connect cimc 1/1
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.

CIMC Debug Firmware Utility Shell [ support ]
[ help ]# help
------------------------------------------
          Debug Firmware Utility
------------------------------------------
Command List
------------------------------------------
alarms
cores
```

```
dimmbl
exit
i2cstats
images
mctools
memory
messages
mrcout
network
obfl
post
power
programmables
sensors
sel
fru
tasks
top
update
users
version
cert
sldp
help
help [COMMAND]
_____________________________________
 Notes:
"enter Key" will execute last command
"COMMAND ?" will execute help for that command
_____________________________________
[ help ]# exit
Connection closed by foreign host.
firepower#
```

Related Commands

Command	Description
exit	Returns you to the previous CLI mode.

connect ftd

To connect to the threat defense CLI, use the **connect ftd** command.

connect ftd *name*

Syntax Description

name	Specifies the threat defense application instance name, which is the same as the logical device name. If you have multiple application instances for an application type, you must specify the name of the instance. To view the instance names, enter the command without a name.

Command Modes

connect module/

Command History

Release	Modification
2.4(1)	Added the *name* argument. The escape character was changed to **exit** from **Ctrl-a, d**.
1.1(4)	Command added.

Usage Guidelines

See the threat defense documentation for commands available from the CLI.

To exit the threat defense console, enter **exit**. For pre-2.4(1) versions, enter **Ctrl-a, d**

Return to the supervisor level of the FXOS CLI:

Exit the console:

Enter **~**, then **quit** to exit the Telnet application.

Example:

```
> exit
Firepower-module1> ~
telnet> quit
firepower#
```

Exit the Telnet session:

Enter **Ctrl-], .**

Example:

```
> exit
Firepower-module1> Ctrl-], .
firepower#
```

Example

This example shows how to connect to the threat defense CLI on module 1:

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect ftd
>
```

Related Commands

Command	Description
connect asa	Connects to the ASA CLI.
connect module	Connects to the module CLI.
connect vdp	Connects to the vDP CLI.

connect fxos

To connect to the FXOS command shell, use the **connect fxos** command.

connect fxos [**a**]

Syntax Description

a	(Optional) Connects to fabric a. **Note** The fabric ID is always **a**. If you omit the fabric ID, you are connected to fabric A.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Type **?** to list available FXOS shell commands; enter *command* **?** to view information about an individual command.

Note When you connect to the FXOS command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to the default prompt with `(fxos)` appended; see the following example.

To exit the FXOS shell, type **exit**.

Example

The following example shows how to connect to the FXOS command shell, and view available commands:

```
firepower# connect fxos
firepower(fxos)# ?
  clear         Reset functions
  cli           CLI commands
  debug         Debugging functions
  debug-filter  Enable filtering for debugging functions
  ethanalyzer   Configure cisco packet analyzer
  no            Negate a command or set its defaults
  ntp           NTP configuration
  show          Show running system information
  system        System management commands
  terminal      Set terminal line parameters
  test          Test command
  undebug       Disable Debugging functions (See also debug)
  end           Go to exec mode
  exit          Exit from command interpreter
  pop           Pop mode from stack or restore from name
  push          Push current mode to stack or save it under name
  where         Shows the cli context you are in
```

```
firepower(fxos)# exit
firepower#
```

Related Commands

Command	Description
connect local-mgmt	Connects to a remote debug shell while connected to a specific adapter.
exit	Returns you to the previous CLI mode.

connect local-mgmt

To connect to the local-management command shell, use the **connect local-mgmt** command.

connect local-mgmt [**a**]

Syntax Description

a	(Optional) Connects to fabric a. **Note** The fabric ID is always **a**. If you omit the fabric ID, you are connected to fabric A.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Type **?** to list available local-management shell commands; enter *command* **?** to view information about an individual command.

Refer to connect local-mgmt: Command List, on page 712 for additional information.

Note When you connect to the local-management command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to the default prompt with `(local-mgmt)` appended; see the following example.

To exit the local-management mode, type **exit**.

Example

The following example shows how to connect to the local-management command shell, and view available commands:

```
firepower# connect local-mgmt
firepower(local-mgmt)#  ?
  cd                Change current directory
  clear             Clear managed objects
  cluster           Cluster mode
  connect           Connect to Another CLI
  copy              Copy a file
  cp                Copy a file
  delete            Delete managed objects
  dir               Show content of dir
  enable            Enable
  end               Go to exec mode
  erase             Erase
  erase-log-config  Erase the mgmt logging config file
  exit              Exit from command interpreter
  fips              FIPS compliance
  ls                Show content of dir
```

```
  mgmt-port         Management Port
  mkdir             Create a directory
  move              Move a file
  mv                Move a file
  ping              Test network reachability
  ping6             Test IPv6 network reachability
  pwd               Print current directory
  reboot            Reboots Fabric Interconnect
  restore-check     Check if in restore mode
  rm                Remove a file
  rmdir             Remove a directory
  run-script        Run a script
  show              Show system information
  shutdown          Shutdown
  ssh               SSH to another system
  tail-mgmt-log     tail mgmt log file
  telnet            Telnet to another system
  terminal          Terminal
  top               Go to the top mode
  traceroute        Traceroute to destination
  traceroute6       Traceroute to IPv6 destination
  verify            Verify Application Image

firepower(local-mgmt)# exit
firepower#
```

Related Commands

Command	Description
connect fxos	Connects to the FXOS command shell.
exit	Returns you to the previous CLI mode.

connect module

To connect to a module command shell, use the **connect module** command.

connect module *module_id* {**console** | **telnet**}

Syntax Description

console	Connects to the serial console. The benefit of a console connection is that it is persistent.
module_id	On 9300 devices the module number can be 1, 2, or 3; on 4100 devices it is 1.
telnet	Connects using a Telnet connection. The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Command Modes

Any command mode

Command History

Release	Modification
2.4(1)	Telnet support added.
1.1(1)	Command added.

Usage Guidelines

From the module CLI, you can connect to the application CLI using the **connect** *application* command.

Type **help** to list available module shell commands; enter **help** *command* to view information about an individual command. You also can use **?** in place of **help** to view help information.

Note When you connect to a module command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to `Firepower-module`*n*, where *n* is the number of the module to which you connected; see the following example.

Refer to connect module: Command List, on page 718 for additional information.

Examples

The following example shows how to connect to the module 1 console, and view available commands:

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>?
    secure-login     => Enable blade secure login
```

```
    show             => Display system information. Enter show ? for options
    config           => Configure the system. Enter config ? for options
    terminalLength   => Terminal settings. Enter terminal ? for options
    ping             => Ping a host to check reachability
    nslookup         => Look up an IP address or host name with the DNS servers
    traceroute       => Trace the route to a remote host
    connect          => Connect to specific csp console (asa, etc)
    support          => System file operations
    help             => Get help on command syntax

Firepower-module1> ~
telnet> close
Connection closed.
firepower#
```

The following example shows how to connect to the module 1 using Telnet, and view available commands:

```
firepower# connect module 1 telnet
Type exit or Ctrl-] followed by . to quit.
Firepower-module1>?
    secure-login     => Enable blade secure login
    show             => Display system information. Enter show ? for options
    config           => Configure the system. Enter config ? for options
    terminalLength   => Terminal settings. Enter terminal ? for options
    ping             => Ping a host to check reachability
    nslookup         => Look up an IP address or host name with the DNS servers
    traceroute       => Trace the route to a remote host
    connect          => Connect to specific csp console (asa, etc)
    support          => System file operations
    exit             => Exit the session
    help             => Get help on command syntax
Firepower-module1> <Ctrl-], .>
firepower#
```

Related Commands

Command	Description
connect asa	Connects to the ASA CLI.
connect ftd	Connects to the threat defense CLI.
connect vdp	Connects to the vDP CLI.

connect vdp

To connect to the Radware DefensePro (vDP) CLI, use the **connect vdp** command.

connect vdp [*name*]

Syntax Description

name	(Optional) Specifies the vDP application instance name, which is the same as the main application logical device/application instance name.

Command Modes

connect module/

Command History

Release	Modification
2.4(1)	Added the *name* argument.
1.1(4)	Command added.

Usage Guidelines

See the vDP documentation for commands available from the CLI.

To exit the vDP console, enter **Ctrl-], .**

Return to the supervisor level of the FXOS CLI:

Exit the console:

Enter **~**, then **quit** to exit the Telnet application.

Example:

```
> Ctrl-], .
Firepower-module1> ~
telnet> quit
firepower#
```

Exit the Telnet session:

Enter **Ctrl-], .**

Example:

```
> Ctrl-], .
Firepower-module1> Ctrl-], .
firepower#
```

Example

This example shows how to connect to the vDP CLI on module 1:

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
```

```
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect vdp
```

Related Commands

Command	Description
connect asa	Connects to the ASA CLI.
connect ftd	Connects to the threat defense CLI.
connect module	Connects to the module CLI.

create app-instance

To define an application instance, use the **create app-instance** command.

create app-instance *app_type app_name*

Syntax Description

app_name	The name of the application instance, between 1 and 64 characters. You will use this device name when you create the logical device for this instance.
app_type	The application type, either **asa**, **ftd**, or **vdp**.

Command Modes

scope ssa/scope slot/

Command History

Release	Modification
2.4(1)	The *app_name* argument is now required.
1.1(1)	Command added.

Usage Guidelines

You can set many parameters for this application instance, including the the image version, deployment type, resource profile and mode. You can also enable, disable and restart the application.

Example

The following example shows how to set the image version for an threat defense application instance:

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance ftd MyDevice1
firepower /ssa/slot/app-instance* # set deploy-type container
firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
firepower /ssa/slot/app-instance* # set startup-version 6.3.0
firepower /ssa/slot/app-instance* #
```

Related Commands

Command	Description
show app-attri	Shows current application attributes.

create bootstrap-key FIREWALL_MODE

To specify the firewall mode, routed or transparent, in the bootstrap configuration for the threat defense and ASA, use the **create bootstrap-key FIREWALL_MODE** command.

create bootstrap-key FIREWALL_MODE

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The default mode is routed.

Command History

Release	Modification
2.4(1)	Added support for the ASA.
1.1(4)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the mode to routed mode:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key MANAGEMENT_TYPE

To specify the manager, FMC, FDM, or CDO in the bootstrap configuration for the threat defense, use the **create bootstrap-key MANAGEMENT_TYPE** command.

create bootstrap-key MANAGEMENT_TYPE

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The default manager is FMC.

Command History

Release	Modification
2.7(1)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the manager to FDM:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

The following example shows how to set the manager to CDO:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value CDO
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key PERMIT_EXPERT_MODE

To permit Expert Mode from FTD SSH sessions for the threat defense, use the **create bootstrap-key PERMIT_EXPERT_MODE** command.

create bootstrap-key PERMIT_EXPERT_MODE

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The default is no.

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

Expert Mode provides FTD shell access for advanced troubleshooting. By default for container instances, Expert Mode is only available to users who access the FTD CLI from the FXOS CLI. This limitation is only applied to container instances to increase isolation between instances. Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the expert command in the FTD CLI.

Example

The following example shows how to enable Expert Mode from SSH:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key MANAGEMENT_TYPE

create bootstrap-key-Secret CDO_ONBOARD

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command History

Release	Modification
2.13(1)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the CDO onboard value for the FTD device:

```
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret CDO_ONBOARD
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap/bootstrap-key* #
Enter a value:(the string “configure manager add cisco-sapphire.app.staging.cdo.cisco.com
TuNDBm6peReVDbU kOpZCgtJ1GqWKbD30 o9B064UXEwmr3AYAEpuflf4qE2E3JKY5 <display_name>” should
be
entered)
Confirm the value: (repeat the string)
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key-secret PASSWORD

To specify the admin password in the bootstrap configuration for the threat defense and ASA, use the **create bootstrap-key-secret PASSWORD** command.

create bootstrap-key-secret PASSWORD

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

When the admin password is not set.

Command History

Release	Modification
1.1(4)	Command added for FTD.
2.4(1)	Added support for the ASA.

Usage Guidelines

The pre-configured ASA admin user and enable password is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Example

The following example shows how to set the mode to routed mode:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # create bootstrap-key-secret
PASSWORD
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key-secret REGISTRATION_KEY

To specify a registration key to be shared between the threat defense device and management center in the bootstrap configuration, use the **create bootstrap-key-secret REGISTRATION_KEY** command.

create bootstrap-key-secret REGISTRATION_KEY

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The registered key is not generated.

Command History

Release	Modification
1.1(4)	Command added for FTD.

Usage Guidelines

You can choose any passphrase for this registration key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD. Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the value for the registration key:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key DNS_SERVERS

To specify a comma-separated list of DNS servers for the threat defense, use the **create bootstrap-key DNS_SERVERS** command.

create bootstrap-key DNS_SERVERS

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The default is no.

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

The FTD uses DNS if you specify a hostname for the FMC.

Example

The following example shows how to specify a hostname:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key FIREPOWER_MANAGER_IP

To specify the IP address or hostname or NAT ID of the managing Firepower Management Center, use the **create bootstrap-key FIREPOWER_MANAGER_IP** command.

create bootstrap-key FIREPOWER_MANAGER_IP

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The default is no.

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. You can specify any text string as the NAT ID, from 1 to 37 characters. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

Example

The following example shows how to enable Expert Mode from SSH:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create bootstrap-key SEARCH_DOMAINS

To specify a comma-separated list of search domains, use the **create bootstrap-key SEARCH_DOMAINS** command.

create bootstrap-key SEARCH_DOMAINS

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/

Command Default

The default is no.

Command History

Release	Modification
2.4(1)	Command added.

Example

The following example shows how to enable Expert Mode from SSH:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.
set value	Sets the value for this command.

create breakout

To create a breakout port, use the **create breakout** command. If a breakout with the specified slot and port IDs already exists, the command will fail.

To add or enter a breakout port, utilize the **enter breakout** command. If the specified breakout does not exist, it is created and entered; if the breakout port exists, it is entered.

You also can use the **scope** form of this command to enter an existing breakout port to view properties.

To delete an existing breakout port, use the **delete** form of this command.

create breakout *slot_ID port_ID*

Syntax Description

slot_ID	Use its slot number to identify the port module to be broken out.
port_ID	Assign an ID number to this breakout port.

Command Modes

scope cabling/scope fabric a/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

In conjunction with the use of a breakout cable, you can use this command to "break out" a 40-Gigabit Ethernet port, creating up to four unconfigured 10-Gigabit ports.

Hardware bypass-capable interfaces cannot be configured as breakout ports.

Note Because configuring breakout on a port causes a system reboot, we recommend you break out all required ports before committing the changes.

Example

The following example shows how to create four breakout ports on slot 2:

```
firepower# scope cabling
firepower /cabling/fabric/ # scope fabric
firepower /cabling/fabric/ # create breakout 2 1
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 2
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 3
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 4
```

```
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # commit-buffer
firepower /cabling/fabric/breakout #
```

Related Commands

Command	Description
delete breakout	Deletes an existing breakout port.
enter aggr-interface	Enters an aggregate interface where you can set parameters.

create certreq

To add a new keyring certificate request, use the **create certreq** command. If a request already exists for the current keyring, the command will fail.

To edit an existing certificate request, use the **enter certreq** command.

You also can use the **scope** form of this command to enter an existing certificate request to assign or change properties.

To delete an existing certificate request, use the **delete** form of this command.

create certreq [**ip** | **subject-name**]

delete certreq

enter certreq
scope certreq

Syntax Description

ip *ip_address*	(Optional) Enter the **ip** keyword and the IPv4 address of the domain on which this device resides. You will be asked to enter and confirm a password for the request. This parameter applies only to the **create certreq** form of the command.
subject-name *name*	(Optional) Enter the **subject-name** keyword and an identifier for this request; for example, the appliance host name. You will be asked to enter and confirm a password for the request. This parameter applies only to the **create certreq** form of the command.

Command Modes

scope security/scope keyring/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you create a new keyring certificate request, you are automatically entered into certificate request mode (security/keyring/certreq) with an asterisk indicating the new certificate request is not yet defined and committed. You also can scope into certificate request mode for an existing keyring.

Use the **set** command in certificate request mode to specify certificate request parameters.

Note Before you create or commit a new certificate request, you must set the RSA key modulus (SSL key length) using set modulus, on page 314.

Example

This example shows how to create a new keyring and its certificate request:

```
firepower # scope security
firepower /security # create keyring test-ring2
firepower /security/keyring* # create certreq ip 209.165.201.20
Certificate request password:
Confirm certificate request password:
firepower /security/keyring* # scope certreq
firepower /security/keyring/certreq* #
firepower /security/keyring/certreq* # set ?
  country        Country name (2 letter code)
  dns            DNS name (subject alternative name)
  e-mail         E-mail name
  fi-a-ip        Certificate request FI A ip address
  fi-a-ipv6      Certificate request FI A ipv6 address
  fi-b-ip        Certificate request FI B ip address
  fi-b-ipv6      Certificate request FI B ipv6 address
  ip             Certificate request ip address
  ipv6           Certificate request ipv6 address
  locality       Locality name (eg, city)
  org-name       Organisation name (eg, company)
  org-unit-name  Organisational Unit Name (eg, section)
  password       Certificate request password
  state          State, province or county (full name)
  subject-name   Certificate request subject name

firepower /security/keyring/certreq* # set
```

Related Commands

Command	Description
delete certreq	Deletes an existing keyring certificate request.
set (certreq)	Sets keyring certificate request-related information.

create class

To add a new class of statistics to a statistics threshold policy, use the **create class** command. If a class with the specified name already exists, the command will fail.

To add or edit an statistics class, use the **enter class** command. If the specified class does not exist, it is created and entered; if the class exists, it is entered.

You also can use the **scope** form of this command to enter an existing class to assign or change properties. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing class of statistics, use the **delete** form of this command.

create class *type*
delete class *type*
enter class *type*
scope class *type*

Syntax Description

type	Specify the desired statistics class. Available classes depend on the statistics threshold policy in your current mode. For example, in `eth-server/` mode, available classes include `chassis-stats` and `ether-error-stats`. In `eth-uplink/` mode, available classes include `ether-rx-stats` and `ether-rx-stats`. In `org/` mode, available classes include `cpu-env-stats` and `ethernet-port-err-stats`. Use the **create class ?** command to view a list of classes available for the current statistics threshold policy.

Command Modes

scope eth-server/scope stats-threshold-policy/

scope eth-uplink/scope stats-threshold-policy/

scope org/scope stats-threshold-policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use classes to place thresholds on specific sets of statistics. For example, you might want to define a threshold on a port that raises a fault if the average number of packets dropped exceeds a certain amount. For this class, you would create threshold properties for Ethernet error statistics.

You can configure multiple classes for a statistics threshold policy.

Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Note There is one default statistics threshold policy each for Ethernet server ports or Ethernet uplink ports. You cannot create additional statistics collection policies and you cannot delete the existing default policies for these components—you can only modify the default policies. However, you can create and delete statistics threshold policies in organization mode (`scope org/`).

Examples

This example shows how to scope into the Ethernet server statistics threshold policy class, create a chassis statistics class, create an input power (Watts) property, specify that the normal power is 8 kW, create an above normal warning threshold of 11 kW, and then commit the class:

```
firepower # scope eth-server
firepower /eth-server # scope stats-threshold-policy default
firepower /eth-server/stats-threshold-policy # create class chassis-stats
firepower /eth-server/stats-threshold-policy/class* # create property input-power
firepower /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
firepower /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
 11000.0
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-server/stats-threshold-policy/class/property/threshold-value #
```

This example shows how to scope into organization mode, create a new statistics threshold policy for server and server component statistics, create a threshold policy class for CPU environment statistics, create a CPU temperature property, specify that the normal CPU temperature is 48.5° C, create an above normal warning threshold of 50° C, and commit the entire transaction:

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

Related Commands

Command	Description
delete class	Deletes an existing class of statistics.
enter class	Enters a statistics class. If the class does not exist, it is created.
enter property	Enters or creates a property for a class of statistics.
scope stats-threshold-policy	Enters stats-threshold-policy mode, where you manage specific statistics classes.

create connection

To add a new IPSec connection, use the **create connection** command. If a connection with the specified name already exists, the command will fail.

To add or edit an IPSec connection, use the **enter connection** command. If the specified connection does not exist, it is created and entered; if the connection exists, it is entered.

You also can use the **scope** form of this command to enter an existing connection to assign or change properties. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing connection, use the **delete** form of this command.

create connection *name*
enter connection *name*
delete connection *name*
scope connection *name*

Syntax Description

name	The connection name; can be up to 16 alphanumeric characters.

Command Modes

scope security/scope ipsec/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you create a new IPSec connection, you are automatically entered into security/ipsec/connection mode with an asterisk indicating the new connection is not yet committed. You can configure the connection before committing it.

After you create a connection, the name cannot be changed. You must delete the connection and create a new one.

Example

This example shows how to create and enter a new IPSec connection:

```
firepower # scope security
firepower /security # scope ipsec
firepower /security/ipsec # enter connection ipsec_conn2
firepower /security/ipsec/connection* #
```

Related Commands

Command	Description
set adminstate	Sets the IPSec connection administrative state to disabled or enabled.
show connection	Shows current IPSec connection information.

create destination

To add a new Smart Call Home destination, use the **create destination** command. If a destination with the specified name already exists, the command will fail.

To add or edit a Smart Call Home destination, use the **enter destination** command. If the specified destination does not exist, it is created and entered; if the destination exists, it is entered.

You also can use the **scope** form of this command to enter an existing destination to assign or change properties. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing destination, use the **delete** form of this command.

create destination *name*
delete destination *name*
enter destination *name*
scope destination *name*

Syntax Description

name	The name identifying the Smart Call Home destination.

Command Modes

scope monitoring/scope callhome/scope profile/

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

When you create a new Smart Call Home destination, you are automatically entered into callhome/profile mode (monitoring/callhome/profile) with an asterisk indicating the new destination is not yet committed. You can set the destination parameters—transport protocol and an email address—and then commit the new destination information.

Note An email address is the only allowed destination address in a callhome profile.

After you create a Smart Call Home destination, the destination name cannot be changed. You must delete the destination and create a new one.

Example

This example shows how to create, enter and configure a Smart Call Home destination:

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # enter destination TestDest
firepower /monitoring/callhome/profile/destination* # set address user1@test.com
firepower /monitoring/callhome/profile/destination* # set protocol email
firepower /monitoring/callhome/profile/destination* # commit-buffer
firepower /monitoring/callhome/profile/destination #
```

Related Commands

Command	Description
delete destination	Deletes an existing Smart Call Home destination.
enter destination	Enters a Smart Call Home destination.
set address	Sets an email address for a Smart Call Home destination.
set protocol	Sets the transport protocol for a Smart Call Home destination.

create dns

To create DNS name server in FXOS, use the **create dns** command.

create dns

Syntax Description

create dns	This command is used to create a DNS name server in FXOS.

Command Modes

scope system/scope services

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command creates the DNS name server in FXOS.

Example

This example shows how to create a DNS name server:

```
firepower# scope system; scope services
firepower /system /services # create dns 192.0.2.1
firepower /system /services* # commit
```

create hw-crypto

To create a TLS crypto acceleration configuration on a container instance, use the **create hw-crypto** command. For more information about TLS crypto acceleration, see the *Management Center Configuration Guide*.

create hw-crypto

Command Modes

connect module

Command History

Release	Modification
2.7.1	This command was introduced.

Usage Guidelines

This command deletes a TLS crypto acceleration configuration for a container instance. If TLS crypto acceleration is enabled on the container instance, the command disables it before deleting the configuration.

Examples

Following is an example of creating a TLS crypto acceleration configuration:

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- --------------- ---------------
 ----------- ---------- ------------ --------------- -------------
ftd        FTD-FDM    1          Enabled     Online          6.5.0.1159      6.5.0.1159
    Native      No                    Not Applicable  None
ftd        ftd2       2          Enabled     Online          6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # create hw-crypto
/ssa/slot/app-instance* # commit-buffer
```

Related Commands

Command	Description
delete hw-crypto	Delete a TLS crypto acceleration configuration for a container instance.
scope hw-crypto	Enable or disable TLS crypto acceleration configuration on a container instance.
show hw-crypto	Display the status of TLS crypto acceleration configuration on a container instance.

create ip-block

To add a new block of IPv4 addresses for service access, use the **create ip-block** command. If an address block with the specified properties already exists, the command will fail.

To add or edit a block of IPv4 addresses, use the **enter ip-block** command. If the specified address block does not exist, it is created and entered; if the address block exists, it is entered.

You also can use the **scope** form of this command to enter an existing address block to assign or change properties.

To delete an existing address block, use the **delete** form of this command.

create ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}
delete ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}
enter ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}
scope ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}

Syntax Description

ip_address	The starting address for the IPv4 address block.
prefix_length	The prefix length; determines the number of addresses in the block. Value can be 0 to 32.
https | **snmp** | **ssh**	The service (HTTPS, SNMP, or SSH) to which the address block is assigned.

Command Modes

scope system/scope services/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to assign a block of IPv4 addresses to provide access to a specified service (HTTPS, SNMP, or SSH).

When you create a new IP block, you are automatically entered into ip-block mode (system/services/ip-block) with an asterisk indicating the new block assignment is not yet committed.

On FXOS versions 2.3.1 and earlier, up to 25 different blocks can be configured for each service. On FXOS versions 2.4.1 and later, up to 100 different blocks can be configured for each service. An address of 0.0.0.0 and a prefix of 0 allows unrestricted access to a service. Each block of addresses is identified by its starting IPv4 address.

Example

This example shows how to create, enter and verify an IPv4 address block to provide SSH access:

```
firepower # scope system
firepower /system # scope services
firepower /system/services # enter ip-block 192.168.200.101 32 ssh
firepower /system/services/ip-block* # commit-buffer
firepower /system/services/ip-block # up
firepower /system/services # show ip-block
```

```
Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    0.0.0.0                     0 https
    0.0.0.0                     0 snmp
    0.0.0.0                     0 ssh
    192.168.200.101            32 ssh
firepower /system/services #
```

Related Commands

Command	Description
create ipv6-block	Creates an IPv6 address block.
delete ip-block	Deletes an existing IPv4 block.

create ipv6-block

To add a new block of IPv6 addresses for service access, use the **create ipv6-block** command. If an address block with the specified properties already exists, the command will fail.

To add or edit a block of IPv6 addresses, use the **enter ipv6-block** command. If the specified address block does not exist, it is created and entered; if the address block exists, it is entered.

You also can use the **scope** form of this command to enter an existing address block to assign or change properties.

To delete an existing address block, use the **delete** form of this command.

create ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}
delete ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}
enter ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}
scope ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}

Syntax Description

ipv6_address	The starting address for the IPv6 address block.
prefix_length	The prefix length; determines the number of addresses in the block. Value can be 0 to 128.
https | **snmp** | **ssh**	The service (HTTPS, SNMP, or SSH) to which the address block is assigned.

Command Modes

scope system/scope services/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to assign a block of IPv6 addresses to provide access to a specified service (HTTPS, SNMP, or SSH).

When you create a new IPv6 block, you are automatically entered into ipv6-block mode (system/services/ipv6-block) with an asterisk indicating the new block assignment is not yet committed.

On FXOS versions 2.3.1 and earlier, up to 25 different blocks can be configured for each service. On FXOS versions 2.4.1 and later, up to 100 different blocks can be configured for each service. An address of 0:0:0:0:0:0:0:0 and a prefix of 0 allows unrestricted access to a service. Each block of addresses is identified by its starting IPv6 address.

Example

This example shows how to create, enter and verify an IPv6 address block to provide SSH access:

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ipv6-block 2001:DB8:1::1 64 ssh
firepower /system/services/ipv6-block* # commit-buffer
firepower /system/services/ipv6-block # up
firepower /system/services # show ipv6-block
```

```
Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    ::                       0 https
    ::                       0 snmp
    ::                       0 ssh
    2001:DB8:1::1
                            64 ssh
firepower /system/services #
```

Related Commands

Command	Description
create ip-block	Creates an IPv4 block.
delete ipv6-block	Deletes an existing IPv6 block.

create keyring

To add a new RSA keyring, use the **create keyring** command. If a keyring with the specified name already exists, the command will fail.

To edit an existing keyring, use the **enter keyring** command.

You also can use the **scope** form of this command to enter an existing keyring to assign or change properties.

To delete an existing keyring, use the **delete** form of this command.

create keyring *name*
delete keyring *name*
enter keyring *name*
scope keyring *name*

Syntax Description

name	The name identifying the keyring; can be between 1 and 16 characters.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you create a new keyring, you are automatically entered into keyring mode (security/keyring) with an asterisk indicating the new keyring is not yet committed. You can create a keyring certificate request, and set keyring parameters such as RSA key modulus and certificate authority trustpoint, and then commit the new keyring information.

Example

This example shows how to create and enter a new RSA keyring:

```
firepower # scope security
firepower /security # enter keyring test_keyring
firepower /security/keyring* # set ?
  cert        Keyring certificate
  modulus     RSA key modulus
  regenerate  Regenerate keyring
  trustpoint  Trustpoint CA

firepower /security/keyring* # set
```

Related Commands

Command	Description
delete keyring	Deletes an existing RSA keyring.

create local-user

To add a new local user account, use the **create local-user** command. If a local user account with the specified name already exists, the command will fail.

To add or edit a local user account, use the **enter local-user** command. If the specified account does not exist, it is created and entered; if the account exists, it is entered.

You also can use the **scope** form of this command to enter an existing local user account to assign or change properties.

To delete an existing local user account, use the **delete** form of this command.

create local-user *user_name*
delete local-user *user_name*
enter local-user *user_name*
scope local-user *user_name*

Syntax Description

user_name	The ID to be used when logging into this local user account. Note the following guidelines and restrictions when entering a user name:
	• The name can contain between 1 and 32 characters, including the following:
	  • Any alphabetic character
	  • Any numeral
	  • _ (underscore)
	  • - (dash)
	  • . (dot)
	• The name must be unique.
	• The name must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
	• The name is case-sensitive.
	• You cannot create an all-number name.
	After you create a user account, you cannot change its name. You must delete the user account and create a new one.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can configure up to 48 local user accounts. Each account must have a unique user name and password.

When you create a new user account, you are automatically entered into local user mode (/security/local-user) with an asterisk indicating the new account is not yet committed. You can specify additional user account information such as password, first and last names, and so on, and then commit the new account information.

After you create the user account, the account name cannot be changed. You must delete the user account and create a new one.

Example

This example shows how to enter security mode, enter a local user account (simultaneously creating the new account since it does not exist), and then assigning first and last names to the account:

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user* # set firstname test
firepower /security/local-user* # set lastname user
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Related Commands

Command	Description
delete local-user	Deletes an existing local user account.
set expiration	Specifies the date on which the user account expires.
set password	Sets a password for the user account.

create member-port

To create a port-channel member port, use the **create member-port** command. If a member port with the specified ID already exists, the command will fail.

To add or enter a member port, utilize the **enter member-port** command. If the specified member port does not exist, it is created and entered; if the member port exists, it is entered.

You also can use the **scope** form of this command to enter an existing member port to assign or change properties..

To delete an existing member port, use the **delete** form of this command.

create member-port *interface_id*

Syntax Description

interface_id	Identify the interface to be added to this port-channel using one of the following formats: • *slot_id port_id* – The port location in the chassis in terms of slot number and port number. • **Ethernet***slot_id*/*port_id* – The Ethernet port label.

Command Modes

scope eth-uplink/scope fabric a/port-channel

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must create or enter a port-channel before you can use this command.

When you create a new member port, you are automatically entered into member-port mode (eth-uplink/fabric/port-channel/member-port) with an asterisk indicating the new member port is not yet committed.

Example

The following example shows how to create a new port-channel, enable it and add member ports:

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create port-channel	Creates a new EtherChannel (port-channel).

create ntp-server

To create NTP server in FXOS, use the **create ntp-server** command.

create ntp-server

Syntax Description

create ntp-server	This command is used to create an NTP server in FXOS.

Command Modes

scope system/scope services/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command creates the NTP server in FXOS.

Example

The following example shows how to create the NTP server:

```
firepower# scope system;scope services

firepower /system/services # create ntp-server 192.0.2.1
firepower /system/services # commit

firepower /system/services/ntp-server # set
  ntp-sha1-key-id     NTP SHA-1 key id   <========== [Optional] Configure NTP authentication
 key ID
  ntp-sha1-key-string  NTP SHA-1 key string  <========== [Optional] Configure NTP
authentication key string

firepower /system/services/ntp-server # commit
```

Related Commands

Command	Description
show ntp-server	This command displays the NTP server.

create policy (callhome)

To add a new Smart Call Home and Smart Licensing policy, use the **create policy** command. If a policy with the specified name already exists, the command will fail.

To add or edit an IPSec connection, use the **enter policy** command. If the specified policy does not exist, it is created and entered; if the policy exists, it is entered.

You also can use the **scope** form of this command to enter an existing policy to assign or change properties.

To delete an existing policy, use the **delete** form of this command.

create policy *event*
delete policy *event*
enter policy *event*
scope policy *event*

Syntax Description

event	The fault or system event type. See Usage Guidelines below for event options.

Command Modes

scope monitoring/scope callhome/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you create a new Smart Call Home policy, you are automatically entered into callhome/policy mode (monitoring/callhome/policy) with an asterisk indicating the new policy is not yet committed. You can set property values and enable/disable services, and then commit the new policy.

After you create a Smart Call Home policy, the policy name cannot be changed. You must delete the policy and create a new one.

Use this command to create an instance of a policy for an existing type of fault or system event. The available keywords for Call Home policy event types are:

- adaptor-mismatch
- arp-targets-config-error
- association-failed
- configuration-failure
- connectivity-problem
- election-failure
- equipment-degraded
- equipment-disabled
- equipment-inaccessible
- equipment-inoperable

- equipment-offline
- equipment-problem
- equipment-removed
- fru-problem
- health-led-amber
- health-led-amber-blinking
- identity-unestablishable
- inventory-failed
- license-graceperiod-expired
- limit-reached
- link-down
- management-services-failure
- management-services-unresponsive
- memory-error
- mgmtif-down
- ndisc-targets-config-error
- near-max-limit
- port-failed
- power-problem
- psu-insufficient
- psu-mixed-mode
- thermal-problem
- version-incompatible
- vif-ids-mismatch
- voltage-problem

Example

This example shows how to create, enter and enable a Call Home policy instance for link-down events:

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
```

```
firepower /monitoring/callhome/policy #
```

Related Commands

Command	Description
delete policy	Deletes an existing Smart Call Home policy.
set admin-state	Enables or disables the administrative state for a Smart Call Home policy.

create policy (flow control)

To add a new named flow-control policy, use the **create policy** command. If a policy with the specified name already exists, the command will fail.

To add or edit a named flow-control policy, use the **enter policy** command. If the specified policy does not exist, it is created and entered; if the policy exists, it is entered.

You also can use the **scope** form of this command to enter an existing policy to assign or change properties.

To delete an existing policy, use the **delete** form of this command.

create policy *name*
delete policy *name*
enter policy *name*
scope policy *name*

Syntax Description

name	A name to identify the flow-control policy. The name can be from 1 to 16 characters.

Command Modes

scope eth-uplink/scope flow-control/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Flow-control policies determine whether the uplink Ethernet ports in an appliance domain send and receive IEEE 802.3x pause frames when the receive buffer for a port reaches full capacity. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears. For flow control to work between devices, you must enable the corresponding send and receive flow-control parameters for both devices.

The `default` flow-control policy disables send and receive control, and sets the priority to auto-negotiate.

When you create a new flow-control policy, you are automatically entered into flow-control/policy mode (eth-uplink/flow-control/policy) with an asterisk indicating the new policy is not yet committed. You can set policy property values and then commit the new policy.

After you create a flow-control policy, the policy name cannot be changed. You must delete the policy and create a new one.

Example

This example shows how to create and enter a named policy for flow control:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
firepower /eth-uplink/flow-control/policy* # commit-buffer
firepower /eth-uplink/flow-control/policy #
```

Related Commands

Command	Description
delete policy	Deletes an existing flow-control policy.
set	In flow-control/policy mode, sets flow-control policy properties.
show policy	Shows property values for a flow-control policy.

create port-channel

To create an EtherChannel (also known as a port-channel), use the **create port-channel** command. If a port-channel with the specified ID already exists, the command will fail.

To add or enter a port-channel, utilize the **enter port-channel** command. If the specified port-channel does not exist, it is created and entered; if the port-channel exists, it is entered.

You also can use the **scope** form of this command to enter an existing port-channel to assign or change properties..

To delete an existing port-channel, use the **delete** form of this command.

create port-channel*id*

Syntax Description

id	Assign an ID number to this port-channel.

Command Modes

scope eth-uplink/scope fabric a/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

When you create a new port-channel, you are automatically entered into port-channel mode (eth-uplink/fabric/port-channel) with an asterisk indicating the new port-channel is not yet committed. You can set the port-channel parameters and then commit the new port-channel.

After creating a new port-channel, enable it and add member ports.

When the Firepower 4100/9300 chassis creates an EtherChannel, the EtherChannel stays in a **Suspended** state until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state in the following situations:

- The EtherChannel is added as a data or management port for a standalone logical device.
- The EtherChannel is added as a management or CCL port for a logical device that is part of a cluster.
- The EtherChannel is added as a data port for a logical device that is part of a cluster and at least one security module has joined the cluster.

Note that the EtherChannel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the EtherChannel will revert to a **Suspended** state.

Note The Firepower 4100/9300 chassis only supports EtherChannels in Active Link Aggregation Control Protocol (LACP) mode. We suggest setting the connecting switch ports to Active mode for the best compatibility.

Example

The following example shows how to create a new port-channel, enable it and add member ports:

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create member-port	Adds a member port to a port-channel.
set (port-channel)	Sets or changes the parameters for an existing port-channel.

create pre-login-banner

To create a banner that is presented prior to the log-in screen, use the **create pre-login-banner** command. If a pre-login banner already exists, the command will fail.

To add or edit the pre-login banner, use the **enter pre-login-banner** command. If a banner does not exist, it is created and entered; if the banner exists, it is entered.

You also can use the **scope** form of this command to enter an existing pre-login banner to set or clear the message.

To delete an existing banner, use the **delete** form of this command.

create pre-login-banner

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security/scope banner/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you create a new pre-login banner, it is initially blank and you are automatically entered into pre-login-banner mode (security/banner/pre-login-banner) with an asterisk indicating the banner is not yet specified and committed.

Use the **set message** command to enter the pre-login banner text. You must enter `ENDOFBUF` (must be all capital letters) to terminate the banner message.

If a pre-login banner already exists when you enter this command, the command will fail with the message `Error: Managed object already exists.`

Example

This example shows how to create and specify a pre-login banner, then commit and view it:

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center
```

```
firepower /security/banner/pre-login-banner #
```

Related Commands

Command	Description
clear message	Removes the text from an existing pre-login banner; the actual banner object itself is not deleted.
set message	Specifies the text lines to be displayed as the pre-login banner.

create profile

To add a new Smart Call Home and Smart Licensing destination profile, use the **create profile** command. If a profile with the specified name already exists, the command will fail.

To add or edit a destination profile, use the **enter profile** command. If the specified profile does not exist, it is created and entered; if the profile exists, it is entered.

You also can use the **scope** form of this command to enter an existing profile to assign or change properties. If the profile does not exist, the command will fail.

To delete an existing profile, use the **delete** form of this command.

create profile *name*
delete profile *name*
enter profile *name*
scope profile *name*

Syntax Description

name	The name identifying the destination profile.

Command Modes

scope monitoring/scope callhome/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When you create a new Smart Call Home profile, you are automatically entered into callhome/profile mode (monitoring/callhome/profile) with an asterisk indicating the new profile is not yet committed. You can define the profile, and then commit the new profile information.

After you create a Smart Call Home destination profile, the profile name cannot be changed. You must delete the profile and create a new one.

Example

This example shows how to create and enter a Smart Call Home destination profile:

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # enter profile TestProfile
firepower /monitoring/callhome/profile* # commit-buffer
firepower /monitoring/callhome/profile #
```

Related Commands

Command	Description
delete profile	Deletes an existing Smart Call Home destination profile.
set	In monitoring/callhome mode, sets profile properties.

Command	Description
show profile	Lists currently defined Smart Call Home and Smart Licensing profiles; available in monitoring/callhome mode.

create property

To add a new property to a network statistics threshold policy class, use the **create property** command. If a property with the specified name already exists, the command will fail.

To add or edit a statistics threshold property, use the **enter property** command. If the specified property does not exist, it is created and entered; if the property exists, it is entered.

You also can use the **scope** form of this command to enter an existing property to assign or change parameters. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing property, use the **delete** form of this command.

create property *property-name*
delete property *property-name*
enter property *property-name*
scope property *property-name*

Syntax Description

property-name	Specify the desired statistics property. Available properties depend on the current mode and the defined class of statistics. For example, for the `chassis-stats` class in `eth-server` mode, `input-power` and `output-power` options are available. In the `ether-rx-stats` class in `eth-uplink` mode, properties such as `broadcast-packets-delta` and `total-bytes-delta` are available. Use the **create property ?** command to view a list of properties available for the current class of statistics.

Command Modes

scope eth-server/scope stats-threshold-policy/scope class/

scope eth-uplink/scope stats-threshold-policy/scope class/

scope org/scope stats-threshold-policy/scope class/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use classes to place thresholds on specific sets of statistics. Use properties to define particular values and statistics thresholds for a policy class. For example, you might want to define a threshold on a port that raises a fault if the average number of packets dropped exceeds a certain amount. For this class, you would create threshold properties for the Ethernet error statistics class.

You can configure multiple properties for a policy class.

Note There is one default statistics threshold policy each for Ethernet server ports or Ethernet uplink ports. You cannot create additional statistics collection policies and you cannot delete the existing default policies for these components—you can only modify the default policies. However, you can create and delete statistics threshold policies in organization mode (`scope org/`).

Example

This example shows how to scope into the default Ethernet uplink statistics threshold policy, create an error statistics class, create a cyclic redundancy check (CRC) error count property, specify that the normal CRC error count per polling interval is 1000, create an above normal warning threshold of 1250, and then commit the class:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope stats-threshold-policy default
firepower /eth-uplink/stats-threshold-policy # create class ether-error-stats
firepower /eth-uplink/stats-threshold-policy/class* # create property crc-delta
firepower /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
firepower /eth-uplink/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
 1250
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

Related Commands

Command	Description
delete property	Deletes an existing property.
enter property	Enters a class property. If the property does not exist, it is created.
enter property	Enters or creates a property for a class of statistics.
scope property	Enters property mode, where you manage properties for a class of statistics.

create resource-profile

To add a resource profile for use with container instances, use the **create resource-profile** command.

create resource-profile *name*

Syntax Description

name	Sets the name of the profile between 1 and 64 characters. Note that you cannot change the name of this profile after you add it.

Command Modes

scope ssa/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

To specify resource usage per container instance, create one or more resource profiles. When you deploy the logical device/application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

- The minimum number of cores is 6.
- You cannot specify 8 cores due to internal architecture.
- You can assign cores as an even number (6, 10, 12, 14 etc.) up to the maximum.
- The maximum number of cores available depends on the security module/chassis model.

The chassis includes a default resource profile called "Default-Small," which includes the minimum number of cores. You can change the definition of this profile, and even delete it if it is not in use. Note that this profile is created when the chassis reloads and no other profile exists on the system.

You cannot change the resource profile settings if it is currently in use. You must disable any instances that use it, then change the resource profile, and finally reenable the instance. If you resize instances in an established High Availability pair, then you should make all members the same size as soon as possible.

If you change the resource profile settings after you add the threat defense instance to the management center, update the inventory for each unit on the **Devices** > **Device Management** > **Device** > **System** > **Inventory** dialog box.

Example

The following example adds three resource profiles.

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
firepower /ssa/resource-profile* # set cpu-core-count 6
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
firepower /ssa/resource-profile* # set cpu-core-count 10
```

```
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

Related Commands

Command	Description
set cpu-count	Sets the number of CPUs for the resource profile.
set resource-profile-name	Assigned the resource profile to the application instance.
show monitor detail	Shows resource usage for the security module/engine slot.
show resource detail	Shows resource allocation for the application instance.
show resource-profile user-defined	Shows resource profile assignments.

create server (scope ldap)

To create a Lightweight Directory Access Protocol (LDAP) server object, use the **create server** command in security/ldap mode. If a server with the specified name already exists, the command will fail.

To add or edit an LDAP server, use the **enter server** command in security/ldap mode. If the specified server does not exist, it is created and entered; if the server exists, it is entered.

You also can use the **scope** form of this command to enter an existing server to assign or change properties.

To delete an existing server, use the **delete** form of this command.

create server *id*

Syntax Description

id	Provide the server ID, using its host name, fully qualified domain name (FQDN), or IP address (can be an IPv4 or IPv6 address).

Command Modes

scope security/scope ldap/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

If you use a host name or FQDN to specify the server *id*, a DNS server must also be configured.

If SSL is enabled, the server *id* must exactly match a Common Name (CN) in the LDAP server's security certificate.

When you create a new LDAP server, you are automatically entered into security/ldap/server mode with an asterisk indicating the new server is not yet committed. You can configure the server before committing it.

Note The FXOS supports a maximum of 16 LDAP providers.

Example

The following example creates a new LDAP server and commits the transaction:

```
firepower # scope security
firepower # scope ldap
firepower /security/ldap # create server 192.168.100.112
Warning: LDAP server name has to be DNS name in Secure LDAP connection. It has to match the
 LDAP server certificate SAN field.
firepower /security/ldap/server* # commit-buffer
firepower /security/ldap/server #
```

Related Commands

Command	Description
create ldap-group-rule	Creates LDAP provider group rule parameters.

Command	Description
set	In security/ldap/server mode, sets a variety of LDAP server-related parameters, including enable/disable of SSL.

create snmp-trap

To create a Simple Network Management Protocol (SNMP) trap host, use the **create snmp-trap** command. If a trap with the specified name already exists, the command will fail.

To add or edit an SNMP trap, use the **enter snmp-trap** command. If the specified trap does not exist, it is created and entered; if the trap exists, it is entered.

You also can use the **scope** form of this command to enter an existing trap to assign or change properties. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing trap, use the **delete** form of this command.

create snmp-trap *destination*

Syntax Description

destination	Specify the trap destination server, using its host name or IP address (can be an IPv4 or IPv6 address).

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must enable SNMP (**enable snmp**), and create an SNMP community (**set snmp community**), before you create an SNMP trap.

When you create a new SNMP trap, you are automatically entered into monitoring/snmp-trap mode with an asterisk indicating the new trap is not yet committed.

Note You can create up to eight SNMP traps.

Example

The following example creates a new SNMP trap and commits the transaction:

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # commit-buffer
firepower /monitoring/snmp-trap #
```

Related Commands

Command	Description
enable snmp	Enables SNMP.

Command	Description
set snmp	Sets SNMP configuration parameters: community, system contact person responsible for SNMP, and location of the host.

create snmp-user

To create a new SNMPv3 user, utilize the **create snmp-user** command. If a user with the specified name already exists, the command will fail.

To add or edit an SNMP user, utilize the **enter snmp-user** command. If the specified user does not exist, it is created and entered; if the user exists, it is entered.

You also can use the **scope** form of this command to enter an existing user to assign or change properties. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing user, use the **delete** form of this command.

create snmp-user *user_name*

Syntax Description

user_name	Specify the SNMPv3 user name; can be a maximum of 32 alphanumeric characters, and underscore (_), dot (.), at-sign (@), and dash (-).

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must enable SNMP (**enable snmp**), and create an SNMP community (**set snmp community**), before you create an SNMP user.

When you create a new SNMP user, you are asked to create a password for the user. This password must be at least eight characters long; it is not displayed as you enter it.

When you create a new SNMP user, you are automatically entered into monitoring/snmp-user mode with an asterisk indicating the new user is not yet committed.

Example

The following example shows how to create an SNMPv3 user:

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user test1
Password:
firepower /monitoring/snmp-user* # commit-buffer
firepower /monitoring/snmp-user #
```

Related Commands

Command	Description
enable snmp	Enables SNMP.
set snmp	Sets SNMP configuration parameters: community, system contact person responsible for SNMP, and location of the host.

create ssh-server

To create a new SSH host key, use the **create ssh-server** command with the **host-key** keyword.

To delete the existing SSH host key, use the **delete ssh-server** command with the **host-key** keyword.

create ssh-server host-key
create ssh-server host-key

Syntax Description

This command has no additional arguments.

Command Modes

scope system/scope services/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **create** form of this command to generate a new SSH host key.

Use the **delete** form of this command to destroy an existing SSH host key before generating a new one.

Examples

This example shows how to generate a new SSH host key:

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ssh-server host-key
firepower /system/services* # commit-buffer
firepower /system/services #
```

This example shows how to delete the existing SSH host key and confirm its deletion:

```
firepower # scope system
firepower /system # scope services
firepower /system/services # delete ssh-server host-key
firepower /system/services* # commit-buffer
firepower /system/services # show ssh-server host-key
Host Key Size: 2048
Deleted: Yes
firepower /system/services #
```

Related Commands

Command	Description
set ssh-server	Sets the SSH server host key size.
show ssh-server	Shows the SSH server properties.

create stats-threshold-policy

To create a new statistics threshold policy in organization mode, use the **create stats-threshold-policy** command. If a policy with the specified name already exists, the command will fail.

To add or edit an threshold policy in organization mode, use the **enter stats-threshold-policy** command. If the specified policy does not exist, it is created and entered; if the policy exists, it is entered.

You also can use the **scope** form of this command to enter an existing statistics threshold policy in organization mode to assign or change properties. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing policy, use the **delete** form of this command.

create stats-threshold-policy *policy-name*

Syntax Description

policy-name	The name of the new statistics threshold policy. **Note** You cannot create or delete the default statistics threshold policy for Ethernet server ports (`scope eth-server/`) or Ethernet uplink ports (`scope eth-uplink/`).

Command Modes

scope org/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if a specified threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

You can create, enter and delete additional statistics threshold policies in organization mode only. You cannot create additional statistics threshold policies for Ethernet server ports or Ethernet uplink ports, and you cannot delete the existing default policies for those components—you can only modify the default policies.

Note Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Example

This example shows how to scope into organization mode, create a new statistics threshold policy for server and server component statistics, create a threshold policy class for CPU environment statistics, create a CPU temperature property, specify that the normal CPU temperature is 48.5° C, create an above normal warning threshold of 50° C, and commit the entire transaction:

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

Related Commands

Command	Description
create class	Creates a new class of statistics.
create property	Creates a new property for a class of statistics.
create threshold-value	Specifies an above- or below-normal threshold for a class property.
scope org	Enters organizations mode.

create subinterface

To add a subinterface to a physical or EtherChannel interface for use with container instances, use the **create subinterface** command.

create subinterface *id*

Syntax Description

id	Sets the ID between 1 and 4294967295. This ID will be appended to the parent interface ID as *interface_id.subinterface_id*. For example, if you add a subinterface to Ethernet1/1 with the ID of 100, then the subinterface ID will be: Ethernet1/1.100. This ID is not the same as the VLAN ID, although you can set them to match for convenience.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/create port-channel/

Command History

Release	Modification
2.4(1)	Command added.

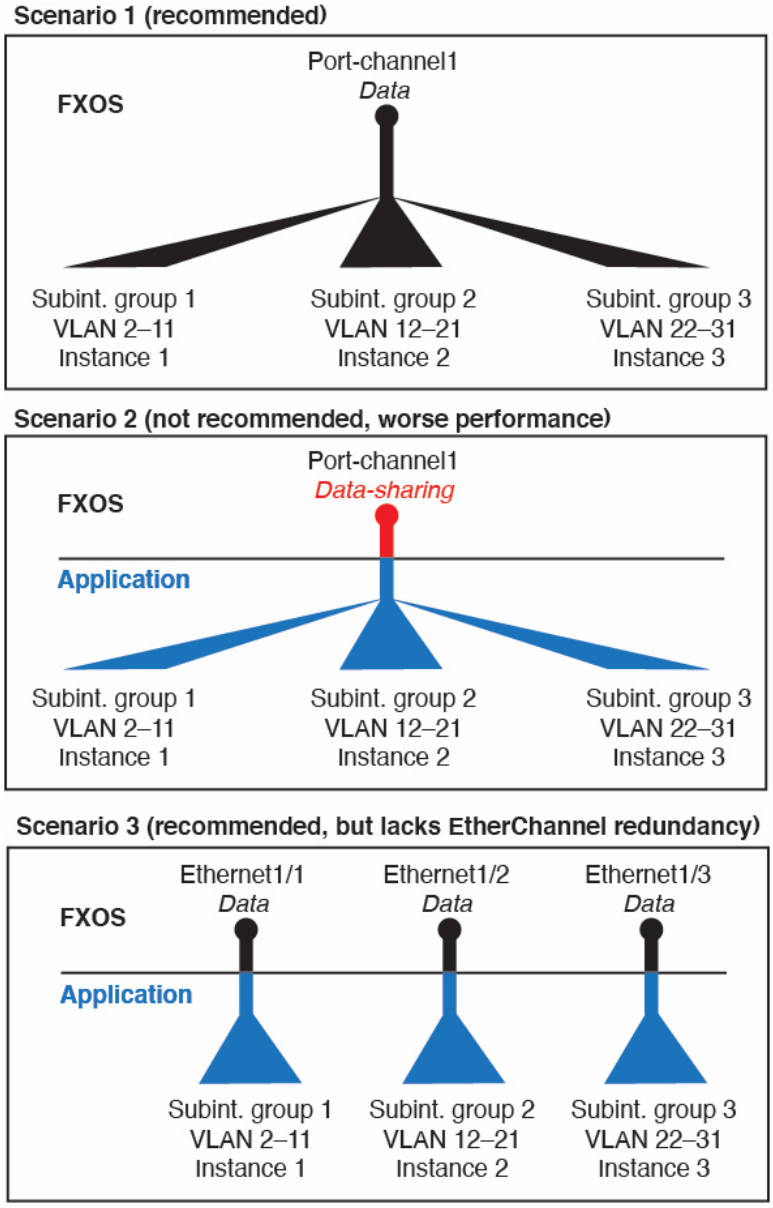
Usage Guidelines

You can add up to 500 subinterfaces to your chassis.

For standalone instances, subinterfaces are supported on data or data-sharing type interfaces only. For multi-instance clustering, you can only add subinterfaces to the Cluster-type interface; subinterfaces on data interfaces are not supported.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on *separate* interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

For native instances, you can create VLAN subinterfaces within the application only. For container instances, you can also create VLAN subinterfaces inside the application on interfaces that do not have FXOS VLAN subinterfaces defined, and these subinterfaces are not subject to the FXOS limit. Choosing in which operating system to create subinterfaces depends on your network deployment and personal preference. For example, to share a subinterface, you must create the subinterface in FXOS. Another scenario that favors FXOS subinterfaces comprises allocating separate subinterface groups on a single interface to multiple instances. For example, you want to use Port-Channel1 with VLAN 2-11 on instance A, VLAN 12-21 on instance B, and VLAN 22-31 on instance C. If you create these subinterfaces within the application, then you would have to share the parent interface in FXOS, which may not be desirable. See the following illustration that shows the three ways you can accomplish this scenario:



You cannot add a subinterface to a physical interface that is currently allocated to a logical device. If other subinterfaces of the parent are allocated, you can add a new subinterface as long as the parent interface itself is not allocated.

Example

The following example creates 3 subinterfaces on Ethernet 1/1, and sets them to be data-sharing interfaces.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
```

```
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Related Commands

Command	Description
create port-channel	Creates an EtherChannel (port channel).
scope interface	Enters the physical interface object.
set port-type	Sets the interface type.
set vlan	Sets the VLAN ID for a subinterface.

create theshold-value

To add an above- or below-normal threshold for a class property, use the **create theshold-value** command. If a threshold with the specified name already exists, the command will fail.

To add or edit a threshold value, use the **enter theshold-value** command. If the specified theshold value does not exist, it is created and entered; if the threshold exists, it is entered.

You also can use the **scope** form of this command to enter an existing theshold value to assign or change parameters. Generally, "scoping into" an object is more convenient than entering it, since the object's name is usually all that is needed, whereas the **enter** form of the command often requires entering all its definition parameters.

To delete an existing theshold value, use the **delete** form of this command.

create theshold-value { **above-normal** | **below-normal** *event_type* }

Syntax Description

above-normal | **below-normal**	Specify the type of threshold: above-normal or below-normal. This determines whether the specified *event_type* is logged when the monitored value (set separately) increases or decreases sufficiently relative to the related normal value (also set separately).
event_type	Specify the type of event logged: • `cleared` • `condition` • `critical` • `info` • `major` • `minor` • `warning`

Command Modes

scope eth-server/scope stats-threshold-policy/scope class/scope property/

scope eth-uplink/scope stats-threshold-policy/scope class/scope property/

scope org/scope stats-threshold-policy/scope class/scope property/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use classes to place thresholds on specific sets of statistics. Use properties to define particular values, including normal values and threshold values, for a policy class. For example, you might want to define a threshold on a port that raises a fault if the average number of packets dropped exceeds a certain amount. For this class, you would create threshold properties for the Ethernet error statistics class.

You can configure multiple properties for a policy class, and you can create multiple threshold values for a property.

Note There is one default statistics threshold policy each for Ethernet server ports or Ethernet uplink ports. You cannot create additional statistics collection policies and you cannot delete the existing default policies for these components—you can only modify the default policies. However, you can create and delete statistics threshold policies in organization mode (`scope org/`).

Example

This example shows how to scope into the default Ethernet server statistics threshold policy class, create a chassis statistics class, create an input power (Watts) property, specify that the normal power level is 8 kW, create an above normal warning threshold of 11 kW, and then commit the class:

```
firepower # scope eth-server
firepower /eth-server # scope stats-threshold-policy default
firepower /eth-server/stats-threshold-policy # create class chassis-stats
firepower /eth-server/stats-threshold-policy/class* # create property input-power
firepower /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
firepower /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
 11000.0
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-server/stats-threshold-policy/class/property/threshold-value #
```

Related Commands

Command	Description
enter class	Enters or creates a class of statistics.
enter property	Enters or creates a property for a class of statistics.
scope stats-threshold-policy	Enters stats-threshold-policy mode, where you manage statistics classes.
set normal-value	Sets the normal value for a class property.

create trustpoint

To add a new trustpoint for validation of a certificate during Internet Key Exchange (IKE) authentication, use the **create trustpoint** command. If a connection with the specified name already exists, the command will fail.

To add or edit a trustpoint, use the **enter trustpoint** command. If the specified trustpoint does not exist, it is created and entered; if the trustpoint exists, it is entered.

You also can use the **scope** form of this command to enter an existing trustpoint to assign or change properties.

To delete an existing trustpoint, use the **delete** form of this command.

create trustpoint *name*
delete trustpoint *name*
enter trustpoint *name*
scope trustpoint *name*

Syntax Description

name	The trustpoint name; can be up to 32 alphanumeric characters.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to identify trustpoints that will be used to validate certificates during Internet Key Exchange (IKE) authentication.

When you create a new trustpoint, you are automatically entered into security/trustpoint mode with an asterisk indicating the new trustpoint is not yet committed. After you create a trustpoint, the name cannot be changed. You must delete the trustpoint and create a new one.

Example

This example shows how to create and enter a trustpoint:

```
firepower # scope security
firepower /security # enter trustpoint tPoint4
firepower /security/trustpoint* #
```

Related Commands

Command	Description
set certchain	Sets certificate information for a trustpoint.
show trustpoint	Shows current trustpoint information.

cycle

To power-cycle a security module/server, use one of the **cycle** commands.

cycle {**cycle-immediate** | **cycle-wait**}

Syntax Description

cycle-immediate	Power-cycles the module immediately.
cycle-wait	The system waits up to five minutes for the application running on the module to shut down before power-cycling the module.

Command Modes

scope service-profile/

Command History

Release	Modification
1.1(1)	This command was introduced.

Example

This example shows how to power-cycle a module after its running application is shut down:

```
firepower # scope service-profile server 1/1
firepower /org/service-profile # cycle cycle-wait
firepower /org/service-profile* # commit-buffer
firepower /org/service-profile #
```

Related Commands

Command	Description
set adminstate	Takes a network module offline or online.

D – R Commands

decommission

To decommission a server, use the **decommission server** command.

decommission server {*id* | *chassis_id* / *blade_id*}

Syntax Description

id	The server identification number. This is a value between 1 and 255.
chassis_id / *blade_id*	The chassis and blade identification numbers in n/n format.

Command Modes

Any command mode

Command History

Release	Modification
2.3(1)	Command added.

Usage Guidelines

Depending on the type of device hosting the module to be decommissioned, identify it using its module ID (4100 series), or the chassis number and module number (9300 devices).

When you decommission a security module, the module object is deleted from the configuration and the module becomes unmanaged. Any logical devices or software running on the module becomes inactive.

Example

This example shows how to decommission a server:

```
firepower# decommission server 1/1
firepower* # commit-buffer
firepower #
```

Related Commands

Command	Description
delete decommissioned	Deletes a decommissioned server.
show server decommissioned	Shows any decommissioned servers.

decommission-secure

To securely decommission a server, use the **decommission-secure server** command.

decommission-secure server *chassis_id*/*blade_id*

Syntax Description

chassis_id/*blade_id*	The chassis and blade identification numbers in n/n format.

Command Modes

Any command mode

Command History

Release	Modification
2.7(1)	Command added.

Usage Guidelines

This command securely erases the specified module. That is, data is not just deleted—the physical storage is "wiped" (completely erased). After a security module is erased, it remains down until acknowledged (similar to a module that is decommissioned).

Example

This example shows how to securely decommission a server:

```
firepower# decommission-secure server 1/2
Warning:
1.Secure decommissioning of the service module may take some time. Please use the CLI command
 'show slot status [n/n] detail' to check for completion.
2.All of the application data on the service module will be lost.  Please back up the
application's configuration files before executing the commit-buffer command.
firepower* #
```

Related Commands

Command	Description
decommission server	Decommissions a server—the module object is deleted from the configuration but the physical storage is not completely erased.
erase secure	Securely erases the specified system component.

delete hw-crypto

To delete a TLS crypto acceleration configuration on a container instance, use the **delete hw-crypto** command. For more information about TLS crypto acceleration, see the *Firepower Management Center Configuration Guide*.

delete hw-crypto

Command Modes

connect module

Command History

Release	Modification
2.7.1	This command was introduced.

Usage Guidelines

This command deletes a TLS crypto acceleration configuration for a container instance. If TLS crypto acceleration is enabled on the container instance, the command disables it before deleting the configuration.

Examples

Following is an example of deleting a TLS crypto acceleration configuration:

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ---------- ------------ ---------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                      Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # delete hw-crypto
/ssa/slot/app-instance* # commit-buffer
```

Related Commands

Command	Description
create hw-crypto	Create a TLS crypto acceleration configuration for a container instance.
scope hw-crypto	Enable or disable TLS crypto acceleration configuration on a container instance.
show hw-crypto	Display the status of TLS crypto acceleration configuration on a container instance.

delete

To delete an existing managed object, use the relevant **delete** command in the appropriate command mode.

delete *object_type name* [*parameters*]

Syntax Description

object_type	The type of object to be deleted. Examples include local user account and organization.
name	The name of the specific object to be deleted.
parameters	(Optional) Any additional properties or parameters needed to identify the object. Refer to the description of the **create** command for the specific object type for more information.

Command Modes

Depends on the type of object being deleted; refer to the description of the **create** command for the specific object type for more information.

Command History

Refer to the description of the **create** command for the specific object type for history information.

Usage Guidelines

Objects are abstract representations of physical components or logical entities that can be managed. For example, the chassis, security modules, network modules, ports, and processors are physical components represented as managed objects, while licenses, user roles, and platform policies are logical entities represented as managed objects.

FXOS provides four general commands for managing objects: **create**, **delete**, **enter**, and **scope**. For example, you can create a local user account, you can delete a local user account, and you can enter a local user account to assign or change properties for that account; you also can "scope into" the local user account to assign or change properties.

Generally, the keywords and options available to each of these object-management commands are the same, so we detail only the **create** version of the various object commands. In other words, for information about the **delete** command for a particular object, refer to the description of the **create** command for that object. For example, refer to create local-user, on page 82 for information related to deleting an existing local user account.

Examples

This example shows how to enter security mode and then delete a local user account:

```
firepower # scope security
firepower /security # delete local-user test_user
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

This example shows how to enter a local-user account and then delete a user role:

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user # delete role aaa
Warning: Change of privileges will terminate active sessions (CLI and Web) of user 'test_user
```

```
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
enter local-user	Adds or edits a local user account.
delete local-user	Deletes an existing local user account.
scope local-user	Enters a existing local user account.

delete decommissioned server

To delete a decommissioned server, use the **delete decommissioned server** command.

delete decommissioned server *vendor model serial_number*

Syntax Description

vendor	The name of the company that manufactured the server; can be no more than 510 characters.
model	The module's model name; can be no more than 510 characters.
serial_number	The module's serial number; can be no more than 510 characters.

Command Modes

Any command mode

Command History

Release	Modification
1.4(1)	Command added.

Example

This example shows how to delete a decommissioned server.

```
FP9300-A # delete decommissioned server Cisco Systems, Inc.
Cisco Firepower 9000 Series Security Module
FLM1949C6J1
FP9300-A* # commit-buffer
```

Related Commands

Command	Description
decommission server	Decommissions a server.

deregister

To remove this Firepower 4100/9300 device from your Cisco Smart Software License account, use the **deregister** command.

deregister

Syntax Description

This command has no arguments or keywords.

Command Modes

License mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Deregistration removes the device from your account, and all license entitlements and certificates on the device are removed. You can use this to free up a license for a new Firepower 4100/9300, or you can remove the device from the Smart Software Manager.

Example

This example shows how to deregister this device.

```
FP9300-A # scope license
FP9300-A /license # deregister
FP9300-A /license #
```

Related Commands

Command	Description
register	Registers a Smart Software Manager account on this Firepower 4100/9300 device.

disable (app-instance)

To disable an existing application instance, use the **disable** command in app-instance mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope ssa/scope slot/scope app-instance

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to disable an application instance without removing it from the system.

Example

This example shows how to display current application instances, including their status, then enter application instance mode and disable an application instance:

```
firepower # scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # show app-instance

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd1       IFT-63     Enabled     Online           6.3.0.12        6.3.0.12
Native                    In Cluster      Slave

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd2       FTD-2      Enabled     Online           6.3.0.12        6.3.0.12
Container   bronze       Not Applicable  None
firepower /ssa/slot # scope app-instance ftd2 FTD-2
firepower /ssa/slot/app-instance # disable
firepower /ssa/slot/app-instance* # commit-buffer
firepower /ssa/slot/app-instance #
```

Related Commands

Command	Description
enable	Enables an existing application instance.
scope app-instance	Enters application mode for a specific application instance.

disable (export-configuration)

To disable an existing export-configuration object, use the **disable** command in export-config mode.

To disable an existing application instance, use the **disable** command in app-instance mode.

To disable an existing export-configuration object, use the **disable** command in export-config mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope system/scope export-config

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In export-configuration mode, use this command to disable an existing export-configuration object without removing it from the system.

Example

This example shows how to scope into an existing exported configuration object and disable it:

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config #disable
firepower /system/export-config* #commit-buffer
```

Related Commands

Command	Description
enable	In export-config mode, enables an existing export-configuration object.
scope export-config	Enters an existing export-configuration object.

disable (interface)

To disable the current interface, use the **disable** command in interface mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope eth-uplink/scope fabric/interface

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to disable the current interface.

Example

This example shows how to disable an interface and confirm its status:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric
firepower /eth-uplink #/fabric # scope interface Ethernet1/5
firepower /eth-uplink/fabric/interface # disable
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface # show

Interface:
    Port Name       Port Type          Admin State Oper State       Allowed Vlan State
Reason
   --------------- ------------------ ----------- ---------------- ------------ ------------

    Ethernet1/5     Data               Disabled     Up               All
firepower /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
enable	Enables the current interface.
set	In interface mode, sets interface configuration parameters.
show interface	Displays interface configuration and status information.

disable (port-channel)

To disable the current port-channel (EtherChannel), use the **disable** command in port-channel mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope eth-uplink/scope fabric/port-channel

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to disable the current port-channel.

Example

This example shows how to disable a port-channel and confirm its status:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric
firepower /eth-uplink #/fabric # scope port-channel 4
firepower /eth-uplink/fabric/port-channel # disable
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel # show

Port Channel:
    Port Channel Id Name             Port Type          Admin State Oper State       Port
Channel Mode Allowed Vlan State Reason
    ---------------- ---------------- ------------------ ----------- ----------------
----------------- ------------ ------------
    4                Port-channel4    Data               Disabled    Failed           Active
            All          Admin config change
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
enable	Enables the current port-channel.
show port-channel	Displays port-channel configuration and status information.

disable (security modes)

To disable Common Criteria mode, or FIPS (Federal Information Processing Standard) mode, use the **disable** command in the security scope.

disable {**cc-mode** | **fips-mode**}

Syntax Description

cc-mode	Use this keyword to disable Common Criteria mode.
fips-mode	Use this keyword to disable FIPS mode.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

A reboot of the system will be required after this command is committed.

Example

This example shows how to enter security mode and disable FIPS mode:

```
firepower # scope security
firepower /security # disable fips-mode
Warning: A reboot of the system is required in order for the system to be
operating in a non-FIPS approved mode.
firepower /security* #
```

Related Commands

Command	Description
enable (security modes)	Enables CC or FIPS mode.
show cc-mode	Shows current Common Criteria mode administrative and operational states.
show fips-mode	Shows current FIPS mode administrative and operational states.

disable reservation

To disable permanent license reservation, use the **disable reservation** command.

disable reservation

Syntax Description

This command has no arguments or keywords.

Command Modes

License (/license) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Enable license reservation before attempting to assign a permanent license to your Firepower 4100/9300 chassis.

Example

This example shows how to enter license mode and disable reservation mode:

```
FP9300-A # scope license
FP9300-A /license # disable reservation
Warning: If you have already generated the authorization code from CSSM
and have not installed it on the device, please abort this command by
issuing discard-buffer and complete the installation.
FP9300-A /license* #
```

Related Commands

Command	Description
enable reservation	Enables permanent license reservation.
show license	Shows current license information.

disable snmp

To disable Simple Network Management Protocol (SNMP) processing on this device, use the **disable snmp** command.

disable snmp

Syntax Description

This command has no arguments or keywords.

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Use this command to disable the SNMP agent on this device. The current SNMP community setting is discarded, the other SNMP configuration settings are not removed.

Example

The following example shows you how to scope into monitoring mode, disable SNMP processing, and then use the **show snmp** command to confirm it is disabled:

```
firepower # scope monitoring
firepower /monitoring # disable snmp
firepower /monitoring* # commit-buffer
firepower /monitoring # show snmp
Name: snmp
    Admin State: Disabled
    Port: 161
    Is Community Set: No
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Related Commands

Command	Description
enable snmp	Enables SNMP.
set snmp	Sets SNMP configuration parameters: community, system contact person responsible for SNMP, and location of the host.
show snmp	Shows current SNMP configuration.

discard-buffer

To cancel pending configuration changes, use the **discard-buffer** command.

discard-buffer

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to cancel and discard all uncommitted configuration changes. While any configuration commands are pending, an asterisk (*) appears before the command prompt. When you enter the **discard-buffer** command, the commands are discarded and the asterisk disappears.

Example

This example shows how to discard pending configuration changes:

```
FP9300-1# scope chassis 1
FP9300-1 /chassis # enable locator-led
FP9300-1 /chassis* # show configuration pending
 scope chassis 1
+    enable locator-led
 exit
FP9300-1 /chassis* # discard-buffer
FP9300-1 /chassis #
```

Related Commands

Command	Description
commit-buffer	Saves or verifies configuration changes.
show configuration pending	Shows uncommitted configuration changes.

download image

To copy an FXOS firmware image to the Firepower 4100/9300 chassis, use the **download image** command in firmware mode.

To copy a logical device software image to the Firepower 4100/9300 chassis, use the **download image** command in application software (/ssa/app-software) mode.

download image {**ftp:** | **scp:** | **sftp:** | **tftp:** | **usbA:** | **usbB:**}

Syntax Description

ftp://*server-ip-addr*/*path*	(Optional) Specifies the URI of an image file to be imported via FTP (File Transfer Protocol).
scp://*username*@*server-ip-addr*/*path*	(Optional) Specifies the URI of an image file to be imported via SCP (Secure Copy Protocol).
sftp://*username*@*server-ip-addr*/*path*	(Optional) Specifies the URI of an image file to be imported via SFTP (SSH File Transfer Protocol or Secure File Transfer Protocol).
tftp://*username*@*server-ip-addr***:***port-num*/*path*	(Optional) Specifies the URI of an image file to be imported via TFTP (Trivial File Transfer Protocol). **Note** TFTP has a file size limitation of 32 MB. Because firmware bundles can be much larger than that, we recommend that you do not use TFTP for firmware downloads.
usbA:/*path*	(Optional) Specifies the path to an image file to be imported from a connected USB Type A device.
usbB:/*path*	(Optional) Specifies the path to an image file to be imported from a connected USB Type B device.

Command Modes

scope firmware/

scope ssa/scope app-software/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Be sure you have the location address and authentication credentials for image file access, as well as the fully qualified name of the file.

FXOS stores firmware images in bootflash on the fabric interconnect.

In firmware mode, you can use the **show package** *image_name* **detail** command to monitor the image download process. The output display does not refresh automatically, so you may have to enter the command multiple times until the task State is “Downloaded.”

In firmware mode, and in application software mode, you can use the **show download-task** command to monitor the image download process. The output display does not refresh automatically, so you may have to enter the command multiple times.

Examples

This example shows how to download a firmware image file using the SCP protocol, and monitor the download progress:

```
FP9300-A# scope firmware
FP9300-A /firmware # download image scp://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
FP9300-A /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
File Name: fxos-k9.1.1.1.119.SPA
Protocol: scp
Server: 192.168.1.1
Userid:
Path:
Downloaded Image Size (KB): 5120
State: Downloading
Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

This example shows how to download a software image file using the SCP protocol, and monitor the download progress:

```
firepower# scope ssa
firepower /ssa # scope app-software
firepower /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
firepower /ssa/app-software # show download-task
Downloads for Application Software:
    File Name                      Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user            Downloaded
```

Related Commands

Command	Description
show download-task	Shows progress of the image file download.
show package	Shows progress of the firmware file download.
verify platform-pack	Verifies a specified FXOS platform image.

enable (app-instance)

To enable an existing application instance, use the **enable** command in app-instance mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope ssa/scope slot/scope app-instance

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to re-enable an application instance that was previously disabled.

Example

This example shows how to display current application instances, including their status, then enter application instance mode and enable a disabled application:

```
firepower # scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # show app-instance

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd1       IFT-63     Enabled     Online           6.3.0.12        6.3.0.12
Native                    In Cluster      Slave

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd2       FTD-2      Disabled    Online           6.3.0.12        6.3.0.12
Container   bronze       Not Applicable  None
firepower /ssa/slot # scope app-instance ftd2 FTD-2
firepower /ssa/slot/app-instance # enable
firepower /ssa/slot/app-instance* # commit-buffer
firepower /ssa/slot/app-instance #
```

Related Commands

Command	Description
disable	In app-instance mode, disables an existing application instance.
scope app-instance	Enters application mode for a specific application instance.

enable (CC and FIPS security modes)

To enable Common Criteria mode, or FIPS (Federal Information Processing Standard) mode, use the **enable** command in the security scope.

enable {**cc-mode** | **fips-mode**}

Syntax Description

cc-mode	Use this keyword to enable Common Criteria mode.
fips-mode	Use this keyword to enable FIPS mode.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Connectivity to one or more services may be denied when this command is committed. Also, a reboot of the system will be required.

Important Prior to FXOS release 2.0.1, the existing SSH host key created during first-time setup of a device was hard-coded to 1024 bits. To comply with FIPS and Common Criteria certification requirements, you must destroy this old host key and generate a new one (see create ssh-server, on page 107 for information about creating and deleting SSH host keys). If you do not perform these additional steps, you will not be able to connect to the Supervisor using SSH after the device has rebooted with Common Criteria mode enabled. If you performed initial setup using FXOS 2.0.1 or later, you do not have to generate a new host key.

Example

This example shows how to enter security mode and enable FIPS mode:

```
firepower # scope security
firepower /security # enable fips-mode
Warning: Connectivity to one or more services may be denied when committed.
Please consult the product's FIPS Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
FIPS approved mode.

firepower /security* #
```

Related Commands

Command	Description
disable (security modes)	Disables CC or FIPS mode.
show cc-mode	Shows current Common Criteria mode administrative and operational states.

Command	Description
show fips-mode	Shows current FIPS mode administrative and operational states.

enable (export-configuration)

To re-enable an existing export-configuration object, use the **enable** command in export-config mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope system/scope export-config

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to re-enable a previously backed-up export-configuration object, prior to exporting the configuration again. The current system configuration is exported according to the object parameters when you issue the **commit-buffer** command.

Example

This example shows how to scope into a previously exported configuration object, enable it, initiate configuration back-up, and then confirm the export is underway:

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config #enable
firepower /system/export-config* #commit-buffer
firepower /system/export-config #show

Export Configuration Task:
    Hostname   User       Protocol Admin State Status    Description
    ---------- ---------- -------- ----------- --------- -----------
    192.168.1.2
               user1      Scp      Enabled     Exporting
```

Related Commands

Command	Description
disable	Disables an existing export-configuration object.
scope export-config	Enters an existing export-configuration object.

enable (interface)

To enable the current interface, use the **enable** command in interface mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope eth-uplink/scope fabric/interface

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to enable or re-enable an interface.

Example

This example shows how to enable an interface and confirm its status:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric
firepower /eth-uplink #/fabric # scope interface Ethernet1/5
firepower /eth-uplink/fabric/interface # enable
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface # show

Interface:
    Port Name       Port Type          Admin State Oper State       Allowed Vlan State
Reason
   --------------- ------------------ ----------- ---------------- ------------ ------------

    Ethernet1/5     Data               Enabled     Up               All
firepower /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
disable	Disables the current interface.
set	In interface mode, sets interface configuration parameters.
show interface	Displays interface configuration and status information.

enable (port-channel)

To enable the current port-channel (EtherChannel), use the **enable** command in port-channel mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

scope eth-uplink/scope fabric/port-channel

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to enable or re-enable a port-channel.

Example

The following example shows how to create a new port-channel, enable it and add member ports:

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create member-port	Adds a member port to a port-channel.
disable	Disables the current port-channel.
set (port-channel)	Sets or changes the parameters for an existing port-channel.
show port-channel	Displays port-channel configuration and status information.

enable reservation

To enable permanent license reservation, use the **enable reservation** command.

enable reservation

Syntax Description

This command has no arguments or keywords.

Command Modes

License (/license) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Enable license reservation before attempting to assign a permanent license to your Firepower 4100/9300 chassis.

Example

This example shows how to enter license mode and enable reservation mode:

```
FP9300-A # scope license
FP9300-A /license # enable reservation
FP9300-A /license #
```

Related Commands

Command	Description
disable reservation	Disables permanent license reservation.
show license	Shows current license information.

enable snmp

To enable Simple Network Management Protocol (SNMP) processing on this device, use the **enable snmp** command.

enable snmp

Syntax Description

This command has no arguments or keywords.

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

After using this command to enable the SNMP agent on this device, you can create an SNMP community, and create SNMP users and traps.

Example

The following example shows you how to scope into monitoring mode and enable SNMP processing:

```
firepower # scope monitoring
firepower /monitoring # enable snmp
firepower /monitoring* # commit-buffer
firepower /monitoring #
```

Related Commands

Command	Description
disable snmp	Disables SNMP.
set snmp	Sets SNMP configuration parameters: community, system contact person responsible for SNMP, and location of the host.
show snmp	Shows current SNMP configuration.

end

To return to the EXEC (top level) mode of the CLI, use the **end** command.

end

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to return to the highest-level mode of the CLI from service profile mode.

```
FP9300-A # scope org Test
FP9300-A /org # scope service-profile Sample
FP9300-A /org/service-profile # end
FP9300-A #
```

Related Commands

Command	Description
top	Enters top level mode from any mode.

enter

To enter a managed object, use the relevant **enter** command in the appropriate command mode. Generally, if the specified object does not exist, it is created.

enter *object_type name* [*parameters*]

Syntax Description

object_type	The type of object to be entered. Examples include local user account and organization.
name	The name of the specific object to be entered.
parameters	(Optional) Any additional properties or parameters needed to identify the object. Refer to the description of the **create** command for the specific object type for more information.

Command Modes

Depends on the type of object being entered; refer to the description of the **create** command for the specific object type for more information.

Command History

Refer to the description of the **create** command for the specific object type for history information.

Usage Guidelines

Objects are abstract representations of physical components or logical entities that can be managed. For example, the chassis, security modules, network modules, ports, and processors are physical components represented as managed objects, while licenses, user roles, and platform policies are logical entities represented as managed objects.

FXOS provides four general commands for managing objects: **create**, **delete**, **enter**, and **scope**. For example, you can create a local user account, you can delete a local user account, and you can enter a local user account to assign or change properties for that account; you also can "scope into" the local user account to assign or change properties.

Generally, the keywords and options available to each of these object-management commands are the same, so we detail only the **create** version of the various object commands. In other words, for information about the **delete** command for a particular object, refer to the description of the **create** command for that object. For example, refer to create local-user, on page 82 for information related to entering an existing local user account.

Example

This example shows how to enter security mode, enter a local user account and display account details:

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user # show detail
Local User test_user:
    First Name: test
    Last Name: user
    Email: test_user@testuser.com
    Phone:
    Expiration: Never
    Password: ****
```

```
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
firepower /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
enter local-user	Adds or edits a local user account.
delete local-user	Deletes an existing local user account.
scope local-user	Enters a existing local user account.

erase

To erase all user configuration from the applicance, or to securely erase elements of the applicance, use the **erase** command.

erase { **configuration** | **secure** { **chassis** | **security_modulesupervisor** } }

Syntax Description

configuration	Use this keyword to erase all user-configuration information on the chassis, restoring it to its original factory-default configuration.
secure	Use this option to securely erase the specified appliance component: • **chassis** – Use this keyword to securely erase the chassis. • **security_module** *module_id* – Use this option to securely erase the specified module. • **supervisor** – Use this keyword to securely erase the chassis supervisor.

Command Modes

connect local-mgmt/

Command History

Release	Modification
2.0.1	Command added.
2.7(1)	**secure** option added.

Usage Guidelines

The **erase configuration** command removes all user-configuration information on the chassis, restoring it to its original factory-default configuration.

The **erase secure** command securely erases the specified appliance component. That is, data is not just deleted—the physical storage is "wiped" (completely erased). This is important when transferring or returning the appliance as hardware storage components do not retain residual data or stubs.

Note The device reboots during secure erase, which means SSH connections are terminated. Therefore, we recommend performing secure erase over a serial console-port connection.

Examples

This example shows how to erase all user-configuration information on the chassis, restoring it to its original factory-default configuration:

```
firepower# connect local-mgmt
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):
```

This example shows how to securely erase security module 2:

```
firepower# connect local-mgmt
firepower# erase secure security_module 2
The physical storages in security module will be securely erased.
ALL DATA AND IMAGES WILL BE LOST AND CANNOT BE RECOVERED!
After the erase the module will reboot and need to be re-initialized.
DO NOT POWER OFF THE DEVICE IF YOU DECIDE TO PERFORM THIS TASK!
Are you sure? (yes/no):
```

Related Commands

Command	Description
decommission-secure	Securely erases the specified module.

exit

To exit the current CLI session and disconnect from the device, or to exit from a connected object mode and return to the EXEC level, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode.

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to exit the current top level CLI session and disconnect from this device.

```
FP9300-A # exit
```

This example shows how to enter and exit a local management connection.

```
FP9300-A # connect local-mgmt
FP9300-A(local-mgmt) # exit
FP9300-A #
```

Related Commands

Command	Description
connect	Connects to another managed object.
end	Returns to the highest level mode of the CLI.

export-config

To export the current system configuration to a remote server as an XML file, use the **export-config** command.

export-config {*URL* **disabled** | **enabled**}

Syntax Description

URL	Provide the full path to the remote system, including user-account name, transport protocol and file name, for the exported XML image file. The following transport protocols can be used: • **ftp:***//username@hostname/path/image_name* • **scp:***//username@hostname/path/image_name* • **sftp:***//username@hostname/path/image_name* • **tftp:***//username@hostname/path/image_name*
disabled	Disables the policy administrative state; configuration file is not exported.
enabled	Enables the policy administrative state; configuration file is exported immediately.

Command Modes

scope system/

Command History

Release	Modification
1.1.3	Command added.

Usage Guidelines

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Please note the following:

- Beginning with FXOS 2.6.1, you must specify a key for use when encrypting sensitive information such as passwords and other secret keys during configuration export, and you must have specified it before you attempt to export the configuration.

  Also, the same key used during export must be set on the target system when you import an exported configuration, unless the file was exported from an FXOS release prior to 2.6.1, in which case the target system will not check the encryption key and will allow the import.

- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.

- Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.

- To avoid overwriting existing back-up files, please be sure to change the file name in the export operation, or copy the existing file to another location.

Depending on the transport protocol, and the remote server configuration, you may have to enter the user's password for connection.

When you export a new configuration file, you are automatically entered into export-config mode (system/export-config) with an asterisk indicating the new file has not yet been exported; enter **commit-buffer** to begin the process.

Example

This example shows how to export an XML file containing logical device and platform configuration settings to a remote server:

```
firepower # scope system
firepower /system # export-config scp://user1@192.168.1.2:/export/cfg-backup.xml enabled
Password:
firepower /system/export-config* # commit-buffer
firepower /system/export-config #
```

Related Commands

Command	Description
cfg-export-policy	Configures a configuration export policy.
import-config	Copies a previously exported XML configuration file to this appliance.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

generate password

To generate a fixed-length random password with or without special characters, use the **generate password** command.

generate password *password*

Syntax Description

password	The password to be used by the user when logging in.

Command Modes

scope security

Command History

Release	Modification
2.10(1)	Command added.

Usage Guidelines

You can generate a fixed-length random password with or without special characters.

Example

This example shows how to enter security mode, generate a fixed-length random password with or without special characters:

```
firepower # scope security
firepower # create local-user admin2
firepower /security/local-user #

firepower /security/local-user # generate password
  8-127  Password length

firepower /security/local-user # generate password 10 with
  with-special-char     With Special Char
  without-special-char  Without Special Char

firepower /security/local-user # generate password 10 with-special-char
@!D4%vlwCN
```

Related Commands

Command	Description
set password	Sets a password for the user account.

import-config

To import a previously exported XML configuration file, use the **import-config** command.

import-config { *URL* **disabled** | **enabled** }

Syntax Description

URL	Provide the full path to the remote system, including transport protocol and file name, for the XML image file to be imported. The following transport protocols can be used: • **ftp:***//username@hostname/path/image_name* • **scp:***//username@hostname/path/image_name* • **sftp:***//username@hostname/path/image_name* • **tftp:***//username@hostname/path/image_name*
disabled	Disables the policy administrative state; configuration file is not imported.
enabled	Enables the policy administrative state; configuration file is imported immediately.

Command Modes

scope system/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Please note the following:

- Beginning with FXOS 2.6.1, you must specify a key for use when encrypting sensitive information such as passwords and other secret keys during configuration export, and you must have specified it before you attempt to export the configuration.

  Also, the same key used during export must be set on the target system when you import an exported configuration, unless the file was exported from an FXOS release prior to 2.6.1, in which case the target system will not check the encryption key and will allow the import.

- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.

- Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.

- When you import a configuration to a Firepower 4100/9300 chassis, all existing configuration on the chassis (including any logical devices) will be deleted and completely replaced by the configuration contained in the import file.
- We recommend that you only import a configuration file to the same Firepower 4100/9300 chassis from which the configuration was exported.
- The platform software version of the Firepower 4100/9300 chassis to which you are importing should be the same version as when the export was taken. If not, the import operation is not guaranteed to be successful. We recommend that you export a back-up configuration whenever the Firepower 4100/9300 chassis is upgraded or downgraded.
- The Firepower 4100/9300 chassis to which you are importing must have the same Network Modules installed in the same slots as when the export was taken.
- The Firepower 4100/9300 chassis to which you are importing must have the correct software application images installed for any logical devices defined in the export file that your are importing.
- If the configuration file being imported contains a logical device whose application has an End-User License Agreement (EULA), the EULA for that application must be accepted on the Firepower 4100/9300 chassis before importing the configuration or the operation will fail.

Depending on the transport protocol, and the remote server configuration, you may have to enter the remote user password for connection.

You can check the import status and follow its progress by entering the **show fsm status** command; see the following example. You may have to enter the command multiple times as the task progresses.

Example

This example shows how to import an XML file containing logical device and platform configuration settings from a remote server:

```
firepower # scope system
firepower /system # import-config scp://user1@192.168.1.2:/export/cfg-backup.xml enabled
Password:
Warning: After configuration import any changes on the breakout port configuration will
cause the system to reboot
firepower /system* # commit-buffer
firepower /system # show fsm status

Hostname: 192.168.1.2

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Import Wait For Switch
        Previous Status: Import Config Breakout
        Timestamp: 2016-01-03T15:45:03.963
        Try: 0
        Progress (%): 97
        Current Task: updating breakout port
configuration(FSM-STAGE:sam:dme:MgmtImporterImport:configBreakout)
```

Related Commands

Command	Description
cfg-export-policy	Configures an export policy.
export-config	Exports the current system configuration to a remote server as an XML file
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

install

To install a reservation authorization code, use the **install** command.

install *code*

Syntax Description

code	The reservation authorization code acquired from the Smart Software Manager.

Command Modes

Reservation (/license/reservation) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you have already generated the authorization code, you must install it.

Example

This example shows how to install a reservation authorization code:

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation # install <code>
FP9300-A /license/reservation* #
```

Related Commands

Command	Description
request universal	Generates a reservation request code.
show license	Shows current license information.

install firmware

To install a previously downloaded firmware upgrade package, use the **install firmware** command.

install firmware pack-version *version_number*

Syntax Description

pack-version *version_number*	Specifies the version of the firmware package to install. **Note** The package *version_number* is not the image file name (although it is usually part of the file name). You can use the **show** command to determine the package *version_number* .

Command Modes

Firmware installation mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You must have administrator privileges to use this command. The upgrade installation process typically takes between 20 and 30 minutes, and the system will reboot during the process.

Before initiating installation, review the current critical/major faults and back up the current configuration.

Upgrade is a two-step process: verification of the package, followed by installation. You are asked at the beginning of each step if you want to proceed. If you enter **no** at either prompt, the process is terminated.

You can use the **show detail** command to monitor the installation process.

Example

This example shows how to install a previously downloaded firmware upgrade package:

```
FP9300-A# scope firmware
FP9300-A /firmware # scope firmware-install
FP9300-A /firmware/firmware-install # install firmware pack-version 1.0.16
Verifying FXOS firmware package 1.0.16. Verification could take several minutes.
Do you want to proceed? (yes/no):yes

FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA : Upgrade from 1.04 to 1.05
This operation upgrades SUP firmware on Security Platform.
Here is the checklist of things that are recommended before starting the install operation
(1) Review current critical/major faults
(2) Initiate a configuration backup
Attention:
   The system will be reboot to upgrade the SUP firmware.
   The upgrade operation will take several minutes to complete.
   PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.
Do you want to proceed? (yes/no):yes
Upgrading FXOS SUP firmware software package version 1.0.10
command executed
```

Related Commands

Command	Description
scope firmware-install	Enters firmware-installation mode.
show download-task	Shows information about firmware-package downloads.
show (firmware-install)	In firmware-installation mode, shows firmware package information.

install platform

To upgrade firmware and software on the security platform components, use the **install platform** command.

install platform platform-vers *version_number*

Syntax Description

platform-vers *version_number*	Specifies the version of the platform package to install.

Command Modes

Auto install (/firmware/auto-install) mode

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

You must have administrator privileges to use this command. The upgrade process typically takes between 20 and 30 minutes.

Before initiating installation, review the current critical/major faults and back up the current configuration.

You can use the **show fsm status expand** command in auto-install mode to monitor the installation process.

To complete the upgrade installation process, you must acknowledge the pending reboot of the primary fabric-interconnect.

Example

This example shows how to install a platform upgrade package:

```
FP9300-A# scope firmware
FP9300-A /firmware # scope auto-install
FP9300-A /firmware/auto-install # install platform platform-vers 2.3(1.51)
The currently installed FXOS platform software package is 2.2(2.19)

INFO: There is no service impact to install this FXOS platform software 2.3(1.51)

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
Do you want to proceed? (yes/no):
```

Related Commands

Command	Description
download image	Downloads an FXOS software image to the Firepower 4100/9300 chassis.
show validate-task	Displays the status of the image verification process.

mgmt-port (connect local-mgmt)

To display and configure the administrative status os the management port information, use the **mgmt-port** command.

mgmt-port

Syntax Description

mgmt-port	Displays management port information.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays management port information.

Example

This example shows how to view management port information:

```
firepower#
firepower# connect local-mgmt...

firepower(local-mgmt)#mgmt-port
  <CR>
  no-shut  Management port up  <====== Administratively enable the chassis management
interface.
  shut     Management port down <====== Administratively disable/shutdown the chassis
management interface.
```

ping (connect local-mgmt)

To test basic network connectivity by pinging another device on the network with its IPv4 address, use the **ping** command.

ping {*hostname* | *IPv4_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**packet-size** *bytes*]

Syntax Description

hostname | *IPv4_address*	The host name or IP address of the network device to be contacted. The maximum number of characters allowed for the host name is 510.
count *number_packets*	(Optional) The number of ping packets to be sent. The range is 1 to 2147483647 packets.
deadline *seconds*	(Optional) The maximum time to continue sending packets when no response packets are received; pinging is terminated after this amount of time. The range is 1 to 60 seconds.
interval *seconds*	(Optional) The interval in seconds between ping packets. The range is 1 to 60 seconds; the default is 1 second.
packet-size *bytes*	(Optional) The number of data bytes to be added to the ping packet. The range is 1 to 65468 bytes. The default is 56 bytes, which results in a 64-byte packet when added to the 8-byte ICMP header.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to test basic IP connectivity from the chassis management interface to an external network by sending ICMP echo request packets to a specified host.

Example

This example shows how to connect to the local management shell and then ping another device on the network twelve times:

```
firepower# connect local-mgmt
firepower(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
```

```
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms
firepower(local-mgmt)#
```

Related Commands

Command	Description
ping6	Tests basic network connectivity by pinging another device on the network with its IPv6 address.
traceroute	Traces the route to a specified destination (IPv4 address).

ping6 (connect local-mgmt)

To ping another device on the network using its IPv6 address, use the **ping6** command.

ping6 {*hostname* | *IPv6_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**mtu-hint** {**do** | **dont** | **want**}] | [**packet-size** *bytes*]

Syntax Description

hostname | *IPv6_address*	The host name or IP address of the network device to be contacted. The maximum number of characters allowed for the host name is 510.
count *number_packets*	(Optional) The number of ping packets to be sent. The range is 1 to 2147483647 packets.
deadline *seconds*	(Optional) The maximum time to continue sending packets when no response packets are received; pinging is terminated after this amount of time. The range is 1 to 60 seconds.
interval *seconds*	(Optional) The interval in seconds between ping packets. The range is 1 to 60 seconds; the default is 1 second.
mtu-hint {**do** | **dont** | **want**}	(Optional) Path MTU discovery strategy; hint may be: • **do**—Prohibits fragmentation, even for local packets; sets a do-not-fragment (DF) flag. • **dont**—Prohibits fragmentation; however, does not set DF flag. • **want**—Performs PMTU discovery, fragments locally when packet size is large.
packet-size *bytes*	(Optional) The number of data bytes to be added to the ping packet. The range is 1 to 65468 bytes. The default is 56 bytes, which results in a 64-byte packet when added to the 8-byte ICMP header.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(4)	Command added.

Usage Guidelines

Use this command to test basic IPv6 connectivity from the chassis management interface to an external network by sending ICMP echo request packets to a specified host.

Example

This example shows how to connect to the local management shell and then ping another device on the network twelve times:

```
firepower# connect local-mgmt
firepower(local-mgmt)# ping6 2001:DB8:0:ABCD::1 count 12
```

```
PING 2001:DB8:0:ABCD::1 (2001:DB8:0:ABCD::1) from 2001:DB8:1::1 eth0: 56(84) bytes of data.
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=12 ttl=61 time=0.261 ms

--- 2001:DB8:0:ABCD::1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms
firepower(local-mgmt)#
```

Related Commands

Command	Description
ping	Tests basic network connectivity by pinging another device on the network with its IPv4 address.
traceroute6	Traces the route to a specified destination (IPv6 address).

power

To power a module off or on, use the **power** command.

power {**down** [**soft-followed-by-hard** | **soft-shut-down**] | **up**}

Syntax Description

soft-followed-by-hard	(Optional) You can use this keyword to "gracefully" power down the module, waiting up to 45 minutes for the SSP operating system to shut down, after which the module is powered down regardless of the OS shut-down state.
soft-shut-down	(Optional) You can use this keyword to gracefully power down the module, with the system waiting indefinitely for the SSP operating system to shut down. The module is powered down only after the SSP OS is successfully shut down.

Command Modes

Service profile mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you do not include one of the optional keywords with the **power down** command, the module is powered down immediately, without gracefully shutting down the module's operating system.

We recommend backing up the module configuration before powering down.

Example

This example shows how to enter service profile mode and then power down the module with a soft shut-down:

```
FP9300-A # scope service-profile server 1/1
FP9300-A /org/service-profile # power down soft-shut-down
FP9300-A /org/service-profile* # commit-buffer
FP9300-A /org/service-profile #
```

Related Commands

Command	Description
shutdown	Shuts down the device.

reboot

To restart the chassis or the fabric-interconnect, use the **reboot** command.

```
(local-mgmt)# reboot
```

```
/chassis # reboot [no-prompt|reason]
```

Syntax Description

	In local management mode, this command has no arguments or keywords.
no-prompt	(Optional) In chassis mode, you can use this keyword to initiate reboot immediately. Otherwise, a **commit-buffer** is required to initiate reboot.
reason	(Optional) In chassis mode, you can enter a text string to be appended to the reboot log; can be up to 510 characters.

Command Modes

Chassis mode

Local management mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

We recommend backing up the system configuration before rebooting.

In local management mode, this command has no keywords or options.

Note We recommend using this command in chassis mode, as it performs a "graceful" system shut-down and restart.

Examples

This example shows how to enter a local management shell and reboot the system:

```
FP9300-A # connect local-mgmt
FP9300-A (local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no)::yes
nohup: ignoring input and appending output to `nohup.out'

Broadcast message from root (Fri Apr 13 17:12:49 2018):

All shells being terminated due to system /sbin/reboot
```

This example shows how to enter chassis mode and reboot the system:

```
FP9300-A # scope chassis 1
FP9300-A /chassis # reboot
This command will reboot the chassis when committed
```

```
FP9300-A /chassis* # commit-buffer
Starting chassis shutdown. Monitor progress with the command "show fsm status"
System is safe to power off after "System halted." message is seen
FP9300-A /chassis #
Broadcast message from root@DOC-FP9300-A (Fri Apr 13 16:27:04 2018):

All shells being terminated due to system /sbin/shutdown
```

Related Commands

Command	Description
shutdown	Shuts down the device.

reinstall

To modify bootstrap settings for a logical device, reinstall the application instance using the **reinstall** command.

reinstall

Syntax Description

This command has no arguments or keywords.

Command Modes

scope slot/scope app/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can modify bootstrap settings for a logical device. You can reinstall the application instance using those new settings or save the changes and reinstall the application instance using those new settings at a later time.

Example

This example shows how to enter license/licdebug mode and manually renew the Smart Software ID certificate and license entitlement.

```
FP9300-A # scope slot 2
FP9300-A /slot # scope app-instance asa cluster1
FP9300-A /slot/app-instance # reinstall app
FP9300-A /slot/app-instance # Do you want to reinstall the app now [Y/N]? Y
…
```

Related Commands

Command	Description
register	Modifies bootstrap settings for a logical device to restart the application instance.

register

To register a Smart Software Manager account on this Firepower 4100/9300 device, use the **register** command.

register idtoken *id_token*

Syntax Description

id_token	The registration token acquired from the Smart Software Manager Satellite.

Command Modes

License (/license) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Request and copy the registration token from the Smart Software Manager or the Smart Software Manager Satellite. See the *Cisco Smart Software Manager Satellite User Guide* for more information.

Example

This example shows how to register this device.

```
FP9300-A # scope license
FP9300-A /license # register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
V8N3R0dXM1Z0NjWkdpR214eFZhMldBOS9CVnNEYnVKM1
FP9300-A /license #
```

Related Commands

Command	Description
deregister	Deregistering removes the device from your account; all license entitlements and certificates on the device are removed.

reinitialize

To completely reformat a module, use the **reinitialize** command.

reinitialize

Syntax Description

This command has no arguments or keywords.

Command Modes

Slot mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Reinitializing a module completely erases all stored application data. Please back up all running configuration files before issuing the **commit-buffer** command.

Example

This example shows how to reinitialize the module in slot 2.

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot # reinitialize
Warning: Reinitializing blade takes a few minutes. All the application data on blade will
get lost. Please backup application running config files before commit-buffer.
FP9300-A /ssa/slot* #
```

Related Commands

Command	Description
decommission	Decommissions a server.

remove server

To remove a previously decommissioned server from the device inventory, use the **remove server** command.

remove server {*id* | *chassis_id*/*blade_id*}

Syntax Description

id	The slot number. The range of valid values is 1 to 255.
chassis_id/*blade_id*	The server chassis and blade numbers, in n/n format. **Note** The chassis number is always **1**.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

When using this command in chassis mode, you need to specify only the slot ID number.

Example

This example shows how to remove a decommissioned server:

```
FP9300-A# remove server 1/1
FP9300-A* # commit-buffer
FP9300-A#
```

Related Commands

Command	Description
decommission server	Decommissions a server.
show server decommissioned	Shows decommissioned server(s).

renew

To manually renew the Smart Software registration certificate and update the entitlements on all security modules, use the **renew** command.

renew

Syntax Description

This command has no arguments or keywords.

Command Modes

License debug (/license/licdebug) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, the ID certificate is automatically renewed every six months, and the license entitlement is renewed every 30 days. You might manually renew the registration for either of these items if you have a limited window for Internet access, for example, or if you make any licensing changes in the Smart Software Manager.

Example

This example shows how to enter license/licdebug mode and manually renew the Smart Software ID certificate and license entitlement.

```
FP9300-A # scope license
FP9300-A /license # scope licdebug
FP9300-A /license/licdebug # renew
FP9300-A /license/licdebug #
```

Related Commands

Command	Description
register	Registers a Smart Software Manager account on this Firepower 4100/9300 device.

reset-password

To enforce the user to change the user password, use the **reset-password** command.

reset-password *password*

Syntax Description

password	The password to be used by the user when logging in.

Command Modes

scope security

Command History

Release	Modification
2.10(1)	Command added.

Usage Guidelines

You can enforce the user to change the user password at the next login.

Example

This example shows how to enter security mode and then reset the password:

```
firepower# scope security
firepower# create local-user admin2
firepower /security/local-user # set
  account-status  Account status
  email           Email
  expiration      User account expiration
  firstname       FirstName
  lastname        LastName
  password        Password
  phone           Phone
  reset-password  Change password at next login

firepower /security/local-user # set reset-password
  no   No
  yes  Yes
```

Related Commands

Command	Description
set password	Sets a password for the user account.
generate password	Generates a password for the user account.

request universal

To generate a reservation request code, use the **request universal** command.

request universal

Syntax Description

This command has no arguments or keywords.

Command Modes

Reservation (/license/reservation) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Before you begin, you must purchase the permanent licenses so they are available in Smart Software Manager. Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it.

Enable license reservation before attempting to assign a permanent license to your Firepower 4100/9300 chassis.

After issuing this command, use **show license resvcode** to view the generated reservation request, authorization and return codes.

Example

This example shows how to generate a reservation request code and view the generated codes:

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation # request universal
FP9300-A /license/reservation # show license resvcode
Warning : generating the reservation code takes a few seconds.
Please run the 'show license resvcode' again if the code is not available.
Reservation request code :
<empty>
Reservation authorization code :
<empty>
Reservation return code :
<empty>
```

Related Commands

Command	Description
enable reservation	Enables permanent license reservation.
show license	Shows current license information.

restart

To modify bootstrap settings for a logical device, restart the application instance using the **restart** command.

restart

Syntax Description

This command has no arguments or keywords.

Command Modes

scope slot/scope app/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can modify bootstrap settings for a logical device. You can then immediately restart the application instance using those new settings or save the changes and restart the application instance using those new settings at a later time.

This example shows how to restart an application:

```
FP9300-A # scope slot 2
FP9300-A /slot # scope app-instance asa cluster1
FP9300-A /slot /app-instance # restart app
FP9300-A /slot /app-instance # Do you want to restart now [Y/N]? Y
```

Related Commands

Command	Description
reinstall	Reinstalls the application instance.

return

To generate a permanent license return code, use the **return** command.

return [*code*]

Syntax Description

code	(Optional) A license code acquired from the Smart Software Manager.

Command Modes

Reservation (/license/reservation) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you no longer need a permanent license, you must officially return it to the Smart Software Manager. If you do not, the license stays in an in-use state and cannot be used elsewhere.

When you enter this command, the Firepower 4100/9300 chassis immediately becomes unlicensed and moves to the Evaluation state.

To complete the return, go to https://software.cisco.com/#SmartLicensing-Inventory, locate your Firepower 4100/9300 chassis using its universal device identifier (UDI), and then remove the product instance.

Example

This example shows how to return a permanent license:

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation # return
FP9300-A /license/reservation #
```

Related Commands

Command	Description
show license udi	Shows the FXOS universal device identifier (UDI) so you can find your FXOS instance in the Smart Software Manager.

PART II

S Commands

scope Commands

scope

To “scope into” (enter) an existing managed object, use the relevant **scope** command in the appropriate command mode.

scope *object_type* *name* [*parameters*]

Syntax Description

object_type	The type of object to be entered. Examples include local user account and organization.
name	The name of the specific object to be entered.
parameters	(Optional) Any additional properties or parameters needed to identify the object. With this command, the *name* is generally sufficient to identify an object. Refer to the description of the **create** command for the specific object type for more information.

Command Modes

Depends on the type of object being scoped into; refer to the description of the **create** command for the specific object type for more information.

Command History

Refer to the description of the **create** command for the specific object type for history information.

Usage Guidelines

Objects are abstract representations of physical components or logical entities that can be managed. For example, the chassis, security modules, network modules, ports, and processors are physical components represented as managed objects, while licenses, user roles, and platform policies are logical entities represented as managed objects.

FXOS provides four general commands for managing objects: **create**, **delete**, **enter**, and **scope**. For example, you can create a local user account, you can delete a local user account, and you can enter a local user account to assign or change properties for that account; you also can “scope into” the local user account to assign or change properties.

Generally, the keywords and options available to each of these object-management commands are the same, so we detail only the **create** version of the various object commands. In other words, for information about the **delete** command for a particular object, refer to the description of the **create** command for that object. For example, refer to create local-user, on page 82 for information related to scoping into an existing local user account.

Example

This example shows how to enter security mode, scope into a local user account and display account details:

```
firepower # scope security
firepower /security # scope local-user test_user
firepower /security/local-user # show detail
Local User test_user:
    First Name: test
    Last Name: user
    Email: test_user@testuser.com
    Phone:
```

```
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
firepower /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
enter local-user	Adds or edits a local user account.
delete local-user	Deletes an existing local user account.

scope adapter

To enter adapter mode, use the **scope adapter** command.

scope adapter {*rack_server*/*id* | *chassis*/*server*/*id*}

Syntax Description

rack_server/*id*	The adapter location specified using the rack-server and adapter IDs entered in n/n format.
chassis/*server*/*id*	The adapter location specified using the chassis, server and adapter IDs entered in n/n/n format. **Note** The chassis ID is always **1**.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In adapter mode, you can activate or update a firmware version, view a variety of adapter-specific data, and scope into host and external Ethernet interfaces.

Example

This example shows how to enter adapter mode using the chassis, server and adapter IDs:

```
firepower# scope adapter 1/1/1
firepower /chassis/server/adapter #
```

Related Commands

Command	Description
connect adapter	Connects to the command shell for a specific adapter.
scope chassis	Enters chassis mode.

scope app-software

To enter application software mode, use the **scope app-software** command.

scope app-software

Syntax Description

This command has no arguments or keywords.

Command Modes

scope ssa/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use the **download image** command in application software mode to copy a logical device software image to the Firepower 4100/9300 chassis.

Example

This example shows how to enter application software mode:

```
firepower# scope ssa
firepower /ssa # scope app-software
firepower /ssa/app-software #
```

Related Commands

Command	Description
download image	Copies a logical device software image to the Firepower 4100/9300 chassis.
show download-task	Shows progress of the image file download.

scope auto-install

To enter automatic installation mode for infrastructure updates, use the **scope auto-install** command.

scope auto-install

Syntax Description

This command has no arguments or keywords.

Command Modes

Firmware (/firmware) mode

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

None

Example

This example shows how to enter firmware mode and then auto-install mode:

```
FP9300-A# scope firmware
FP9300-A /firmware # scope auto-install
FP9300-A /firmware/auto-install #
```

Related Commands

Command	Description
install platform	Upgrades UCS Infra components (UCSM, FI and IOM) to infra version specified.

scope auto-macpool

To manage the MAC address pool for container instance interface , use the **scope auto-macpool** command.

scope auto-macpool

Syntax Description

This command has no arguments or keywords.

Command Modes

scope ssa/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

The FXOS chassis automatically generates MAC addresses for container instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the application, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the application.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.

Note Even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

The FXOS chassis generates the MAC address using the following format:

A2*xx*.*yyzz*.*zzzz*

Where *xx*.*yy* is a user-defined prefix or a system-defined prefix, and *zz*.*zzzz* is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xxyy*) to match the chassis native form:

A2**4D**.**00***zz*.*zzzz*

For a prefix of 1009 (03F1), the MAC address is:

A2**F1**.**03***zz*.*zzzz*

Example

This example shows how to enter mac-pool mode:

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool #
```

Related Commands

Command	Description
scope ssa	Enters ssa mode.
set prefix	Sets the MAC address prefix.
show mac-address	Shows the assigned MAC addresses.

scope banner

To enter banner-management mode, use the **scope banner** command.

scope banner

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In this mode, you can manage the banner presented by the appliance prior to user log-in.

Example

This example shows you how to enter banner mode and view the current pre-login banner:

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # show pre-login-banner

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner #
```

Related Commands

Command	Description
clear message	Removes the text from an existing pre-login banner; the actual banner object itself is not deleted.
create pre-login-banner	Creates a banner to be presented prior to the log-in screen; the banner object is initially empty.
set message	Adds or replaces the lines of text presented as the pre-login banner.

scope cabling

To enter cabling mode, use the **scope cabling** command.

scope cabling

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can access fabric mode from cabling mode, where you can view and manage port breakouts.

Example

This example shows how to enter cabling mode:

```
FP9300-A # scope cabling
FP9300-A /cabling #
```

Related Commands

Command	Description
scope fabric-interconnect	Enter fabric interconnect mode.

scope callhome

To enter callhome mode, use the **scope callhome** command.

scope callhome

Syntax Description

This command has no arguments or keywords.

Command Modes

Monitoring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter callhome mode from monitoring mode:

```
FP9300-A#scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
show callhome	Shows Call Home configuration and status information.

scope card

To enter adminstrative mode for a specific fabric card, use the **scope card** command.

scope card *card_ID*

Syntax Description

card_ID	The fabric card's numeric identifier.

Command Modes

scope fabric-interconnect/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In card mode, you can take the fabric card offline or online.

Example

This example shows how to enter card mode and view available commands:

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # scope card 2
firepower /fabric-interconnect/card # ?
  acknowledge  Acknowledge
  scope        Changes the current mode
  set          Set property values
  show         Show system information

firepower /fabric-interconnect/card #
```

Command	Description
set adminstate	Takes a fabric card offline or online.

scope cfg-export-policy

To enter the configuration export policy, use the **scope cfg-export-policy** command.

scope cfg-export-policy*name*

Syntax Description

name	The name of the configuration export policy to enter. You cannot create or delete a configuration export policy. You can only configure the existing default policy; enter **default** as the policy name.

Command Modes

scope org/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

You cannot create or delete a configuration export policy; you can only configure the existing default policy.

Example

This example shows how to enter the configuration export policy and view the details of its current settings:

```
firepower # scope org
firepower /org # scope cfg-export-policy default
firepower /org/cfg-export-policy # show detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Ftp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Daily
    Port: Default
    Current Task:
firepower /org/cfg-export-policy #
```

Related Commands

Command	Description
export-config	Exports the current system configuration to a remote server as an XML file; creates an export-configuration object.
import-config	Copies a previously exported XML configuration file to this appliance.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

scope cfg-export-reminder

To enter the configuration-export reminder object, use the **scope cfg-export-reminder** command.

scope cfg-export-reminder

Syntax Description

This command has no arguments or keywords.

Command Modes

scope org/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

You cannot create or delete a configuration-export reminder object; you can only configure the existing reminder object.

Example

This example shows how to enter the configuration-export reminder object and view its current settings:

```
firepower # scope org
firepower /org # scope cfg-export-reminder
firepower /org/cfg-export-reminder # show

Config Export Reminder:
    Config Export Reminder (Days): 30
    AdminState: Enable
firepower /org/cfg-export-reminder #
```

Related Commands

Command	Description
import-config	Copies a previously exported XML configuration file to this appliance.
scope cfg-export-policy	Enters the configuration export policy.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

scope chassis

To enter chassis mode, use the **scope chassis** command.

scope chassis *chassis_id*

Syntax Description

chassis_id	Chassis identification number. This value is always **1**.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter chassis mode:

```
firepower# scope chassis 1
firepower /chassis #
```

Related Commands

Command	Description
show chassis	Shows chassis information.

scope cloud-connector

To enter cloud connector mode, use the **scope cloud-connector** command.

scope cloud-connector

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter cloud connector mode:

```
FP9300-A # scope cloud-connector
FP9300-A /cloud-connector #
```

Related Commands

Command	Description
show cloud-connector	Shows cloud connector configuration information.

scope default-auth

To enter default authentication mode, use the **scope default-auth** command.

scope default-auth

Syntax Description

This command has no arguments or keywords.

Command Modes

Security mode

Authentication domain (/security/auth-domain)

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

Use the **set** commands in this mode to configure default authentication parameters such as authentication service and session timeout values.

An authentication domain must be created prior to using this command to enter the default authentication mode for a domain.

Example

This example shows how to enter security mode and then default authentication mode:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set realm	Sets the default authentication service.
show	Shows default authentication settings.

scope environment-features

To enter environment features in configuration mode, use the **scope environment-features** command.

scope environment-features

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter environment features mode:

```
firepower # scope system
firepower /system # scope environment-features
firepower /system/environment-features # show
```

Related Commands

Command	Description
show	Shows the information about the domain environment features.

scope eth-uplink

To enter Ethernet uplink mode, use the **scope eth-uplink** command.

scope eth-uplink

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter Ethernet uplink mode:

```
firepower#scope eth-uplink
firepower /eth-uplink #
```

Related Commands

Command	Description
show	Shows Ethernet uplink information.

scope export-config

To enter an existing export-configuration object, use the **scope export-config** command.

scope export-config*hostname*

Syntax Description

hostname	The identifier of the export-configuration object; this is the name or IP address of the remote server on which the configuration was backed up.

Command Modes

scope system/

Command History

Release	Modification
1.1.(1)	Command added.

Usage Guidelines

An export-configuration object is created when you issue an **export-config** command to back up the current logical device and platform configuration, and **scope export-config** is used to enter the object and edit its parameters—there are no **create** or **enter** commands associated with export-configuration objects. There is a **delete** command available which you can use to delete an export-configuration object.

Example

This example shows how to scope into a previously exported configuration object:

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config #
```

Related Commands

Command	Description
cfg-export-policy	Configures a configuration export policy.
delete export-config	Deletes an existing export-configuration object.
export-config	Exports the current system configuration to a remote server as an XML file; creates an export-configuration object.

scope fabric

To enter fabric mode, use the **scope fabric** command.

scope fabric [**a**]

Syntax Description		
	a	Specifies Fabric A. There is only one fabric on Firepower devices. Use of this keyword is optional.

Command Modes

scope eth-uplink/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In fabric mode, you can manage interfaces, port-channels, aggregate interfaces, and VLANs.

Example

This example shows how to enter fabric mode:

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric #
```

Related Commands

Command	Description
show interface	In fabric mode, lists information for all device interfaces.
show port-channel	In fabric mode, lists information and status for all port-channels.

scope fabric-interconnect

To enter fabric interconnect mode, use the **scope fabric-interconnect** command.

scope fabric-interconnect a

Syntax Description

a	Specifies Fabric A. There is only one fabric on Firepower devices.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter fabric interconnect mode:

```
firepower# scope fabric-interconnect a
firepower /fabric-interconnect #
```

Related Commands

Command	Description
show fabric-interconnect	Shows fabric interconnect information.

scope fan-module

To enter a specific fan module, use the **scope fan-module** command in chassis mode.

scope fan-module {**1** *module_id*}

Syntax Description

tray_id	The *tray_id* is always **1**.
module_id	Identifies the specific fan module to enter; value can be 1 through 8.

Command Modes

scope chassis/

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to scope into fan-module mode:

```
firepower# scope chassis
firepower /chassis # scope fan-module 1 2
firepower /chassis/fan-module #
```

Related Commands

Command	Description
scope fan	Scopes into a specific fan.

scope faulty-policy

To enter the fault policy for one of the functional areas of the system, use the **scope faulty policy** command.

scope faulty policy

Syntax Description

This command has no arguments or keywords.

Command Modes

scope monitoring

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Related Commands

Command	Description
Show detail	Shows the detailed fault policy information of the system.
Set Ack-action	Specifies acknowledge action.
Set Clear-action	Specifies Clear action.
Set Clear-interval	Specifies Clear interval.
Set Flap-interval	Specifies Flap interval.
Set Retention-interval	Specifies Retention interval. (dd:hh:mm:ss)

scope firmware

To enter firmware mode, use the **scope firmware** command.

scope firmware

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter firmware mode:

```
firepower# scope firmware
firepower /firmware #
```

Related Commands

Command	Description
show server firmware	Shows server firmware information.
show server version	Shows server firmware version.

scope firmware-install

To enter firmware-installation mode, use the **scope firmware-install** command.

scope firmware-install

Syntax Description

This command has no arguments or keywords.

Command Modes

Firmware mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this scope to update system firmware with a previously downloaded firmware package.

Example

This example shows how to enter firmware-installation mode:

```
FP9300-A# scope firmware
FP9300-A /firmware # scope firmware-install
FP9300-A /firmware-install #
```

Related Commands

Command	Description
download image	Downloads a firmware package.
install firmware	Installs a firmware package.

scope flow-control

To enter flow-control mode, use the **scope flow-control** command.

scope flow-control

Syntax Description

This command has no arguments or keywords.

Command Modes

scope eth-uplink/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Flow-control policies determine whether the Ethernet ports send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears. For flow control to work between devices, you must enable the corresponding send and receive flow-control parameters for both devices.

The `default` flow-control policy disables send and receive control, and sets the priority to auto-negotiate.

Example

The following example shows how to scope into flow-control mode and view current policy information:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # show policy detail
Flowctrl policy:
    Name: default
    receive: Off
    send: Off
    Prio: Auto
firepower /eth-uplink/flow-control #
```

Related Commands

Command	Description
create policy	Adds a new named flow-control policy.
set	In flow-control/policy mode, sets flow-control policy properties.
show policy	Shows property values for a flow-control policy.

scope health monitoring policy

Memory usage metrics

Memory stats collected can be enabled or disabled using the cli under **scope** 'stats-collection-memory'. By default, it is enabled.

Also fault threshold can be set for all memory monitoring faults. The threshold-value can range between 50-99. By default, it is set at 95%.

scope health-monitoring-policy
scope stats-collection-memory
enable | disable
set fault-threshold <threshold-value>

Command Modes

Monitoring mode

Command History

Release	Modification
2.11.1	This command was introduced.

Usage Guidelines

This command enables or disables memory monitoring and also changes the fault threshold value for all the memory monitoring faults.

Example

```
firepower# scope monitoring
firepower /monitoring # scope health-monitoring-policy
firepower /monitoring/health-monitoring-policy # scope stats-collection-memory
firepower /monitoring/health-monitoring-policy/stats-collection-memory # set fault-threshold
 75
firepower /monitoring/health-monitoring-policy/stats-collection-memory # disable
firepower /monitoring/health-monitoring-policy/stats-collection-memory* # commit-buffer
firepower /monitoring/health-monitoring-policy/stats-collection-memory # show
Memory stats collection policy:
Admin State Fault-Threshold (%)
-----------
Disabled 75
firepower /monitoring/health-monitoring-policy/stats-collection-memory # show detail
Admin State: Disabled
Fault Threshold (%): 75
```

CPU usage metrics

CPU stats collected can be enabled or disabled using the cli under scope 'stats-collection-cpu'. By default it is enabled.

Also fault threshold can be set for all cpu monitoring faults. The threshold-value can range between 50-99. By default it is set at 90%.

scope health-monitoring-policy
scope stats-collection-cpu

enable | disable
set fault-threshold <threshold-value>

Command Modes

Monitoring mode

Command History

Release	Modification
2.11.1	This command was introduced.

Usage Guidelines

This command enables or disables CPU monitoring and also changes the fault threshold value for all the CPU monitoring faults.

Example

```
firepower# scope monitoring
firepower /monitoring # scope health-monitoring-policy
firepower /monitoring/health-monitoring-policy # scope stats-collection-cpu
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # set fault-threshold
85
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # enable
firepower /monitoring/health-monitoring-policy/stats-collection-cpu * # commit-buffer
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # show
Cpu stats collection policy:
Admin State Fault-Threshold (%)
-----------
Enabled 85
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # show detail
Admin State: Enabled
Fault Threshold (%): 85
```

scope hw-crypto

To enable or disable TLS crypto acceleration on a container instance, use the **scope hw-crypto** command. For more information about TLS crypto acceleration, see the *Management Center Configuration Guide*.

scope hw-crypto

Command Modes

connect module

Command History

Release	Modification
2.7.1	This command was introduced.

Usage Guidelines

This command enables or disables TLS crypto acceleration on a container instance.

Examples

Following is an example of enabling TLS crypto acceleration on a container instance:

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ---------- ---------------- --------------- ---------------
 ----------- ---------- ------------ --------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                    Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # scope hw-crypto
/ssa/slot/app-instance/hw-crypto # set admin-state enabled
 /ssa/slot/app-instance/hw-crypto* # commit-buffer
```

Following is an example of disabling TLS crypto acceleration on a container instance:

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ---------- ---------------- --------------- ---------------
 ----------- ---------- ------------ --------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                    Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
 /ssa/slot/app-instance # scope hw-crypto
 /ssa/slot/app-instance/hw-crypto # set admin-state disbled
 /ssa/slot/app-instance/hw-crypto* # commit-buffer
```

Related Commands

Command	Description
create hw-crypto	Create a TLS crypto acceleration configuration for a container instance.
delete hw-crypto	Delete a TLS crypto acceleration configuration for a container instance.
show hw-crypto	Displays status of TLS crypto acceleration configuration on a container instance.

scope import-config

To enter an existing import-configuration object, use the **scope import-config** command.

scope import-config*hostname*

Syntax Description

hostname	The identifier of the import-configuration object; this is the name or IP address of the remote server on which the configuration resides.

Command History

Release	Modification
1.1.(1)	Command added.

Usage Guidelines

An export-configuration object is created when you issue an **export-config** command to back up the current logical device and platform configuration; the **import-config** command is used to import a previously exported configuration file, while simultaneously creating an import-configuration object.

You can use **scope import-config** to enter an existing import-configuration object and edit its parameters. There are no **create** or **enter** commands associated with import-configuration objects. There is a **delete** command available which you can use to delete an import-configuration object.

Example

This example shows how to scope into an existing import-configuration object:

```
firepower # scope system
firepower /system # scope import-config 192.168.1.2
firepower /system/import-config #
```

Related Commands

Command	Description
cfg-export-policy	Configures a configuration export policy.
delete import-config	Deletes an existing import-configuration object.
import-config	Imports previously exported system configuration from a remote server; creates an import-configuration object.

scope info-policy

To enter system info policies in configuration mode, use the **scope info-policy** command.

scope info-policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter info policy mode:

```
firepower # scope system
firepower /system # scope info-policy
firepower /system/info-policy #
```

Related Commands

Command	Description
Show	Shows the information about the info policies.

scope interface

To enter configuration mode for a specific interface, use the **scope interface** command.

scope interface {**Ethernet***slot_id*/*port_id* | *slot_num*}

Syntax Description

Ethernet*slot_id*/*port_id*	The Ethernet port name.
slot_num	The interface slot number.

Command Modes

scope eth-uplink/scope fabric a/

Command History

Release	Modification
1.1.1	Command added.

Example

This example shows how to scope into configuration mode for a specific interface and view its current configuration:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/5
firepower /eth-uplink/fabric/interface # show detail

Interface:
    Port Name: Ethernet1/5
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:
firepower /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
disable	Disables the current interface.

Command	Description
enable	Enables the current interface.
set	In interface mode, sets interface configuration parameters.
show interface	Displays interface configuration and status information.

scope ipsec

To enter IPSec mode, use the **scope ipsec** command.

scope ipsec

Syntax Description

This command has no arguments or keywords.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter IPSec mode:

```
FP9300-A# scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec #
```

Related Commands

Command	Description
show connection	Shows information about the IPSec connection.

scope ipv6-config

To enter IPv6 configuration mode, where you can configure the fabric's IPv6 management interface, use the **scope ipv6-config** command in fabric interconnect mode.

scope ipv6-config

Syntax Description

This command has no arguments or keywords.

Command Modes

Fabric interconnect mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter IPv6 configuration mode:

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config #
```

Related Commands

Command	Description
show ipv6-if	Shows IPv6 management-interface information.

scope ldap

To enter Lightweight Directory Access Protocol (LDAP) configuration mode, use the **scope ldap** command.

scope ldap

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter LDAP mode:

```
firepower# scope security
firepower /security # scope ldap
firepower /security/ldap #
```

Related Commands

Command	Description
create ldap-group-rule	Creates LDAP provider group rule parameters.
create server	In security/ldap mode, creates a new LDAP server.
set	In security/ldap/server mode, sets a variety of LDAP server-related parameters, including enable/disable of SSL.

scope licdebug

To enter license debug mode from license mode, use the **scope licdebug** command.

scope licdebug

Syntax Description

This command has no arguments or keywords.

Command Modes

License mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter license debug mode from license mode:

```
FP9300-A # scope license
FP9300-A /license # scope licdebug
FP9300-A /license/licdebug #
```

Related Commands

Command	Description
scope license	Enters license mode.

scope license

To enter license mode, use the **scope license** command.

scope license

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter license mode from EXEC level:

```
FP9300-A# scope license
FP9300-A /license #
```

Related Commands

Command	Description
show license	Shows the usage of some or all license packages.

scope mem-leak-logging

To enable the stack trace state to detect the memory leak of each UCSM process, use the **scope mem-leak-logging** command.

scope mem-leak-logging *set*

Syntax Description

set	set memory leak logging for the knob.

Command Modes

scope monitoring/scope sysdebug

Usage Guidelines

Use this command to enable the memory leak feature to debug memory leak issues for the specified process and to enable the stack trace.

Example

This example shows how to set the knob state and enable stack trace mode:

```
Firepower#scope monitoring
Firepower /monitoring# scope sysdebug
Firepower /monitoring/sysdebug#  scope mem-leak-logging
Firepower /monitoring/sysdebug/mem-leak-logging # set  ?
  appag-log               Memory Leak Logging for appAG
  bladeag-log            Memory Leak Logging for bladeAG
  dcosag-log             Memory Leak Logging for dcosAG
  dme-log                 Memory Leak Logging for dme
  extvmmag-log       Memory Leak Logging for extvmmAG
  hostagentag-log     Memory Leak Logging for hostagentAG
  licenseag-log         Memory Leak Logging for licenseAG
  nicag-log               Memory Leak Logging for nicAG
  portag-log              Memory Leak Logging for portAG
  rsdag-log                Memory Leak Logging for rsdAG
  serviceorchag-log   Memory Leak Logging for serviceOrchAG
  sessionmgrag-log   Memory Leak Logging for sessionmgrAG
  statsag-log              Memory Leak Logging for statsAG
  svcmonag-log        Memory Leak Logging for svcmonAG
Firepower /monitoring/sysdebug/mem-leak-logging # set statsag-log enable ?
  <CR>
  stacktrace  Stacktrace for Memory Leak Report
Firepower /monitoring/sysdebug/mem-leak-logging # set statsag-log enable stacktrace ?
  off  Off
  on   On
```

scope monitoring

To enter system monitoring mode, use the **scope monitoring** command.

scope monitoring

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter monitoring mode:

```
FP9300-A#scope monitoring
FP9300-A /monitoring #
```

Related Commands

Command	Description
show server status	Shows information about the status of a server.

scope network-features

To enter network features in configuration mode, use the **scope network-features** command.

scope network-features

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter network features mode:

```
firepower # scope system
firepower /system # scope network-features
firepower /system/network-features* # show
```

Related Commands

Command	Description
show	Shows the information about the domain network features.

scope org

To enter organization mode, use the **scope org** command.

scope org [*org_name*]

Syntax Description

org_name	(Optional) The organization name.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter organization mode:

```
FP9300-A# scope org org100
FP9300-A /org #
```

Related Commands

Command	Description
show org	Lists currently defined organizations.

scope packet-capture

To enter packet capture mode, use the **scope packet-capture** command.

scope packet-capture

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter packet capture mode:

```
FP9300-A#scope packet-capture
FP9300-A /monitoring #
```

Related Commands

Command	Description
traceroute	Traces the route to another device on the network.

scope password-profile

To enter password profile mode, use the **scope password-profile** command.

scope password-profile

Syntax Description

This command has no arguments or keywords.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter password profile security mode:

```
FP9300-A # scope security
FP9300-A /security # scope password-profile
FP9300-A /security/password-profile #
```

Related Commands

Command	Description
show password-profile	Shows password-profile information.

scope profile

To enter Smart Call Home and Smart Licensing destination profile mode, use the **scope profile** command.

scope profile *profile_name*

Syntax Description

profile_name	The name of the destination profile; between 1 and 16 characters.

Command Modes

Callhome (/monitoring/callhome/) mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter profile mode and then display the destination configured for the profile:

```
FP9300-A /monitoring/callhome # scope profile SLProfile
FP9300-A /monitoring/callhome/profile # show destination

Destination:
    Name       Transport Protocol Email or HTTP/HTTPS URL Address
    ---------- ------------------ ------------------------------
    SLDest     Https
https://tools.cisco.com/its/service/oddce/services/DDCEService
FP9300-A /monitoring/callhome/profile #
```

Related Commands

Command	Description
show profile	Lists currently defined Smart Call Home and Smart Licensing profiles; available in monitoring/callhome mode.

scope radius

To enter Remote Authentication Dial-In User Service (RADIUS) configuration mode, use the **scope radius** command.

scope radius

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter radius mode:

```
firepower # scope security
firepower /security # scope radius
firepower /security/radius #
```

scope reservation

To enter license reservation mode, use the **scope reservation** command.

scope reservation

Syntax Description

This command has no arguments or keywords.

Command Modes

License mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter reservation mode from license mode:

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation #
```

Related Commands

Command	Description
request universal	Generates a reservation request code.
show license	Shows the usage of some or all license packages.

scope security

To enter security mode, use the **scope security** command.

scope security

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter security mode:

```
firepower# scope security
firepower /security #
```

Related Commands

Command	Description
show security	In EXEC mode, shows information about current security policies.

scope server

To enter server mode, use the **scope server** command.

scope server {*id* | *dynamic_uuid* | *chassis_id* / *blade_id*}

Syntax Description

id	The server ID; an integer between 1 and 255.
dynamic_uid	The server's dynamic universally unique ID (UUID).
chassis_id / *blade_id*	The server specified using chassis and blade IDs; must be entered in n/n format. **Note** The chassis ID is always **1**.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter server mode:

```
FP9300-A# scope server 1/1
FP9300-A /chassis/server #
```

Related Commands

Command	Description
show server adapter	Shows information about the network adapters in a server.
show server identity	Shows identity information about a server.

scope server-features

To enter server features in configuration mode, use the **scope server-features** command.

scope server-features

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter server features mode:

```
firepower # scope system
firepower /system # scope server-features
firepower /system/server-features* # show
```

Related Commands

Command	Description
show	Shows the information about the domain server features.

scope service-profile

To enter service profile mode, use the **scope service-profile** command.

scope service-profile {*dynamic_uuid* | *org* | *server*}

Syntax Description

dynamic_uuid	The dynamic UUID of the service profile.
org	The name of the organization for which the service profile was created; between 1 and 16 characters.
server	The ID of the server for which the service profile was created.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

To use this command with the *org* option, an organization and a service profile for that organization must already exist.

To use this command with the *server* option, the server can be specified with its server ID, or the chassis ID and blade ID (n/n format). The chassis ID is always **1**.

Example

This example shows how to enter service profile mode:

```
firepower # scope service-profile server 1/1
firepower /org/service-profile #
```

Related Commands

Command	Description
show service-profile	Shows service-profile information.

scope services

To enter system services in configuration mode, use the **scope services** command.

scope services

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter services mode:

```
firepower # scope system
firepower /system # scope services
firepower /system/services #
```

Related Commands

Command	Description
Show	Shows the information about the services.

scope slot

To enter slot mode for a specific SSP module, use the **scope slot** command.

scope slot *slot_ID*

Syntax Description

slot_ID / *id*	Identifies the module slot. For the FP9300, this value can be 1, 2, or 3; on the FP4100, this value is 1.

Command Modes

scope ssa/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In slot mode, you can update the application image on the logical device.

Example

This example shows how to enter slot mode:

```
firepower# scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot #
```

Related Commands

Command	Description
show security	Shows security information.

scope ssa

To enter security services (ssa) mode, use the **scope ssa** command.

scope ssa

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter ssa mode:

```
FP9300-A# scope ssa
FP9300-A /ssa #
```

Related Commands

Command	Description
show security	Shows security information.

scope stats-collection-policy

To enter the statistics collection policy for one of the functional areas of your system, use the **scope stats-collection-policy** command.

scope stats-collection-policy *policy-area*

Syntax Description

policy-area	The specific collection policy area: • `Adapter` – statistics related to the adapters. • `Chassis` – statistics related to the blade chassis. • `FEX` – statistics related to configured Fabric Extender(s). • `Host` – this policy is a placeholder for future support. • `Port` – statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports. • `Server` – statistics related to servers.

Command Modes

scope monitoring/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Statistics can be collected and reported for several of the functional areas of your system.

Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides sufficient data to calculate and report minimum, maximum, and average values.

Note There is one default statistics collection policy for each of the functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Example

This example shows how to enter the statistics collection policy for ports, set the collection interval to one minute, set the reporting interval to 30 minutes, and then commit the transaction:

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
```

```
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Related Commands

Command	Description
set collection-interval	Specifies how frequently statistics are collected.
set reporting-interval	Specifies how frequently statistics are reported.

scope stats-threshold-policy

To enter the statistics threshold policy for one of the components of your system, use the **scope stats-threshold-policy** command.

scope stats-threshold-policy *policy-name*

Syntax Description

policy-name	The name of the specific threshold policy to enter. You cannot create or delete a statistics threshold policy for Ethernet server ports or Ethernet uplink ports. You can only configure the existing default policy, so for these policies, enter **default** as the *policy-name*.

Command Modes

scope eth-server/

scope eth-uplink/

scope org/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if a specified threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

There is one default statistics threshold policy each for Ethernet server ports or Ethernet uplink ports. You cannot create additional statistics threshold policies and you cannot delete the existing default policies for these components—you can only modify the default policies.

However, you can create and delete statistics threshold policies in organization mode (`scope org/`). See the **create stats-threshold-policy** command for more information.

Note Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Examples

This example shows how to scope into the default Ethernet uplink statistics threshold policy, create an error statistics class, create a cyclic redundancy check (CRC) error count property, specify that the normal CRC error count per polling interval is 1000, create an above normal warning threshold of 1250, and then commit the class:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope stats-threshold-policy default
firepower /eth-uplink/stats-threshold-policy # create class ether-error-stats
```

```
firepower /eth-uplink/stats-threshold-policy/class* # create property crc-delta
firepower /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
firepower /eth-uplink/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
 1250
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

This example shows how to scope into organization mode, create a new statistics threshold policy for server and server component statistics, create a threshold policy class for CPU environment statistics, create a CPU temperature property, specify that the normal CPU temperature is 48.5° C, create an above normal warning threshold of 50° C, and commit the entire transaction:

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

Related Commands

Command	Description
create class	Creates a new class of statistics.
create property	Creates a new property for a class of statistics.
create threshold-value	Specifies an above- or below-normal threshold for a class property.
scope stats-collection-policy	Enters stats-collection-policy mode, where you manage statistics collection and reporting intervals.

scope storage-features

To enter storage features in configuration mode, use the **scope storage-features** command.

scope storage-features

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter storage features mode:

```
firepower # scope system
firepower /system # scope environment-features
firepower /system/environment-features # show
```

Related Commands

Command	Description
show	Shows the information about the domain storage features.

scope system

To enter system-management mode, use the **scope system** command.

scope system

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In this mode, you can manage the system configuration, including exporting and importing a configuration file.

Example

This example shows how to enter system-management mode:

```
firepower# scope system
firepower /system #
```

Related Commands

Command	Description
show system	Shows information about the systems configured on this device.

scope tacacs

To enter Terminal Access Controller Access Control System (TACACS) configuration mode, use the**scope tacacs** command.

scope tacacs

Syntax Description

This command has no arguments or keywords.

Command Modes

Scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object

Example

This example shows how to enter tacacs mode:

```
firepower # scope security
firepower /security # scope tacacs
firepower /security/tacacs #
```

scope telemetry

To enter telemetry mode, use the **scope telemetry** command.

scope telemetry

Syntax Description

This command has no arguments or keywords.

Command Modes

scope system, scope services

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You can use the enable or disable and show commands

Related Commands

Command	Description
show detail	Shows the telemetry information of the system.

scope vnic

To enter virtual NIC mode, use the **scope vnic** command.

scope vnic *dynamic_mac*

Syntax Description

dynamic_mac	The virtual NIC's dynamic MAC address.

Command Modes

EXEC mode

Service profile mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter virtual NIC mode while in organization mode:

```
FP9300-A # scope org org10
FP9300-A /org # scope service-profile sp10
FP9300-A /org/service-profile # scope vnic vNIC10
FP9300-A /org/service-profile/vnic #
```

Related Commands

Command	Description
show server adapter	Shows information about the available network adapters.

sub scopes (scope fabric-interconnect)

To enter switch uplink mode, use the **scope sw-uplink** command in scope fabric interconnect mode.

scope sw-uplink

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

You do not have to enter this mode with a managed object.

Example

This example shows how to enter sw-uplink mode:

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # scope sw-uplink
firepower /fabric-interconnect/sw-uplink #
```

Related Commands

Command	Description
show	Shows the information about the sw-uplink.

set Commands

set absolute-session-timeout

To set the absolute session timeout, use the **set absolute-session-timeout** command.

set absolute-session-timeout *seconds*

Syntax Description

seconds	Absolute session timeout for Web, SSH, and Telnet sessions; value can be 0 to 3600 seconds. To disable this timeout, set the value to 0.

Command Modes

Default authentication (/security/default-auth) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The absolute session timeout closes user sessions after the specified timeout period has passed, regardless of session use. This absolute timeout is global across all forms of access including serial console, SSH, and HTTPS.

Example

This example shows how to enter default authentication mode and then set the absolute timeout for all sessions to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set account-status

To specify whether a local user account is active or inactive, use the **set account-status** command.

set account-status {**active** | **inactive**}

Syntax Description

active	Specifies that the local user account is active.
inactive	Specifies that the local user account is disabled.

Command Modes

Local user (/security/local-user) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You must be a user with admin or AAA privileges to use this command.

The admin account is always set to active. It cannot be modified.

Example

This example shows how to enter local user mode and deactivate a local user account:

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # set account-status inactive
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
set expiration	Specifies the date on which the user account expires.

set address

To set an email or URL address for a Smart Call Home or Smart Licensing destination, use the **set address** command.

set address *address*

Syntax Description

address	The email address or URL of the Smart Call Home or Smart Licensing destination.

Command Modes

scope monitoring/scope callhome/scope profile/scope destination/

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

Each Firepower 4100/9300 chassis must be registered with the Smart Call Home License Authority or Smart License satellite server. Use this command to set an email or HTTP/HTTPS URL address as the licensing destination.

License Authority example: `https://tools.cisco.com/its/service/oddce/services/DDCEService`

Satellite server example: `https://ip_address/Transportgateway/services/DeviceRequestHandler`

Example

This example shows how to create and enter a Smart Call Home destination:

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # scope destination SLDest
firepower /monitoring/callhome/profile/destination # set address
https://tools.cisco.com/its/service/oddce/services/DDCEService
firepower /monitoring/callhome/profile/destination* # commit-buffer
firepower /monitoring/callhome/profile/destination #
```

Related Commands

Command	Description
create destination	Creates a new Smart Call Home destination.
delete destination	Deletes an existing Smart Call Home destination.
set protocol	Sets the transport protocol for a Smart Call Home destination.

set admin-state

To enable or disable the administrative state of a Smart Call Home policy, use the **set admin-state** command.

set admin-state { **disabled** | **enabled** }

Syntax Description

disabled	Sets the policy administrative state to disabled.
enabled	Sets the policy administrative state to enabled.

Command Modes

scope monitoring/scope callhome/policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to enable or disable the Call Home policy when a fault or system event matching the associated cause is encountered.

Example

This example shows how to enter and enable a Call Home policy instance for link-down events:

```
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
firepower /monitoring/callhome/policy #
```

Related Commands

Command	Description
enter policy	Enters a Smart Call Home policy.
delete policy	Deletes an existing Smart Call Home policy.
scope policy	Scopes into a Smart Call Home policy.
show	Displays Call Home configuration or policy information.

set auth-server-group

To specify a default authentication server group, use the **set auth-server-group** command.

set auth-server-group *admin*

Syntax Description

admin	The name of the authentication server group.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to specify the default authentication server group:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set auth-server-group admin_server
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set realm	Specifies the default authentication service.

set authentication

To set the default authentication method for the user during login and when connecting to the FXOS CLI via the console port, use the **set authentication** command.

set authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security

Command History

Release	Modification
2.10(1)	Command added.

Usage Guidelines

You can set the default method by which a user is authenticated during login and when connecting to the FXOS CLI via the console port.

Example

This example shows how to enter security mode and set default authentication method:

```
firepower# scope security
firepower /security # set authentication
  console  Console authentication
  default  Default authentication
```

Related Commands

Command	Description
show authentication	Displays the existing authentication service.

set auto-negotiation

To enable or disable the autonegotiation of an interface, use the **set auto-negotiation** command.

set auto-negotiation {**on** | **off**}

Syntax Description

on	(Optional) Auto-Negotiation is turned on.
off	(Optional) Auto-Negotiation is turned off.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

Command History

Release	Modification
2.1.1	Command added.

Usage Guidelines

This command works only on specific port types.

Example

This example shows how to enable or disable autonegotiation:

```
Firepower-9300 # scope eth-uplink
Firepower-9300 /eth-uplink # scope fabric a
Firepower-9300 /eth-uplink #/fabric # scope interface Ethernet2/1
Firepower-9300 /eth-uplink/fabric/interface* # set auto-negotiation on
Firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
Firepower-9300 /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
scope interface	Displays the Ethernet interface information of the interface.

set cert

To add an RSA certificate to a keyring, use the **set cert** command.

set cert

Syntax Description

This command has no arguments or keywords.

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After entering the command, you are prompted to enter the certificate text, which must end with **ENDOFBUF**.

Example

This example shows how to enter the certificate text for a keyring:

```
FP9300-A /security/keyring # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw>0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoW>KWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7p>V57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
G>jnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5>L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgV>juaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0>K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
```

```
ENDOFBUF
FP9300-A /security/keyring* #
```

Related Commands

Command	Description
set modulus	Specifies the RSA key modulus (SSL key length) in bits.
set regenerate	Regenerates the RSA keys in the default keyring.
set trustpoint	Specifies whether the keyring certificate can be regenerated.

set certchain

To enter a list (or chain) of certificates for the current trustpoint, use the **set certchain** command.

set certchain [*cert_chain*]

Syntax Description

cert_chain	(Optional) The certificate chain obtained from a Certificate Authority. If this variable is omitted, you are prompted to enter the certificate information manually.

Command Modes

Trustpoint mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The certificates must be in Base64 encoded X.509 (CER) format.

If you do not specify the certificate chain with the command, you are prompted to enter a certificate or a list of trust points defining a certification path to the root Certificate Authority (CA). Type ENDOFBUF to finish the entry.

See "Certificates, Key Rings, and Trusted Points" in the *Cisco FXOS CLI Configuration Guide* for information about obtaining a trust certificate.

Example

This example shows how to create and enter a new trustpoint, and then paste a certificate chain into the trustpoint :

```
FP9300-A # scope security
FP9300-A /security # enter trustpoint tPoint4
FP9300-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
```

```
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
FP9300-A /security/trustpoint* # commit-buffer
FP9300-A /security/trustpoint #
```

Related Commands

Command	Description
enter trustpoint	Enters a trustpoint.
show trustpoint	Shows current trustpoint information.

set (certreq)

To specify parameters for a keyring certificate request, use the **set** command in certificate request mode.

set { *country* | *dns* | *e-mail* | *fi-a-ip* | *fi-a-ipv6* | *fi-b-ip* | *fi-b-ipv6* | *ip* | *ipv6* | *locality* | *org-name* | *org-unit-name* | *password* | *state* | *subject-name* }

Syntax Description

country	(Optional) Specify a two-letter country code for the request; letters must be capitalized.
dns	(Optional) Specify the domain name assigned to the network; common to all host names. This is an alternative to *subject-name*.
e-mail	(Optional) Specify the email address associated with the request.
fi-a-ip	Not used.
fi-a-ipv6	Not used.
fi-b-ip	Not used; there is no fabric interconnect B.
fi-b-ipv6	Not used; there is no fabric interconnect B.
ip	(Optional) Specify the IPv4 address of the device domain.
ipv6	(Optional) Specify the IPv6 address of the device domain.
locality	(Optional) Specify the city or town in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
org-name	(Optional) Specify the name of the organization requesting the certificate. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
org-unit-name	(Optional) Specify the name of the unit within the organization. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
password	(Optional) You are asked to enter and then confirm a password for the request.

state	(Optional) Specify the state or province in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
subject-name	(Optional) Specify the fully qualified domain name of the local fabric interconnect.

Command Modes

scope security/enter keyring/scope certreq/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After creating or entering a certificate request, use these options to specify information about the request.

Example

This example shows how to specify information about a certificate request:

```
firepower /security/keyring # enter certreq
firepower /security/keyring/certreq # set subject-name FP9300-1.testnet.com
firepower /security/keyring/certreq* # set password
Certificate request password:
Confirm certificate request password:
firepower /security/keyring/certreq* #
```

Related Commands

Command	Description
create certreq	Creates a new keyring certificate request.
delete certreq	Deletes an existing keyring certificate request.
enter certreq	Enters a keyring certificate request.
set (keyring)	Sets keyring-related information, inluding modulus and trustpoint.

set (cfg-export-policy)

To specify or edit the parameters for an existing configuration-export policy, use the **set** command in configuration-export-policy mode.

set {**adminstate** | **descr** | **hostname** | **password** | **port** | **protocol** | **remote-file** | **schedule** | **user**}

Syntax Description

adminstate {**disable** | **enable**	Enables or disables policy administration. When disabled, configuration back-ups are not exported according to the policy schedule.
descr *description*	(Optional) You can add a description to the configuration object; the description can be between one and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; the string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
hostname *host_ID*	(Optional) Specify the IP address or host name of the remote server to which the configuration back-up is exported. This host can be a server, storage array, local drive, or any read/write media that is accessible on the network. **Note** To use an actual host name, a configured DNS server must be available.
password	(Optional) Specify the password used to connect to the remote server; you are asked to enter and then confirm the password.
port {*number* | **default**}	(Optional) You can change the port on which communications with the remote server take place; if this option is not specified, the protocol's default port is used. The options are a port-ID number between zero and 4294967295, or **default** for the current protocol's default port.
protocol *name*	(Optional) Specify the file-transfer protocol to use. Available options are: • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	(Optional) Specify the full path, including a file name, for the exported configuration; can be between one and 128 characters.
schedule {**bi-weekly** | **daily** | **weekly**}	(Optional) Specify how frequently the configuration is automatically exported: • **bi-weekly** – Export occurs every two weeks. • **daily** – Export occurs every day. • **weekly** – Export occurs once a week.

user *name*	(Optional) Specify the user-account name employed to connect to the remote host; can be between zero and 510 characters.

Command Modes

scope org/scope cfg-export-policy/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Changing `set adminstate` to `enable` and then issuing a `commit-buffer` command immediately triggers a configuration export.

Example

This example shows how to configure the default configuration-export policy, and then check the policy parameters:

```
firepower # scope org
firepower /org # scope cfg-export-policy default
firepower /org/cfg-export-policy # set protocol scp
firepower /org/cfg-export-policy* # set hostname 192.168.1.2
firepower /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
firepower /org/cfg-export-policy* # set user user1
firepower /org/cfg-export-policy* # set password
Enter a password:
Confirm the password:
firepower /org/cfg-export-policy* # set schedule weekly
firepower /org/cfg-export-policy* # set adminstate enable
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-policy # show detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Scp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Weekly
    Port: Default
    Current Task:
firepower /org/cfg-export-policy #
```

Related Commands

Command	Description
export-config	Exports the current system configuration to a remote server as an XML file; creates an export-configuration object.
import-config	Copies a previously exported XML configuration file to this appliance.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

set (cfg-export-reminder)

To specify or edit the parameters for the configuration-export reminder object, use the **set** command in configuration-export-reminder mode.

set {**adminstate** | **frequency**}

Syntax Description

adminstate {**disable** | **enable**	Enable or disable the export reminder. When disabled, configuration back-up reminder faults are not generated.
frequency *number_of_days*	Specify the number of days that can pass without a configuration back-up occuring. After this period, the system will generate a reminder fault. This value can be between one and 365 days.

Command Modes

scope org/scope cfg-export-reminder/

Command History

Release	Modification
1.1.3	Command added.

Usage Guidelines

When the reminder is enabled, the system generates a fault when a configuration export hasn't been executed in the specified number of days.

Example

This example shows how to enter the export-reminder object, enable it, specify how often back-ups must occur, and then view the settings:

```
firepower # scope org
firepower /org # scope cfg-export-reminder
firepower /org/cfg-export-reminder # set adminstate enable
firepower /org/cfg-export-reminder* # set frequency 30
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-reminder # show

Config Export Reminder:
    Config Export Reminder (Days): 30
    AdminState: Enable
firepower /org/cfg-export-reminder #
```

Related Commands

Command	Description
scope cfg-export-policy	Enters the configuration export policy.
show	In configuration-export reminder mode, shows the current reminder object set-up.

set cli

To specify whether command output lines wrap or truncate to fit the width of the terminal window, whether table headers are displayed, and whether commas or spaces are used to separate fields in command output tables, use the **set cli** command.

set cli { **suppress-field-spillover** { **off** | **on** } | **suppress-headers** { **off** | **on** } | **table-field-delimiter** { **comma** | **none** } }

Syntax Description

suppress-field-spillover { **off** | **on** }	Use **off** to wrap output lines in the terminal window. Use **on** to truncate output lines at the end of the terminal window.
suppress-headers { **off** | **on** }	Use **off** to display table headers. Use **on** to not display table headers.
table-field-delimiter { **comma** | **none** }	Use **comma** to separate fields in command output tables with commas. Use **none** to separate fields in command output tables with spaces.

Command Default

Command output lines wrap in the terminal window.

Table headers are displayed.

Spaces are used to separate fields in command output tables.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify whether command output lines wrap or truncate to fit the width of the terminal window, whether table headers are displayed, and whether commas or spaces are used to separate fields in command output tables.

Example

This example shows how to specify that command output lines truncate, and then how to reset to wrap:

```
FP9300-A# set cli suppress-field-spillover on
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
mezz cards in 1/6(FSM-STAGE:sam:dme:ComputeBladeDiscover:NicPresence)
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R
esult: end-point-unavailable Code: unspecified Message: sendSamDmeAdapterInfo: i
dentify failed

FP9300-A# set cli suppress-field-spillover off
FP9300-A# show fault
```

```
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R

FP9300-A#
```

Related Commands

Command	Description
show cli	Shows current CLI settings.
terminal	Sets the number of lines, and the width of the lines, displayed in the terminal window.

set clock

To manually set the clock timing in FXOS, use the **set clock** command.

set clock

Syntax Description

set clock	Use **set clock** to maunally set the clock in FXOS.

Command Modes

scope system/scope services

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to set the clock in FXOS:

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set clock aug 23 2021 12 00 00
firepower /system/services* # commit
firepower /system/services # show clock
Tue Aug 24 12:00:02 UTC 2021
```

set cluster-control-link network

To set the cluster control link IP network in the cluster bootstrap configuration for the threat defense and ASA, use the **set cluster-control-link network** command.

set cluster-control-link network *a.b*.**0.0**

Syntax Description

a.b.**0.0**	Specifies any /16 network address, except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. If you set the value to 0.0.0.0, then the default network is used: 127.2.0.0.

Command Default

The default network is 127.2.0.0.

Command Modes

scope ssa/create logical-device/create cluster-bootstrap/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: *a.b.chassis_id.slot_id*.

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the mode to routed mode:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 clustered
Firepower /ssa/logical-device* # create cluster-bootstrap
firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network 10.10.0.0
firepower /ssa/logical-device/cluster-bootstrap* #
```

Related Commands

Command	Description
create logical-device	Creates the logical device.
create cluster-bootstrap	Creates the cluster bootstrap configuration for the application.

set collection-interval

To define how frequently monitored statistics are collected, use the **set collection-interval** command.

set collection-interval *interval*

Syntax Description

interval	Length of time defining the statistics collection interval; available values are: • `1minute` – one-minute intervals • `2minutes` – two-minute intervals • `30seconds` – 30-second intervals • `5minutes` – five-minute intervals

Command Modes

scope monitoring/scope stats-collection-policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides sufficient data to calculate and report minimum, maximum, and average values.

Statistics can be collected and reported for each of the following functional areas of your Firepower system; use the **scope stats-collection-policy** command to access a specific collection policy:

- `Adapter` – statistics related to the adapters.
- `Chassis` – statistics related to the blade chassis.
- `FEX` – statistics related to configured Fabric Extender(s).
- `Host` – this policy is a placeholder for future support.
- `Port` – statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports.
- `Server` – statistics related to servers.

Note There is one default statistics collection policy for each of the functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Example

This example shows how to enter the statistics collection policy for ports, set the collection interval to one minute, set the reporting interval to 30 minutes, and then commit the transaction:

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Related Commands

Command	Description
scope stats-collection-policy	Enters stats-collection-policy mode, where you manage statistics collection and reporting intervals.
set reporting-interval	Specifies how frequently statistics are reported.

set con-absolute-session-timeout

To set the serial console absolute session timeout, use the **set con-absolute-session-timeout** command.

set con-absolute-session-timeout *seconds*

Syntax Description

seconds	Serial console absolute session timeout; value can be 0 to 3600 seconds. To disable this timeout, set the value to 0.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can separately configure the absolute session timeout for serial console sessions. This means you can disable the serial console absolute session timeout for debugging while maintaining the absolute timeout for other forms of access.

Example

This example shows how to enter default authentication mode and then set the serial console absolute timeout to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set con-session-timeout

To set the serial console idle session timeout, use the **set con-session-timeout** command.

set con-session-timeout *seconds*

Syntax Description

seconds	Serial console idle session timeout; value can be 0 to 3600 seconds. To disable this timeout, set the value to 0.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the idle session timeout for serial console sessions.

Example

This example shows how to enter default authentication mode and then set the serial console idle timeout to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set cpu-core-count

To set the CPU cores for a resource profile for use with container instances, use the **set cpu-core-count** command.

set cpu-core-count *cores*

Syntax Description

cores	Sets the number of cores for the profile, between 6 and the maximum, depending on your chassis, as an even number. You *cannot* specify 8 cores.

Command Modes

scope ssa/create resource-profile/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

To specify resource usage per container instance, create one or more resource profiles. When you deploy the logical device/application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

- The minimum number of cores is 6.
- You cannot specify 8 cores due to internal architecture.
- You can assign cores as an even number (6, 10, 12, 14 etc.) up to the maximum.
- The maximum number of cores available depends on the security module/chassis model.

The chassis includes a default resource profile called "Default-Small," which includes the minimum number of cores. You can change the definition of this profile, and even delete it if it is not in use. Note that this profile is created when the chassis reloads and no other profile exists on the system.

You cannot change the resource profile settings if it is currently in use. You must disable any instances that use it, then change the resource profile, and finally reenable the instance. If you resize instances in an established High Availability pair, then you should make all members the same size as soon as possible.

If you change the resource profile settings after you add the threat defense instance to the management center, update the inventory for each unit on the **Devices** > **Device Management** > **Device** > **System** > **Inventory** dialog box.

Example

The following example adds three resource profiles.

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
firepower /ssa/resource-profile* # set cpu-core-count 6
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
```

```
firepower /ssa/resource-profile* # set cpu-core-count 10
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

Related Commands

Command	Description
create resource-profile	Adds a resource profile for use with container instances.
set resource-profile-name	Assigned the resource profile to the application instance.
show monitor detail	Shows resource usage for the security module/engine slot.
show resource detail	Shows resource allocation for the application instance.
show resource-profile user-defined	Shows resource profile assignments.

set deploy-type

To set the deployment type for an application instance, either native or container, use the **set deploy-type** command.

set deploy-type {**native** | **container**}

Syntax Description

container	Sets the application instance to the container type.
native	Sets the application instance to the native type.

Command Default

The default type is native.

Command Modes

scope ssa/scope slot/create app-instance/

Command History

Release	Modification
2.4(1)	Command added for threat defense.

Usage Guidelines

Application instances run in the following deployment types:

- Native instance—A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance.
- Container instance—A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances. Multi-instance capability is only supported for the threat defense; it is not supported for the ASA.

Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full threat defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the threat defense.

For the Firepower 9300, you can use a native instance on some modules, and container instances on the other module(s).

Example

The following example adds an threat defense application instance, and sets it to the container type:

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
```

```
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Related Commands

Command	Description
show app-attri	Shows current application attributes.
create resource-profile	Creates a resource profile for use with constainer instances.
show resource-profile-name	Shows available resource profiles.

set descr

To set a description for the port-channel, use the **set descr** command.

set descr *description*

Syntax Description

description	(Optional) Description. Enter up to 256 characters.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output Ethernet.

Example

This example shows how to set the description:

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set descr "link"
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the duplex parameter.

set duplex

To set the duplex for all members of the port-channel, use the **set duplex** command.

set duplex {**fullduplex** | **halfduplex**}

Syntax Description

fullduplex	(Optional) Specifies the duplex mode as full.
halfduplex	(Optional) Specifies the duplex mode as half.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

You must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is set for Gigabit Ethernet.

Example

This example shows how to set the interface duplex mode:

```
firepower-9300# scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set duplex halfduplex
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the duplex parameter.

set email

To set a contact email address for a user account, use the **set email** command.

set email *email_address*

Syntax Description

email_address	An email address for the user account. Specify the email address in the format: *user_name@domain_name*.

Command Modes

Callhome (/monitoring/callhome) mode – to specify a primary contact email address to be included in Call Home messages.

Local user (/security/local-user) mode – to specify a contact email address for the current local user.

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If the email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends using email addresses which comply with RFC2821 and RFC2822, and include only 7-bit ASCII characters.

In callhome mode, you can use a maximum of 2083 characters for the email address.

In local user mode, you can use a maximum of 510 characters for the email address.

Example

This example shows how to specify an email address for the current local user:

```
FP9300-A /security/local-user # set email admin@example.com
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
set phone-contact	Specifies a telephone contact number for a Smart Call Home account.

set enforce-strong-password

To enable and disable strong password enforcement, use the **set enforce-strong-password** command.

set enforce-strong-password {**no** | **yes**}

Syntax Description

no	Disables strong password enforcement.
yes	Enables strong password enforcement.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

A password is required for each locally authenticated user account. A user with admin or AAA privileges can configure the system to perform a password strength check on all user passwords. If password strength checking is enabled, each user must have a "strong" password.

We recommend that each user have a strong password. If password strength checking is enabled for locally authenticated users, FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters. (The set min-password-length, on page 312 command can be used to specify the minimum number of characters required.)
- Must include at least one uppercase alphabetic character.
- Must include at least one lowercase alphabetic character.
- Must include at least one non-alphanumeric (special) character.
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.
- Must not be identical to the user name or the reverse of the user name.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Must not be blank for local user and admin accounts.

Example

This example shows how to enter security mode and enable strong password enforcement:

```
FP9300-A# scope security
FP9300-A /security # set enforce-strong-password yes
FP9300-A /security* # commit-buffer
```

```
FP9300-A /security #
```

Related Commands

Command	Description
set min-password-length	Specifies a minimum password length.

set expiration

To set an expiration date for a local user account, use the **set expiration** command.

set expiration { { **apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep** } *day* *year* }

Syntax Description

{ **apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep** }	The three-letter month abbreviation.
day	Numeric day of the month; valid values are 1 through 31.
year	Numeric year for expiration; maximum value is 2037.

Command Modes

Local user mode—to specify an expiration date for the current local user.

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can however, reconfigure the account with a different expiration date.

Example

This example shows how to enter security mode, create a new local user account and specify an expiration date for that account:

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set expiration dec 31 2019
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
set password	Specifies a password for a user account.

set (export-config)

To edit the parameters for an existing export-configuration object, use the **set** command in export-configuration mode.

set {**descr** | **password** | **port** | **protocol** | **remote-file** | **user**}

Syntax Description

descr *description*	(Optional) You can add a description to the configuration object; can be between one and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; the string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
password	(Optional) You can change the password used to connect to the remote server; you are asked to enter and then confirm the password.
port {*number* | **default**}	(Optional) You can change the port on which communications with the remote server take place. The options are a port-ID number between zero and 4294967295, or **default** for the current protocol's default port.
protocol *name*	(Optional) You can change the file-transfer protocol used to transmit the configuration back-up to the remote server. Available options are: • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	(Optional) You can change the name of the back-up configuration file; can be between one and 128 characters.
user *name*	(Optional) You can change the user-account name employed to connect to the remote host; can be between zero and 510 characters.

Command Modes

scope system/scope export-config/

Command History

Release	Modification
1.1.3	Command added.

Usage Guidelines

Use these options to change the back-up options for an existing export-configuration object.

An export-configuration object is created when you issue an **export-config** command to back up the current logical device and platform configuration, and **scope export-config** is used to enter the object and edit its parameters.

Please note the following:

- Beginning with FXOS 2.6.1, you must specify a key for use when encrypting sensitive information such as passwords and other secret keys during configuration export, and you must have specified it before you attempt to export the configuration.

  Also, the same key used during export must be set on the target system when you import an exported configuration, unless the file was exported from an FXOS release prior to 2.6.1, in which case the target system will not check the encryption key and will allow the import.

- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.

- To avoid overwriting existing back-up files, please be sure to change the file name in the export operation, or copy the existing file to another location.

Example

This example shows how to add a description to an existing export-configuration object:

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config # set descr one-time_back-up_be_sure_to_change_file_name
firepower /system/export-config* # commit-buffer
firepower /system/export-config #
```

Related Commands

Command	Description
cfg-export-policy	Configures a configuration export policy.
export-config	Exports the current system configuration to a remote server as an XML file; creates an export-configuration object.
import-config	Copies a previously exported XML configuration file to this appliance.
set password-encryption-key	Specifies a key used when encrypting sensitive information during configuration export.

set firstname

To specify the first name of a local user, use the **set firstname** command.

set firstname *name*

Syntax Description

name	The user's first name; can be zero to 32 characters.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter security mode, create a new local user account and specify a first name and a last name for that user:

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Command	Description
create local-user	Creates a new local user account.
set lastname	Specifies the surname for a local user account.

set flow-control-policy

To assign a flow control policy to an interface or a port-channel, use the **set flow-control-policy** command.

set flow-control-policy *name*

Syntax Description

name	The name of the flow control policy; maximum of 16 characters.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope port-channel/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

When you create a new flow control policy, you are automatically entered into flow-control/policy mode (eth-uplink/flow-control/policy) with an asterisk indicating the new policy is not yet committed. You can set policy property values and then commit the new policy. After you create a flow control policy, the policy name cannot be changed. You must delete the policy and create a new one.

Example

This example shows how to assign a flow control policy to an interface:

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric
firepower-9300 /eth-uplink #/fabric # scope interface Ethernet1/8
firepower-9300 /eth-uplink/fabric/interface* # set flow-control-policy eth1-8flowcontrol
firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
firepower-9300 /eth-uplink/fabric/interface #
```

Related Commands

Command	Description
create policy (flow control)	Creates a new flow control policy.
show interface	Displays the interface status, which includes the speed parameters.
show port-channel	Displays information about a port channel.

set (flow-control policy)

To specify or edit the parameters for an existing flow-control policy, use the **set** command in flow-control/policy mode.

set { **prio** | **receive** | **send** }

Syntax Description

prio { **auto** | **on**	Sets the flow-control priority option: • **auto** – This device and the network will negotiate whether Point-to-Point Protocol (PPP) is used on this fabric. • **on** – PPP is enabled on this fabric.
receive **off**	Specifies that pause requests from the network are ignored and traffic flow continues normally.
send **off** | **on**	Sets the flow-control send parameter: • **off** – Traffic flows normally regardless of packet load. • **on** – This device sends a pause request to the network if the incoming packet buffer becomes full. The pause remains in effect for a few milliseconds while traffic returns to normal levels.

Command Modes

scope eth-uplink/scope flow-control/policy/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Use this command to specify flow control receive options. When you specify off, pause requests from the network are ignored and traffic flow continues as normal. When you specify on, pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.

Use this command to specify flow control send options. When you specify **off**, traffic on the port flows normally regardless of the packet load. When you specify **on**, the FXOS sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.

Example

This example shows how to create and enter a named policy for flow control, and then set policy parameters:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
firepower /eth-uplink/flow-control/policy* # set prio auto
firepower /eth-uplink/flow-control/policy* # set send on
firepower /eth-uplink/flow-control/policy* # commit-buffer
```

```
firepower /eth-uplink/flow-control/policy #
```

Related Commands

Command	Description
show policy	In flow-control/policy mode, displays property values for the current flow-control policy. In flow-control mode, displays property values for all currently defined flow-control policies.

set frequency

To generate a fault when a configuration export hasn't been executed in a certain number of days, use the **set frequency** command.

set frequency *days*

Syntax Description

days	Config Export Reminder (Days).

Command Modes

scope org/scope cfg-export-reminder/

Command History

Release	Modification
2.0.1	Command added.

Example

This example shows how to set the configuration frequency days for export reminder:

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-reminder
firepower-9300 /org/scope cfg-export-reminder* # set frequency 2
firepower-9300 /org/scope cfg-export-reminder* # commit-buffer
firepower-9300 /org/scope cfg-export-reminder* # show detail
Config Export Reminder:
Config Export Reminder (Days): 10
AdminState: Enable
```

Related Commands

Command	Description
set adminstate	Specifies the admin state for the export reminder.

set http-proxy-server-enable

To enable or disable an HTTP/HTTPS proxy for Smart Software Licensing and Smart Call Home, use the **set http-proxy-server-enable** command.

set http-proxy-server-enable {**off** | **on**}

Syntax Description

off	Disables the Smart Call Home HTTP/HTTPS proxy.
on	Enables the Smart Call Home HTTP/HTTPS proxy.

Command Default

The HTTP/HTTPS proxy is disabled by default.

Command Modes

Callhome mode

Usage Guidelines

If your network uses an HTTP proxy for Internet access, you must enable the proxy and configure its address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example

This example shows how to enable an HTTP proxy:

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-enable on
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
set http-proxy-server-url	Sets the HTTP or HTTPS address of the proxy server.
set http-proxy-server-port	Sets the communications port for the proxy server.

set http-proxy-server-port

To set the HTTP/HTTPS proxy server port for Smart Software Licensing and Smart Call Home, use the **set http-proxy-server-port** command.

set http-proxy-server-port *port_number*

Syntax Description

port_number	The port for the HTTP or HTTPS proxy server; range is 1 to 65535.

Command Default

The HTTP/HTTPS proxy is disabled by default. The proxy must be enabled before you enter the server address and port number.

Command Modes

Callhome mode

Usage Guidelines

If your network uses an HTTP proxy for Internet access, you must enable the proxy and configure its address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example

This example shows how to enter an HTTP/HTTPS proxy-server port number:

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-port 443
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
set http-proxy-server-enable	Enables or disables the HTTP/HTTPS proxy for Smart Software Licensing and Smart Call Home.
set http-proxy-server-url	Sets the HTTP/HTTPS address for the proxy server.

set http-proxy-server-url

To set the HTTP/HTTPS proxy server address for Smart Software Licensing and Smart Call Home, use the **set http-proxy-server-url** command.

set http-proxy-server-url *url*

Syntax Description

url	The HTTP or HTTPS address of the proxy server; can be a maximum of 2083 characters.

Command Default

The HTTP/HTTPS proxy is disabled by default. The proxy must be enabled before you enter the server address.

Command Modes

Callhome mode

Usage Guidelines

If your network uses an HTTP proxy for Internet access, you must enable the proxy and configure its address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example

This example shows how to enter an HTTPS proxy-server address:

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-url https://209.165.201.10
FP9300-A /monitoring/callhome #
```

Related Commands

Command	Description
set http-proxy-server-enable	Enables or disables the HTTP/HTTPS proxy for Smart Software Licensing and Smart Call Home.
set http-proxy-server-port	Sets the communications port for the proxy server.

set https

To specify HTTPS service parameters, use the **set https** command.

set https {**auth-type** {**cert-auth** | **cred-auth**} | **cipher-suite** *cipher_string* | **cipher-suite-mode** {**custom** | **high-strength** | **low-strength** | **medium-strength**} | **crl-mode** {**relaxed** | **strict**} | **keyring** *keyring_name* | **port** *port_number*}

Syntax Description

auth-type {**cert-auth** | **cred-auth**}	(Optional) Specifies the type of authentication to use for HTTPS access: • **cert-auth**—Sets your system to use a client certificate in conjunction with LDAP to authenticate users for HTTPS access. • **cred-auth**—Sets the system to use credential-based user authentication for HTTPS access.
cipher-suite *cipher_string*	(Optional) Specifies the definition string for the cipher suite to be used with the custom **cipher-suite-mode**. The specification string can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters, except ! (exclamation point), + (plus sign), - (hyphen), and : (colon). See http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite for additional information. **Note** This string is ignored if **cipher-suite-mode** is set to anything other than **custom**.
cipher-suite-mode {**custom** | **high-strength** | **low-strength**	(Optional) Sets the level of Cipher Suite security used: • **custom**—Lets you define a custom Cipher Suite security specification string using the **cipher-suite** option. • **high-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:!LOW:!MEDIUM:!eNULL:!RC4:!MD5: !IDEA:+HIGH:+EXP • **low-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:RC4+RSA: !IDEA:+HIGH:+MEDIUM:+LOW:+EXP:+eNULL • **medium-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56: !LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL Generally, cipher strength is roughly based on the bits of security (or symmetric key size), with "low" meaning less than 128 bits of security, "medium" meaning equal to 128 bits, and "high" meaning greater than 128 bits of security.

crl-mode {**relaxed** | **strict**}	(Optional) Defines the level of certificate revocation list (CRL) checking for HTTPS connections: • **relaxed**—Certificates found on a CRL may be used to allow HTTPS authentication, depending on the reason for the certificate's listing; a warning message is logged whenever this occurs. Essentially disables CRL checking. • **strict**—Connection authentication fails for any certificate on a CRL; a warning message is logged whenever this occurs. Also, the CRL must be up to date.
keyring *keyring_name*	(Optional) Specifies the name of the RSA keyring to be used for HTTPS connections.
port *port_number*	(Optional) Specifies the port to be used for HTTPS connections; can be 1 to 65535. Default is 443.

Command Default

The default HTTPS authentication configuration on the Firepower 4100/9300 chassis is credential-based.

The default Cipher Suite security level is medium strength.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If certificate authentication is enabled, that is the only form of authentication permitted for HTTPS.

The following requirements must be met by the client certificate to use this feature:

- The user name must be included in the X509 attribute Subject Alternative Name email.
- The client certificate must be signed by a root CA which has had its certificate imported into a trustpoint on the supervisor.

Caution When you commit most of these configuration parameters (specifically keyring, port, cipher-suite, and custom cipher-suite-mode), all current HTTP and HTTPS sessions are closed without user warning.

Example

This example shows how to enable certificate-based authentication for HTTPS access:

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # set https auth-type cert-auth
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

Related Commands

Command	Description
enable https	Enables the HTTPS service.
show https	Shows current HTTPS service configuration.

set (interface)

To specify or change the parameters for an interface, use the **set** command in interface mode.

set
{**admin-duplex** | **admin-speed** | **auto-negotiation** | **descr** | **eth-link-profile** | **flow-control-policy** | **nw-ctrl-policy** | **port-type** | **user-label** }

Syntax Description

admin-duplex {**fullduplex** | **halfduplex** }	Defines the duplex mode for the interface: • **fullduplex** – Specifies simultaneous two-way communications. • **halfduplex** – Specifies one-way-at-a-time communications.
admin-speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps** }	Specify the interface data-transfer speed: • **100gbps** – One hundred Gigabits per second. • **100mbps** – One hundred Megabits per second. • **10gbps** – Ten Gigabits per second. • **10mbps** – Ten Megabits per second. • **1gbps** – One Gigabit per second. • **40gbps** – Forty Gigabits per second.
auto-negotiation {**no** | **yes** }	Enables or disables auto-negotiation of common transmission parameters such as speed, duplex and flow control. • **no** – Disables auto-negotiation. • **yes** – Enables auto-negotiation.
descr *description*	You can add a description to the interface; the description can be between zero and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; spaces are not allowed. The string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
eth-link-profile *name*	You can assign an Ethernet Link Profile to the interface, automatically configuring the interface according to the profile parameters. Provide the name of the profile; can be up to 16 alphanumeric characters.
flow-control-policy *name*	You can assign a flow-control policy to the interface; provide the policy name, which can be up to 16 alphanumeric characters.
nw-ctrl-policy *name*	You can assign a network-control policy to the interface; provide the policy name, which can be up to 16 alphanumeric characters.

port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}	Specify the interface type or function: • **cluster** – Specify **cluster** only if you want to use this interface as the cluster control link. • **data** – Use for regular data transmission. This is the default type. • **data-sharing** – Use for regular data; only supported with container instances. • **firepower-eventing** – Use this interface as a secondary management interface for threat defense devices. The firepower-eventing interface is used to carry all event traffic (such as Web events). • **mgmt** – Use to manage application instances. You can only assign one management interface per logical device. See set port-type, on page 329 for more information about this command.
user-label *label*	You can apply a descriptive label to this interface. can be beween zero and 16 alphanumeric characters.

Command Modes

scope eth-uplink/scope fabric a/interface/

Command History

Release	Modification
2.4(1)	We added the **data-sharing** type.
1.1(4)	We added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

The type `cluster` is a special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on port-channel 48.

Data interfaces cannot be shared between logical devices.

The type `data-sharing` is supported only with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.

A `firepower-eventing` interface is a secondary management interface for threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as Web events). See the “Management Interfaces” section in the *System Configuration* chapter of the Management Center configuration guide. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.

Use `mgmt` interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

If you edited the default flow control policy, it is already applied to interfaces. If you created a new policy, you can apply it to the interface.

Example

This example shows how to set the interface speed to 10 Gbps and the port type to data:

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/8
firepower /eth-uplink/fabric/interface # enable
firepower /eth-uplink/fabric/interface* # set admin-speed 10gbps
firepower /eth-uplink/fabric/interface* # set port-type data
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface
```

Related Commands

Command	Description
enter interface	Enters an interface so you can configure and manage the interface settings.
scope interface	Scopes into an interface so you can configure and manage the interface settings.
show interface	Displays interface configuration and status information.

set ipv6

To enable or disable the IPv6 support on firepower device, use the **set ipv6** command in fabric interconnect mode.

set ipv6 [**enable** | **disable**]

Syntax Description

enable/disable	Enables or disables IPv6 support on the firepower device.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Usage Guidelines

By default, IPv6 will not be set. Use this command to enable or disable IPv6.

Example

This example shows how to enable IPv6 in a firepower device:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6 enable
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-auto eui64

To generate IPv6 address based on eui64 method, use the **set ipv6-auto eui64** command in fabric interconnect mode. The lower 64 bits are derived from the hardware address identifier such as MAC.

set ipv6 auto eui64

Syntax Description

auto eui64	Generates the ipv6 address based on the hardware identifiers.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Usage Guidelines

You must have a valid global adddress present on the management interface to set ipv6-auto eui64.

Example

This example shows how to set the ipv6-auto eui64:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-auto eui64
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-auto stablesec

To generate ipv6 address based on stable secret seed mechanism, use the **set ipv6-auto stablesec** command in fabric interconnect mode.

set ipv6 auto stablesec

Syntax Description

auto stablesec	Generates the ipv6 address based on the stable secret seed values.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Example

This example shows how to set the ipv6-auto stablesec:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-auto stablesec
Warning: Setting ipv6readycfg to stablesec will require reboot
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-ready

To set the IPv6 address based on eui64 or stable secret seed method based on the input IPv6 address, use the **set ipv6-ready** command in fabric interconnect mode.

set ipv6-ready [**ipv6-addr** *address* **ipv6-readyconfig-eui64 ipv6-readyprefix** *prefix* | **ipv6-addr** *address* **ipv6-readyconfig stablesec ipv6-readyprefix** *prefix*]

Syntax Description

ipv6-addr <address>	Input IPv6 adress
ipv6-readyconfig eui64	eui64 method to generate the ipv6 address based on the input address
ipv6-readyconfig stablesec	stablesec method to generate the ipv6 address based on the input address
ipv6-readyprefix <prefix>	IPv6 prefix

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Example

This example shows how to set the set the ipv6 address based on eui64 method :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-ready ipv6-addr 2003::12
ipv6-readyconfig eui64 ipv6-readyprefix 64
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

This example shows how to set the set the ipv6 address based on stablesec method :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-ready ipv6-addr
e2ca:83a7:eb48:8f6f:da04:949b:b701:1049 ipv6-readyconfig stablesec ipv6-readyprefix 64
Warning: Setting ipv6readycfg to stablesec will require reboot
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set keyring-name

To assign a keyring to an IPSec connection, use the **set keyring-name** command.

set keyring-name *name*

Syntax Description

name	The name of a keyring to be assigned to the IPSec connection; maximum of 16 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to add a keyring to an IPSec connection.

Example

This example shows how to add a keyring to the current IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set keyring-name kr22
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set keyring-passwd	Specifies the passphrase for a keyring assigned to an IPSec connection.

set lastname

To specify the last name of a local user, use the **set lastname** command.

set lastname *name*

Syntax Description

name	The user's surname; can be 0 to 32 characters.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter security mode, create a new local user account, and then specify a first name and a last name for that user.

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Command	Description
create local-user	Creates a new local-user account.
set firstname	Specifies the first name for a local user account.

set link-state-sync

To synchronize the operational link state with the physical link state for data interfaces using a service state, use the **set link-state-sync** command.

set link-state-sync

Syntax Description

This command has no arguments or keywords.

Command Modes

scope ssa

Command History

Release	Modification
2.9(1)	Command added.

Usage Guidelines

Use this command to synchronize the FTD operational link state with the physical link state for data interfaces.

Example

This example shows how to enter scope ssa mode and then set the link-state-sync.

```
firepower# scope ssa
firepower /ssa # scope logical-device <logical device identifier>
firepower /ssa/logical-device # set link-state-sync ?
  disabled  Disabled
  enabled   Enabled
```

set local-address

To specify the local IP address for an IPSec connection, use the **set local-address** command.

set local-address *ip_address*

Syntax Description

ip_address	Provide an IPv4 or IPv6 local gateway address for the IPSec connection; maximum of 510 characters.

Command Modes

Connection mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command and the **set remote-address** command to define the endpoints of an IPSec connection.

Example

This example shows how to set the local address for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.201.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set log-level

To specify the IPSec logging level, use the **set log-level** command.

set log-level *log_level*

Syntax Description

log_level	Enter a value between 0 and 4 to specify IPSec log verbosity; default is 1. **0** – Basic auditing information; for example, SA up/down. **1** – General control flow information, with errors. **2** – More detailed control flow information; includes debugging information. **3** – Includes raw data dumps (hexadecimal). **4** – Includes sensitive information in the data dumps; for example, SA keys.

Command Modes

IPSec mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **show ipsec-log** command to view the logs.

Example

This example shows how to set the IPSec logging level to 2:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # set log-level 2
FP9300-A /security/ipsec* # commit-buffer
FP9300-A /security/ipsec #
```

Related Commands

Command	Description
show ipsec-log	Shows the IPSec log file.

set max-login-attempts

To specify the maximum number of failed login attempts allowed, use the **set max-login-attempts** command.

set max-login-attempts *max_attempts*

Syntax Description

max_attempts	The maximum number of failed login attempts before the user is locked out of the system. The value can range from 0 to 10; the default is 0.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If any user (including admin users) exceeds this maximum number of login attempts, the user is locked out of the system and must wait a specified amount of time before being allowed to log in again. No notification appears indicating that the user is locked out.

Example

This example shows how to enter security mode and specify a maximum number of login attempts:

```
FP9300-A# scope security
FP9300-A /security # set max-login-attempts 4
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
clear lock-status	Clears a user's locked-out status.
set user-account-unlock-time	Specifies the amount of time a user remains locked out of the system after reaching the maximum number of login attempts.

set message

To add or replace the lines of text presented as the pre-login banner, use the **set message** command.

set message

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security/scope banner/scope pre-login-banner/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After entering the command, you are prompted to enter the lines of banner text. You must enter `ENDOFBUF` (must be all capital letters) to terminate the banner text.

Note The pre-login banner object must already exist; see create pre-login-banner, on page 94.

Example

This example shows you how to create and specify a pre-login banner, then commit and view it:

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner/pre-login-banner #
```

Related Commands

Command	Description
clear message	Removes the text from an existing pre-login banner; the actual banner object itself is not deleted.

Command	Description
create pre-login-banner	Creates a banner to be presented prior to the log-in screen; the banner object is initially empty.

set min-password-length

To specify a minimum length for user passwords, use the **set min-password-length** command.

set min-password-length *num_chars*

Syntax Description

num_chars	The minimum number of characters required for user passwords; value can range from 8 to 80.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If enabled, users must create passwords with the specified minimum number of characters or more. For example, if *num_chars* is set to 15, passwords must consist of at least 15 characters.

Example

This example shows how to enter security mode and specify a minimum password length of 15 characters:

```
FP9300-A# scope security
FP9300-A /security # set min-password-length 15
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
set enforce-strong-password	Enables and disables strong password enforcement.

set mode

To specify the IPSec connection mode, use the **set mode** command.

set mode {**transport** | **tunnel**}

Syntax Description

transport	Sets the connection mode to **transport**.
tunnel	Sets the connection mode to **tunnel**.

Command Modes

Connection mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In transport mode, only the payload of an IP packet is encrypted; in tunnel mode, the entire packet is encrypted. Transport mode is generally used for end-to-end sessions, and tunnel mode is used for all other types of connections (for example, between gateways).

Example

This example shows how to set the IPSec connection mode to tunnel:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set mode tunnel
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set local-addr	Sets the local IP address for an IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set modulus

To specify the RSA key modulus (SSL key length) in bits, use the **set modulus** command.

set modulus {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

Syntax Description

RSA key modulus (SSL key length) in bits	Valid options are: • **mod1536** – Modulus is 1536 bits • **mod2048** – Modulus is 2048 bits • **mod2560** – Modulus is 2560 bits • **mod3072** – Modulus is 3072 bits • **mod3584** – Modulus is 3584 bits • **mod4096** – Modulus is 4096 bits

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the key length for a keyring.

Example

This example shows how to specify a key length of 2048 bits for a keyring:

```
FP9300-A# scope security
FP9300-A /security # scope keyring test-ring
FP9300-A /security/keyring # set modulus 2048
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

Related Commands

Command	Description
set cert	Enters an RSA certificate for a keyring.
set regenerate	Regenerates the RSA keys in the default keyring.
set trustpoint	Specifies whether the keyring certificate can be regenerated.

set nd

To enable or disable the IPv6 ND support on the firepower device, use the **set nd** command in fabric interconnect mode.

set nd [**enable** | **disable**]

Syntax Description

enable	Enables the rdnssd (ipv6 recursive dns server discovery daemon) to run, once it is set to enable.
disable	Disables the rdnssd daemon in the firepower device.

Command Modes

scope fabric-interconnect/scope ipv6-config

Command History

Release	Modification
2.13(1)	Command added.

Usage Guidelines

By default, ND will not be set. Use this command to enable or disable IPv6.

Example

This example shows how to enable ND in a firepower device:

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set nd enable
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set out-of-band

To change the management IP address for the device, use the **set out-of-band** command.

For an IPv4 address:

set out-of-band {**gw** *gateway_address* | **ip** *ip_address* | **netmask** *network_mask*}

For an IPv6 address:

set out-of-band {**ipv6** *ipv6_address* | **ipv6-gw** *ipv6_gateway* | **ipv6-prefix** *ipv6_prefix*}

Syntax Description

gw *gateway_address*	Provide an IPv4 gateway address.
ip *ip_address*	Provide an IPv4 address for device management access.
netmask *network_mask*	Provide a netmask for the IPv4 address.
ipv6 *ipv6_address*	Provide an IPv6 address for device management access.
ipv6-gw *ipv6_gateway*	Provide an IPv6 gateway address.
prefix *ipv6_prefix*	Provide a prefix length for the IPv6 address.

Note Only IPv6 Global Unicast addresses are supported as the chassis's IPv6 management address.

Command Modes

IPv4 address: fabric interconnect mode

IPv6 address: IPv6 configuration (fabric-interconnect/ipv6-config) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After changing the management IP address, you will need to re-establish any existing connections using the new address.

You can enter the three keywords and variables, for either IP address type, in any order on one command line. See the following examples.

Note Only IPv6 Global Unicast addresses are supported as the chassis's IPv6 management address.

Examples

This example shows how to display the current IPv4 management interface and gateway addresses, and specify new addresses:

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # show
```

```
Fabric Interconnect:
ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
Prefix Operability
---- --------------- --------------- --------------- ---------------- ----------------
------ -----------
A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::               64
    Operable
FP9300-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw
192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect #
```

This example shows how to display the current IPv6 management interface and gateway addresses, and specify new addresses:

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address                       Prefix     IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998                         64         2001::1
FP9300-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999 ipv6-prefix 64
 ipv6-gw 2001::1
FP9300-A /fabric-interconnect/ipv6-config* # commit-buffer
FP9300-A /fabric-interconnect/ipv6-config #
```

Command	Description
show	Shows the current device management IP addresses.
show ipv6-if	Shows the current device management IPv6 address.

set password

To specify the password for a user account, use the **set password** command.

set password

Syntax Description

This command has no arguments or keywords.

Command Modes

`scope security/` – to change the password for the currently logged-in user

`scope security/scope local-user/` – to specify a password for the current local user

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

After entering the **set password** command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI window.

This password must be a minimum of eight characters and a maximum of 80 characters. Use set min-password-length, on page 312 to define a specific minimum number of characters. Use set enforce-strong-password, on page 281 to require use of "strong" passwords.

Example

This example shows how to enter security mode, create a new local user account and specify a password for that user:

```
firepower# scope security
firepower /security # create local-user test_user
firepower /security/local-user* # set password
Enter a password:
Confirm the password:
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Command	Description
create local-user	Creates a new local-user account.
set expiration	Specifies the date on which the user account expires.

set password-encryption-key

To specify a key for use when encrypting sensitive information during configuration export, use the **set password-encryption-key** command.

set password-encryption-key

Syntax Description

This command has no arguments or keywords. After you enter the command, you are asked to enter and confirm an encryption key.

The key can be between four and 40 characters long; the key you enter is then used to generate a 128-bit MD5 hash value.

Command Modes

scope security/

Command History

Release	Modification
2.6.1	Command added.

Usage Guidelines

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Beginning with FXOS 2.6.1, you must specify a key for use when encrypting sensitive information such as passwords and other secret keys during configuration export, and you must have specified it before you attempt to export the configuration.

Also, the same key used during export must be set on the target system when you import an exported configuration, unless the file was exported from an FXOS release prior to 2.6.1, in which case the target system will allow the import.

Once a password encryption key is set, it cannot be changed or deleted unless you perform a factory-reset or password-recovery. Factory-reset or password-recovery will clear the key as if it had never been set.

Example

This example shows how to specify a password encryption key prior to exporting the current configuration:

```
firepower # scope security
firepower /security # set password-encryption-key
Enter a key:
Confirm the key:
Warning: Please make note of the encryption key configured. If you change the key, importing
 configurations that were exported with the previous key will fail, because Import and
Export requires the same encryption key on the system.
firepower /security* # commit-buffer
firepower /security #
```

Related Commands

Command	Description
cfg-export-policy	Configures an export policy.
export-config	Exports the current system configuration to a remote server as an XML file.
import-config	Copies a previously exported XML configuration file to this appliance.

set (password-profile)

To specify or change local-user password-profile parameters, use the **set** command in password-profile mode.

set { **change-count** | **change-during-interval** | **change-interval** | **history-count** | **no-change-interval** }

Syntax Description

change-count *count*	The maximum number of times a user can change his or her password (during the time period specified with **set change-interval**); value can be 0 to 10.
change-during-interval { **disable** | **enable** }	Enable or disable restrictions on the number of password changes a locally authenticated user can make: • `disable` – Disables restrictions on the number of password changes. • `enable` – Enables restrictions on the number of password changes. This option must be enabled before you can specify the maximum number of times a locally authenticated user can change his or her password, and the number of hours over which that number of password changes can be made.
change-interval *interval*	The interval over which a user's password changes are tallied to ensure they do not exceed the maximum number specified with the **set change-count** command; the number of hours can be 1 to 745. The **set change-during-interval** option must be enabled before you can specify this interval.
history-count *count*	The number of unique passwords that a locally authenticated user must create before that user can re-use a previously used password; value can be 0 to 15. By default, the *count* value is zero, which disables the password history count, allowing users to re-use previously used passwords at any time.
no-change-interval *hours*	The length of time in hours during which a user cannot change her or his password again; value can be 1 to 745. The **set change-during-interval** option must be disabled before you set this time period, otherwise this value is ignored.

Command Modes

scope security/scope password-profile/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The **set change-during-interval** option must be enabled before you can specify the maximum number of times a locally authenticated user can change his or her password, and the number of hours over which that number of password changes can be made.

By default, the **set history-count** value is zero, which disables the password history count, allowing users to re-use previously used passwords at any time.

Examples

This example shows how to enter password profile mode, enable password-change restrictions, specify that a user can change his or her password only twice in any 48-hour period, and then view the current settings:

```
firepower # scope security
firepower /security # scope password-profile
firepower /security/password-profile # set change-during-interval enable
firepower /security/password-profile* # set change-count 2
firepower /security/password-profile* # set change-interval 48
firepower /security/password-profile* # commit-buffer
firepower /security/password-profile # show detail

Password profile:
    Password history count: 5
    No password changes allowed (in Hours): 24
    Password change during interval: Enable
    Password change interval (in Hours): 48
    Password change count: 2
firepower /security/password-profile #
```

Related Commands

Command	Description
show detail	Displays the current password-profile settings.

set phone

To set a contact telephone number for a user account, use the **set phone** command.

set phone *tel_number*

Syntax Description

tel_number	A contact telephone number for the user account; maximum of 20 characters.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to specify an telephone number for the current local user:

```
FP9300-A /security/local-user # set phone +1-408-555-1212
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
set phone-contact	Specifies a contact telephone number for a Smart Call Home account.

set (port-channel)

To specify or edit the parameters for an existing port-channel, use the **set** command in port-channel mode.

set { **auto-negotiation** | **descr** | **duplex** | **flow-control-policy** | **lacp-policy-name** | **nw-ctrl-policy** | **port-channel-mode** | **port-type** | **speed** }

Syntax Description

auto-negotiation { **no** | **yes** }	Enables or disables auto-negotiation of common transmission parameters such as speed, duplex and flow control. • **no** – Disables auto-negotiation. • **yes** – Enables auto-negotiation.
descr *description*	You can add a description to the port-channel; the description can be between zero and 256 characters. Most alphanumeric characters are allowed, as are dashes and underscores; spaces are not allowed. The string can end with punctuation such as semi-colon, period (full stop), and exclamation point, but you cannot embed those characters in the description.
duplex { **fullduplex** | **halfduplex** }	Defines the duplex mode for the port-channel: • **fullduplex** – Specifies simultaneous two-way communications. • **halfduplex** – Specifies one-way-at-a-time communications.
flow-control-policy *name*	You can assign a flow-control policy to the port-channel; provide the policy name, which can be up to 16 alphanumeric characters.
lacp-policy-name *name*	You can assign a LACP policy to the port-channel; provide the policy name, which can be up to 16 alphanumeric characters.
nw-ctrl-policy *name*	You can assign a network-control policy to the port-channel; provide the policy name, which can be up to 16 alphanumeric characters.
port-channel-mode { **active** | **on** }	Define the mode for the port-channel's physical data or data-sharing interfaces: • **active** – Sends and receives LACP updates. An active port-channel can establish connectivity with either an active or a passive port-channel. You should use the active mode unless you need to minimize the amount of LACP traffic. This is the default. • **on** – The port-channel is always on, and LACP is not used. An "on" port-channel can only establish a connection with another "on" port-channel. Non-data interfaces support only active mode.

port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}	Specify the port-channel type or function: • **cluster** – Specify **cluster** only if you want to use this port-channel as the cluster control link. • **data** – Use for regular data transmission. This is the default type. • **data-sharing** – Use for regular data; only supported with container instances. • **firepower-eventing** – Use this port-channel as a secondary management interface for threat defense devices. The firepower-eventing port-channel is used to carry all event traffic (such as Web events). • **mgmt** – Use to manage application instances. You can only assign one management interface per logical device. See set port-type, on page 329 for more information about this command.
speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps**}	Specify the port data-transfer speed: • **100gbps** – One hundred Gigabits per second. • **100mbps** – One hundred Megabits per second. • **10gbps** – Ten Gigabits per second. • **10mbps** – Ten Megabits per second. • **1gbps** – One Gigabit per second. • **40gbps** – Forty Gigabits per second.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.4(1)	We added the **data-sharing** type.
1.1(4)	We added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

Assign member interfaces to the port-channel before using this command to set parameters.

The LACP port-channel mode applies to data and data-sharing interfaces only. For non-data and non-data-sharing interfaces, the mode is always `active`.

The type `cluster` is a special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on port-channel 48.

Data interfaces cannot be shared between logical devices.

The type `data-sharing` is supported only with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number

of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.

A `firepower-eventing` interface is a secondary management interface for threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as Web events). See the "Management Interfaces" section in the *System Configuration* chapter of the Management Center configuration guide. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.

Use `mgmt` interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

If you edited the default flow control policy, it is already applied to interfaces. If you created a new policy, you can apply it to the port-channel.

Example

The following example creates Port-Channel 1 with four member interfaces, sets the type to data, and sets the EtherChannel to On mode.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface.
scope interface	Enters a physical interface so you can configure and manage the interface settings.

set port-channel-mode

To set the port channel mode for an EtherChannel, use the **set port-channel-mode** command.

set port-channel-mode {**active** | **on**}

Syntax Description

active	Sets the interface in an EtherChannel to be active.
on	Sets the interface in an EtherChannel to be on. Only supported for Data or Data-sharing interfaces.

Command Default

The default mode is active.

Command Modes

scope eth-uplink/scope fabric a/create port-channel/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

You can configure each physical Data or Data-sharing interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- On—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.

Non-data interfaces only support active mode.

Example

The following example adds Port-Channel 1 with 4 member interfaces, sets the type to data, and sets the EtherChannel to On mode.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface.
create member-port	Assigns a member to the EtherChannel.
set port-type	Sets the interface type.

set port-type

To set the port type for an interface, use the **set port-type** command.

set port-type { **cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt** }

Syntax Description

cluster	Special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on port-channel 48. For multi-instance clustering, you cannot share a Cluster-type interface across devices. You can add VLAN subinterfaces to the Cluster EtherChannel to provide separate cluster control links per cluster. If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster. device manager does not support clustering.
data	Data interfaces cannot be shared between logical devices.
data-sharing	Only supported with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, clusters,or failover links.
firepower-eventing	This interface is a secondary management interface for threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as web events). See the "Management Interfaces" section in the *System Configuration* chapter of the Management Center configuration guide. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.
mgmt	Use management interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.

Command Default

The default type is data.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

Command History

Release	Modification
2.8(1)	You can set the **cluster** type on a VLAN subinterface for use with multi-instance clustering.
2.4(1)	We added the **data-sharing** type.
1.1(4)	We added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

Container instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

In addition to the forwarding table, the chassis maintains a VLAN group table for VLAN subinterface forwarding. Depending on the number of parent interfaces and other deployment decisions, you can create up to 500 VLAN subinterfaces.

See the following limits for shared interface allocation:

- Maximum 14 instances per shared interface. For example, you can allocate Ethernet1/1 to Instance1 through Instance14.
- Maximum 10 shared interfaces per instance. For example, you can allocate Ethernet1/1.1 through Ethernet1/1.10 to Instance1.

See the following table for interface type support for FTD and ASA applications in standalone and cluster deployments.

Table 4: Interface Type Support

Application		Data	Data: Subinterface	Data-Sharing	Data-Sharing: Subinterface	Mgmt	Firepower-Eventing	Cluster (EtherChannel only)	Cluster: Subinterface
FTD	Standalone Native Instance	**Yes**	—	—	—	**Yes**	**Yes**	—	—
	Standalone Container Instance	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	—	—
	Cluster Native Instance	**Yes** (EtherChannel only for inter-chassis cluster)	—	—	—	**Yes**	**Yes**	**Yes**	—
	Cluster Container Instance	**Yes** (EtherChannel only for inter-chassis cluster)	—	—	—	**Yes**	**Yes**	**Yes**	**Yes**
ASA	Standalone Native Instance	**Yes**	—	—	—	**Yes**	—	**Yes**	—
	Cluster Native Instance	**Yes** (EtherChannel only for inter-chassis cluster)	—	—	—	**Yes**	—	**Yes**	—

Examples

The following example adds Port-Channel 1 with 4 member interfaces, sets the type to data, and sets the EtherChannel to On mode.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

```
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

The following example adds three subinterfaces and sets the port type to data-sharing.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/1
firepower /eth-uplink/fabric/interface # enter subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface.
scope interface	Enters a physical interface so you can configure and manage the interface settings.

set port-type (aggr-interface)

To configure the port type for the interface, use the **set port-type** command.

set port-type { *data* | *data-sharing* | *mgmt* | *firepower-eventing* | *cluster* }

Syntax Description

data	(Optional) Data interfaces cannot be shared between logical devices.
data-sharing	(Optional) Only supported with container instances, these data interfaces can be shared by one or more logical devices/container instances (FTD-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.
mgmt	(Optional) Use management interfaces to manage application instances. They can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device.
firepower-eventing	(Optional) This interface is a secondary management interface for FTD devices. To use this interface, you must configure its IP address and other parameters at the FTD CLI. For example, you can separate management traffic from events (such as web events). See the "Management Interfaces" section in the Management Center configuration guide System Configuration chapter. Firepower-eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.
cluster	(Optional) Special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on Port-channel 48.

Command Modes

scope cabling/scope fabric a/

Command History

Release	Modification
2.4(1)	Added the **data-sharing** type.
1.1(4)	Added the **firepower-eventing** type.
1.1(1)	Command added.

Usage Guidelines

Container instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance

must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

Example

The following example shows to configure the interface port-type and then list the available commands:

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
```

The system reboots after you use the `commit-buffer` command.

```
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    Afirepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information
```

```
firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* #
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type
  cluster             Cluster
  data                Data
  data-sharing        Data Sharing
  firepower-eventing  Firepower Eventing
  mgmt                Mgmt

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type cluster
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create port-channel	Adds an EtherChannel interface
scope interface	Edits a physical interface.

set prefix

To set the MAC address prefix to use when autogenerating MAC addresses for container instance interfaces, use the **set prefix** command.

set prefix *prefix*

Syntax Description

prefix	Specifies a decimal value between 1 and 65535. This prefix is converted to a four-digit hexadecimal number, and used as part of the MAC address.

Command Modes

scope ssa/scope auto-macpool/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

The FXOS chassis automatically generates MAC addresses for container instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the application, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the application.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.

Note Even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

The FXOS chassis generates the MAC address using the following format:

A2*xx.yyzz.zzzz*

Where *xx.yy* is a user-defined prefix or a system-defined prefix, and *zz.zzzz* is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xxyy*) to match the chassis native form:

A2**4D**.**00***zz.zzzz*

For a prefix of 1009 (03F1), the MAC address is:

A2**F1**.**03***zz.zzzz*

Example

The following example sets the MAC prefix to 33.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool # set prefix 33
firepower /ssa/auto-macpool* # commit-buffer
firepower /ssa/auto-macpool
```

Related Commands

Command	Description
scope ssa	Enters ssa mode.
scope auto-macpool	Enter auto-macpool mode.
show mac-address	Shows the assigned MAC addresses.

set protocol

To specify the protocol to use when communicating with the remote server for the export policy, use the **set protocol** command.

set protocol { **ftp** | **scp** | **sftp** | **tfp** }

Syntax Description

ftp	Specifies the File Transfer Protocol (FTP) for file transfer.
scp	Specifies the Secure Copy Protocol (SCP) for file transfer.
sftp	Specifies the Secure File Transfer Protocol (SFTP) for file transfer.
tfp	Specifies the Trivial File Transfer Protocol (TFTP) for file transfer.

Command Modes

Configuration export policy (/org/cfg-export-policy)

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

Use this command to specify a file transfer protocol.

Example

This example shows how to set the port number for the export policy:

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-policy default
firepower-9300 /org/cfg-export-policy* # set protocol scp
firepower-9300 /org/cfg-export-policy* # commit-buffer
firepower-9300 /org/cfg-export-policy #
```

Related Commands

Command	Description
set adminstate (/org)	Enables the export policy.
set hostname (/org)	Specifies the hostname location where the backup file must be stored.
set password (/org)	Specifies the password for the remote server username.
set port (/org)	Specifies the port number.
set protocol (/org)	Specifies the protocol to use when communicating with the remote server.
set remote-file (/org)	Specifies the full path to where you want the configuration file exported including the filename.
set schedule (/org)	Specifies the schedule on which you would like to have the configuration automatically exported.

Command	Description
set user (/org)	Specifies the username the system should use to log in to the remote server.

set realm

To specify the default authentication service, use the **set realm** command.

set realm {**ldap** | **local** | **none** | **radius** | **tacacs**}

Syntax Description

ldap	Specifies LDAP authentication.
local	Specifies local authentication.
none	Allows local users to log on without specifying a password.
radius	Specifies RADIUS authentication.
tacacs	Specifies TACACS+ authentication.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter security/default-auth mode and set the default authentication service to Radius:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set realm radius
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set auth-server-group	Specifies an associated authentication provider group.
set use-2-factor	Sets the authentication method to two-factor authentication for a Radius or TACACS+ realm.

set refresh-period

To set the Web session refresh period—the maximum time allowed between refresh requests for a user in this domain—use the **set refresh-period** command.

set refresh-period *seconds*

Syntax Description

seconds	Number of seconds after which a Web session is considered inactive. Value can be 0 to 3600 seconds; default is 600 seconds.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If this time limit is exceeded, FXOS considers the Web session to be inactive, but it does not terminate the session.

Example

This example shows how to enter default authentication mode and set the session refresh interval:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set refresh-period 800
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set timeout values	The **set absolute-session-timeout**, **set con-absolute-session-timeout**, **set con-session-timeout**, and **set session-timeout** commands are used to set various timeout values.

set regenerate

To regenerate the keys in the default keyring, use the **set regenerate** command.

set regenerate {**no** | **yes**}

Syntax Description

no	Do not regenerate the keys.
yes	Regenerate the keys.

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to regenerate the RSA keys in the default keyring. This command is accepted only in the default keyring.

Example

This example shows how to regenerate the keys in the default keyring:

```
FP9300-A# scope security
FP9300-A /security # scope keyring default
FP9300-A /security/keyring # set regenerate yes
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

Related Commands

Command	Description
set cert	Enters an RSA certificate for a keyring.
set modulus	Specifies the RSA key modulus (SSL key length) in bits.
set trustpoint	Specifies whether the keyring certificate can be regenerated.

set remote-address

To specify the remote IP address for an IPSec connection, use the **set remote-address** command.

set remote-address *ip_address*

Syntax Description

ip_address	Provide an IPv4 or IPv6 remote gateway address for the IPSec connection; maximum of 510 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command and the **set local-address** command to define the endpoints of an IPSec connection.

Example

This example shows how to set the remote address for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.202.129
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set local-addr	Sets the local IP address for an IPSec connection.

set remote-ike-ident

To specify the remote peer IKE identity for an IPSec tunnel connection, use the **set remote-ike-ident** command.

set remote-ike-ident *remote_ID*

Syntax Description

remote_ID	The IKE identification of the remote peer; maximum of 510 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the remote peer's IKE ID for an IPSec connection. This identification is used for peer validation during IKE negotiations.

Example

This example shows how to specify the remote IKE ID for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-ike-ident 203.0.113.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set remote-subnet

To specify the remote subnet for an IPSec tunnel connection, use the **set remote-subnet** command.

set remote-subnet *ip_address/mask_bits*

Syntax Description

ip_address/mask_bits	Provide an IPv4 or IPv6 remote subnet address/mask for the IPSec connection; maximum of 510 characters.

Command Modes

Connection (/security/ipsec/connection) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the IP address/mask of an IPSec connection's remote subnet.

Example

This example shows how to set the remote subnet for an IPSec connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-subnet 209.165.202.128/27
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Command	Description
create connection	Creates a new IPSec connection.
set remote-addr	Sets the remote IP address for an IPSec connection.

set remote-user

To restrict access to those users matching an established user role, use the **set remote-user** command.

set remote-user default-role { **assign-default-role** | **no-login** }

Syntax Description

assign-default-role	When a user attempts to log in and the remote authentication provider does not supply a user role with the user's authentication information, the user is allowed to log in with a read-only user role.
no-login	When a user attempts to log in and the remote authentication provider does not supply a user role with the user's authentication information, access is denied.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

assign-default-role is the default behavior.

Example

This example shows how to enter security mode and deny access to users without a user role:

```
FP9300-A# scope security
FP9300-A /security # set remote-user default-role no-login
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
set authentication	Specifies the default authentication service.

set reporting-interval

To define how frequently monitored statistics are reported, use the **set reporting-interval** command.

set reporting-interval *interval*

Syntax Description

interval	Length of time defining the statistics reporting interval; available values are: • `15minutes` – 15-minute intervals • `2hours` – two-hour (120-minute) intervals • `2minutes` – two-minute intervals • `30minutes` – 30-minute intervals • `4hours` – four-hour (240-minute) intervals • `60minutes` – 60-minute (one-hour) intervals • `8hours` – eight-hour (480-minute) intervals

Command Modes

scope monitoring/scope stats-collection-policy/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **set collection-interval** command to define how frequently statistics are collected, and use the **set reporting-interval** command to define how frequently the statistics are reported. These intervals define a statistics collection policy.

Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides sufficient data to calculate and report minimum, maximum, and average values.

Statistics can be collected and reported for each of the following functional areas of your Firepower system; use the **scope stats-collection-policy** command to access a specific collection policy:

- `Adapter` – statistics related to the adapters.
- `Chassis` – statistics related to the blade chassis.
- `FEX` – statistics related to configured Fabric Extender(s).
- `Host` – this policy is a placeholder for future support.
- `Port` – statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports.
- `Server` – statistics related to servers.

Note There is one default statistics collection policy for each of the functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Example

This example shows how to enter the statistics collection policy for ports, set the collection interval to one minute, set the reporting interval to 30 minutes, and then commit the transaction:

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Related Commands

Command	Description
scope stats-collection-policy	Enters stats-collection-policy mode, where you manage statistics collection and reporting intervals.
set collection-interval	Specifies how frequently statistics are collected.

set resource-profile-name

To set the resource profile for an application instance, use the **set resource-profile-name** command.

set resource-profile-name *profile_name*

Syntax Description

profile_name	Sets the resource profile name for this application instance.

Command Modes

scope ssa/scope slot/create app-instance/

Command History

Release	Modification
2.4(1)	Can now be used for container instances.
1.1(1)	Command added for use with vDP.

Usage Guidelines

For vDP, resource profiles are pre-created in the FXOS configuration when you download the vDP image. For container instances, create resource profiles using the **create resource-profile**command. Use the **show resource-profile system** command to view available profiles.

If you change the resource profile for an application instance that is running, then the instance reboots.

Example

The following example shows how to set the the resource profile for a vDP application instance:

```
firepower# scope ssa
firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default App

    ---------- --------------- ---------- ---------------------- ----------- --------------

    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes

firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
----------------- ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
VDP-10-CORES       vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES         vdp        8.13.01.09-2 No         all
 2           8192 No              System
```

```
VDP-4-CORES        vdp        8.13.01.09-2 No         all
 4          16384 No             System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 8          32768 No             System
firepower /ssa/app # exit
firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance vdp VDP1
firepower /ssa/slot/app-instance* # set resource-profile-name VDP-10-CORES
firepower /ssa/slot/app-instance* #
```

Example

The following example shows how to set the the resource profile for a threat defense container instance:

```
firepower# scope ssa
firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
bronze              N/A        N/A          No         all
 6            N/A No              Custom       low end device
silver              N/A        N/A          No         all
 8            N/A No              Custom       mid-level

firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance ftd FTD1
firepower /ssa/slot/app-instance* # set resource-profile-name silver
firepower /ssa/slot/app-instance* #
```

Related Commands

Command	Description
show app-attri	Shows current application attributes.
create resource-profile	Creates a resource profile for use with constainer instances.
show resource-profile-name	Shows available resource profiles.

set session-timeout

To set the idle session timeout for Web, SSH, and Telnet sessions, use the **set session-timeout** command.

set session-timeout *seconds*

Syntax Description

seconds	Idle session timeout for Web, SSH, and Telnet sessions; value can be 0 to 3600 seconds.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the idle session timeout for Web, SSH, and Telnet sessions.

Example

This example shows how to enter default authentication mode and then set the idle session timeout to four minutes:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set refresh-period	Sets the Web session refresh period.
show detail	Displays the current session and absolute session timeout settings.

set snmp

To set Simple Network Management Protocol (SNMP) configuration parameters, use the **set snmp** command.

set snmp {**community** | **syscontact** | **syslocation**}

Syntax Description

community	After you enter this command, you are asked to enter a SNMP community name, which can be between 1 and 32 alphanumeric characters. The community name is not displayed as you type; however after you press **Enter**, the system prompt is displayed with an asterisk indicating you need to commit the buffer.
syscontact *name*	Enter the name of the person to contact regarding SNMP on this system; can be 0 to 255 alphanumeric characters.
syslocation *location*	Enter a location for this system; can be 0 to 510 alphanumeric characters.

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Cisco recommends that you enable only the communication services needed to interact with other network applications.

You must enable the SNMP agent (**enable snmp**) before configuring SNMP on this system.

Use **set snmp community** to specify the community access string used to permit access to the SNMP trap destination. If SNMPv1 or v2c is set as the SNMP version, the community argument is used as the community string. If SNMPv3 is configured, it is used as the SNMP user name for sending trap messages.

When you specify an SNMP community name, you are also automatically enabling SNMP versions 1 and 2c for polling requests from the SNMP remote manager.

Note Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.

There can be only one community name; however, you can use **set snmp community** to overwrite the existing name. To delete an existing community name, enter **set snmp community** but do not type a community string; that is, simply press **Enter** again. After you commit the buffer, **show snmp** output will include the line `Is Community Set: No`.

Example

The following example shows you how to scope into monitoring mode, enable SNMP processing, set the SNMP community string and a system contact, commit your changes, and use the **show snmp** command to confirm the changes:

```
firepower # scope monitoring
firepower /monitoring # enable snmp
firepower /monitoring* # set snmp community
Enter a snmp community:
firepower /monitoring* # set snmp syscontact R_Admin
firepower /monitoring* # commit-buffer
firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Related Commands

Command	Description
disable snmp	Disables SNMP.
enable snmp	Enables SNMP.
show snmp	Shows the current SNMP configuration.

set (snmp-trap)

To specify Simple Network Management Protocol (SNMP) trap parameters, use the **set** command in snmp-trap mode.

set { **community** | **notificationtype** | **port** | **v3privilege** | **version** }

Syntax Description

community	Specifies the SNMPv1/v2c community string, or the SNMPv3 user name, to permit access to the trap destination. You are queried for the community name after you enter this command. The name can be up to 32 characters with no spaces; the name is not displayed as you type.
notificationtype { **informs** | **traps** }	Specifies the type of SNMP notification produced by this agent: • **informs** – These are unsolicited notifications sent to notify the manager of significant local events. These messages are acknowledged. This option can be used only if **version** is set to **vc2**. • **traps** – These are unsolicited notifications sent to notify the manager of significant local events. These messages are not acknowledged.
port *port_num*	Use this command to change the port on which the agent receives SNMP requests; the default port is 161.
v3privilege { **auth** | **noauth** | **priv** }	Use this command to specify the Simple Network Management Protocol version 3 (SNMPv3) security level for the transmitted SNMP traps. • **auth** – Specifies keyed-hash authentication but no encryption. • **noauth** – Specifies no authentication or encryption. Note that while you can specify it, FXOS does not support this security level with SNMPv3. • **priv** – Specifies keyed-hash authentication and data encryption (privacy).
version { **v1** | **v2c** | **v3** }	Use this command to specify the SNMP security model used when sending trap notifications: • **v1** – Specifies SNMP version 1. • **v2c** – Specifies SNMP version 2c. • **v3** – Specifies SNMP version 3. **Note** Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.

Command Modes

scope monitoring/snmp-trap

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must enable SNMP (**enable snmp**), and create an SNMP community (**set snmp community**), before you create an SNMP trap and set these parameters.

When you create a new SNMP trap, you are automatically entered into monitoring/snmp-trap mode with an asterisk indicating the new trap is not yet committed.

Note You can create up to eight SNMP traps.

If SNMPv1 or v2c is configured with **set version**, the **set community** argument is used as the community string. If SNMPv3 is configured, it is used as the user name for transmitting the notifications.

With SNMPv3, the trap's **v3privilege** setting must be compatible with the associated SNMPv3 user's security level; that is, the associated user's security configuration must be at least as secure as the trap's. For example, if authentication is enabled for the SNMPv3 user (perform authentication but not privacy encryption), then the user's priv-password would not be set. But to send notifications with privacy enabled (that is, authenticate and do privacy encryption) the user's priv-password would be set. The password associated with the SNMPv3 user is used to authenticate the user when a trap/inform is sent.

Example

The following example enables SNMP, creates an SNMP trap using an IPv4 address, sets the version to v3, sets the v3 privilege level to privacy, and commits the transaction:

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # set notificationtype traps
firepower /monitoring/snmp-trap* # set version v3
firepower /monitoring/snmp-trap* # set v3privilege priv
firepower /monitoring/snmp-trap* # commit-buffer
firepower /monitoring/snmp-trap #
```

Related Commands

Command	Description
create snmp-trap	Creates a new SNMP trap destination.
enable snmp	Enables SNMP.

set (snmp-user)

To specify parameters for an existing Simple Network Management Protocol (SNMP) v3 user, use the **set** command in `snmp-user` mode.

set {**aes-128** | **auth** | **password** | **priv-password**}

Syntax Description

aes-128 {**no** | **yes**}	Disable or enable the use of Advanced Encryption Standard (AES)-128 encryption: enter `no` or `yes`. By default, AES-128 encryption is disabled.
auth sha	Enables authentication for SNMPv3 users based on the HMAC Secure Hash Algorithm (SHA).
password	Specify a password for this user; you are asked to enter the password, and confirm it, after you enter this command.
priv-password	Specify a user privacy password; you are asked to enter the password, and confirm it, after you enter this command. The AES privacy password must be a minimum of eight characters.

Command Modes

scope monitoring/snmp-user

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must enable SNMP (**enable snmp** before you create an SNMP user and set these parameters.

When you create a new SNMP user, you are automatically entered into monitoring/snmp-user mode with an asterisk indicating the new user is not yet committed.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, the Firepower chassis uses the privacy password to generate a 128-bit AES key.

Example

The following example creates an SNMPv3 user named `snmp-user14`, enables AES-128 encryption, sets a privacy password, and commits the transaction:

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user snmp-user14
Password:
firepower /monitoring/snmp-user* # set aes-128 yes
firepower /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
firepower /monitoring/snmp-user* # commit-buffer
firepower /monitoring/snmp-user #
```

Related Commands

Command	Description
create snmp-user	Creates a new SNMPv3 user.
enable snmp	Enables SNMP.

set speed

To set the interface speed., use the **set speed** command.

Note This command is available in port-channel scope only.

set speed { **10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps** }

Syntax Description

10mbps	(Optional) Sets the speed at 10 Mbps.
100mbps	(Optional) Sets the speed at 100 Mbps.
1gbps	(Optional) Sets the speed at 1 Gbps.
10gbps	(Optional) Sets the speed at 10 Gbps.
40gbps	(Optional) Sets the speed at 40 Gbps.
100gbps	(Optional) Sets the speed at 100 Gbps.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.4.1(1)	Command added.

Usage Guidelines

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

Example

This example shows how to set the interface speed:

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
duplex	Specifies the duplex mode as full or half.

Command	Description
show interface	Displays the interface status, which includes the speed parameters.

set speed (aggr-interface)

To set the speed of the interface, use the **set speed** command.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

Syntax Description

10mbps	(Optional) Sets the speed at 10 Mbps.
100mbps	(Optional) Sets the speed at 100 Mbps.
1gbps	(Optional) Sets the speed at 1 Gbps.
10gbps	(Optional) Sets the speed at 10 Gbps.
40gbps	(Optional) Sets the speed at 40 Gbps.
100gbps	(Optional) Sets the speed at 100 Gbps.

Command Modes

scope eth-uplink/scope fabric a/port-channel/

Command History

Release	Modification
2.4.1(1)	Command added.

Usage Guidelines

The interface speed that you specify can affect the duplex mode used for an interface, so you must set the speed before setting the duplex mode. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1Gbps) or faster, full duplex is automatically used.

This example shows how to set the interface speed:

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    A
firepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
```

```
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information

firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
  100gbps  100 Gbps
  100mbps  100 Mbps
```

```
  10gbps   10 Gbps
  10mbps   10 Mbps
  1gbps    1 Gbps
  40gbps   40 Gbps

firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
duplex	Specifies the duplex mode as full or half.
show interface	Displays the interface status, which includes the speed parameters.

set ssh-server

To set the SSH host key size, use the **set ssh-server** command.

set ssh-server host-key rsa *key_size*

Syntax Description

rsa	Specifies the host key type.
key-size	The size of the host key.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to set the SSH host key size.

Example

This example shows how to set the SSH host key size to 2048 bits:

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # set ssh-server host-key rsa 2048
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

Related Commands

Command	Description
create ssh-server	Creates a new SSH server host key.
delete ssh-server	Deletes the existing SSH host key.
show ssh-server	Shows the host key size.

set sshkey

To specify an SSH key that allows access without a password, use the **set sshkey** command.

set sshkey [**none** | *user_ssh_key*]

Syntax Description

none	(Optional) Enter the **none** keyword to clear the user's SSH public key.
user_ssh_key	(Optional) Enter or paste the user's public SSH key.

Command Modes

Local user mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you press **Enter** after entering **set sshkey**, you are prompted to provide the SSH key, one line at a time. Enter ENDOFBUF to finish. Press Ctrl-C to abort.

Example

This example shows how to specify a public SSH key for the current local user:

```
FP9300-A /security/local-user # set sshkey
"ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
 m8HPh2LOgyH7Ei1MI8="
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Related Commands

Command	Description
create local-user	Creates a new local-user account.
set password	Specifies a password for a user account.

set startup-version

To specify the startup version of an application, use the **set startup-version** command.

set startup-version

Syntax Description

startup-version	The startup software version of an application instance

Command Modes

scope ssa

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you press **Enter** after **scope app-instance ftd ftd1** , you are prompted to set the startup version.

Example

This example shows how to set the startup version for an ftd application:

```
FPR# scope ssa
FPR /ssa # scope slot 1
FPR /ssa/slot # scope app-instance ftd ftd1
FPR /ssa/slot/app-instance # set startup-version 6.6.1.91
Warning: Upgrade of ftd through FXOS is not supported. The specified version of ftd will
be installed. Please reinitialize or reinstall ftd.
```

set timezone

To set the timezone in FXOS, use the **set timezone** command.

set timezone

Syntax Description

set timezone	Use the command set timezone to set the timezone in FXOS

Command Modes

scope system/scope services

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to set the timezone in FXOS.

Example

This example shows how to set the timezone in FXOS:

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean


#? 8 <====== Europe


Please select a country.
 1) Aaland Islands        18) Greece               35) Norway
 2) Albania               19) Guernsey             36) Poland
 3) Andorra               20) Hungary              37) Portugal
 4) Austria               21) Ireland              38) Romania
 5) Belarus               22) Isle of Man          39) Russia
 6) Belgium               23) Italy                40) San Marino
 7) Bosnia & Herzegovina  24) Jersey               41) Serbia
 8) Britain (UK)          25) Latvia               42) Slovakia
 9) Bulgaria              26) Liechtenstein        43) Slovenia
10) Croatia               27) Lithuania            44) Spain
11) Czech Republic        28) Luxembourg           45) Sweden
12) Denmark               29) Macedonia            46) Switzerland
13) Estonia               30) Malta                47) Turkey
14) Finland               31) Moldova              48) Ukraine
15) France                32) Monaco               49) Vatican City
16) Germany               33) Montenegro
17) Gibraltar             34) Netherlands

#? 36 <======Poland

The following information has been given:
```

```
        Poland

Therefore timezone 'Europe/Warsaw' will be set.
Local time is now:      Sun Oct 24 08:51:04 CEST 2021.
Universal Time is now:  Sun Oct 24 06:51:04 UTC 2021.
Is the above information OK?
1) Yes
2) No


#? 1 <======== Yes

firepower /system/services* # commit
firepower /system/services # show timezone
Timezone: Europe/Warsaw <======= Timezone is set

To set the timezone to UTC:

firepower /system/services* # set timezone UTC
firepower /system/services* # commit
```

set trustpoint

To set the certificate trustpoint for a keyring, use the **set trustpoint** command.

set trustpoint *trustpoint_name*

Syntax Description

trustpoint_name	Name of a defined trustpoint. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Command Modes

scope security/scope keyring/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to specify the trusted point that signed this keyring's certificate.

Example

This example shows how to regenerate the keys in the default keyring:

```
firepower# scope security
firepower /security # scope keyring test-ring
firepower /security/keyring # set trustpoint CiscoCA5
firepower /security/keyring* # commit-buffer
firepower /security/keyring #
```

Command	Description
set cert	Enters an RSA certificate for a keyring.
set modulus	Specifies the RSA key modulus (SSL key length) in bits.
set regenerate	Regenerates the RSA keys in the default keyring.

set use-2-factor

To enable and disable two-factor authentication for the authentication realm, use the **set use-2-factor** command.

Note Two-factor authentication applies only to RADIUS and TACACS+ realms.

set use-2-factor {**no** | **yes**}

Syntax Description

no	Disables two-factor authentication for the realm.
yes	Enables two-factor authentication for the realm.

Command Modes

Default authentication mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the session-refresh and session-timeout periods so that remote users do not have to re-authenticate too frequently.

Example

This example shows how to enter default authentication mode and enable two-factor authentication:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set use-2-factor yes
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Related Commands

Command	Description
set authentication	Specifies the default authentication service.
set timeout values	The **set absolute-session-timeout**, **set con-absolute-session-timeout**, **set con-session-timeout**, and **set session-timeout** commands are used to set various timeout values.

set user-account-unlock-time

To specify the amount of time a user remains locked out of the system after reaching the maximum number of login attempts, use the **set user-account-unlock-time** command.

set user-account-unlock-time *unlock_time*

Syntax Description

unlock_time	The amount of time in seconds a user remains locked out of the system. The value can range from 600 to 36000; the default is 1800 seconds (30 minutes).

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If any user (including admin users) exceeds the specified maximum number of login attempts, the user is locked out of the system and must wait this amount of time before being allowed to log in again. No notification appears indicating that the user is locked out.

Example

This example shows how to enter security mode and specify the amount of time that must pass before a locked-out user can log in again:

```
FP9300-A # scope security
FP9300-A /security # set user-account-unlock-time 900
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Related Commands

Command	Description
clear lock-status	Clears a user's locked-out status.
set max-login-attempts	Specifies the maximum number of failed login attempts before the user is locked out of the system.

set user-label

To assign a user-defined identifier to the appliance chassis, use the **set user-label** command in `chassis/` mode.

To assign a user-defined identifier to one of the installed servers, use the **set user-label** command in `server/` mode.

set user-label *user_label*

Syntax Description

user_label	The label you want assigned to the appliance or server; maximum of 32 characters.

Command Modes

scope chassis/

scope chassis/scope server

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use the **show detail** command in `chassis/` mode to view the user label currently assigned to the chassis.

You can use the **show detail** command in `chassis/server/` mode to view the user label currently assigned to the connected server.

Example

This example shows how to assign a user-defined label to the appliance chassis:

```
firepower # scope chassis 1
firepower /chassis # set user-label FP9300-4
firepower /chassis* # commit-buffer
firepower /chassis # show detail

Chassis:
    Chassis: 1
    User Label: FP9300-4
    Overall Status: Operable
    Oper qualifier: N/A
    Operability: Operable
    Conf State: Ok
    Admin State: Acknowledged
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Product Name: Cisco Firepower 9300 Security Appliance AC
    PID: FPR-C9300-AC
    VID: V02
    Part Number: 68-100280-04
    Vendor: Cisco Systems Inc
    Model: FPR-C9300-AC
    Serial (SN): JMX1950196H
    HW Revision: 0
```

```
    Mfg Date: 2015-12-16T00:00:00.000
    Power State: Ok
    Thermal Status: Ok
    SEEPROM operability status: Operable
    Dynamic Reallocation: Chassis
    Reserved Power Budget (W): 600
    PSU Capacity (W): 0
    PSU Line Mode: High Line
    PSU State: Ok
    Current Task:
firepower /chassis #
```

Related Commands

Command	Description
show detail	In `chassis/` mode, shows detailed chassis information including the chassis' current user label. In `chassis/server/` mode, shows detailed server information including the connected server's user label.

set value (create bootstrap-key FIREWALL_MODE)

To specify the firewall mode, routed or transparent, in the bootstrap configuration for the threat defense and ASA, use the **set value** command.

set value {**routed** | **transparent**}

Syntax Description

routed	Sets the firewall mode to routed firewall mode.
transparent	Sets the firewall mode to transparent firewall.

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key FIREWALL_MODE/

Command Default

The default mode is routed.

Command History

Release	Modification
2.4(1)	Added support for the ASA.
1.1(4)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the mode to routed mode:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create bootstrap-key FIREWALL_MODE	Sets the firewall mode for the application.
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.

set value (create bootstrap-key MANAGEMENT_TYPE)

To specify the manager, FMC or FDM, in the bootstrap configuration for the threat defense, use the **set value** command.

set value {**FMC** | **LOCALLY_MANAGED**}

Syntax Description

FMC	Sets the manager to FDM.
LOCALLY_MANAGED	Sets the manager to FMC.

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key LOCALLY_MANAGED/

Command Default

The default manager is FMC.

Command History

Release	Modification
2.7(1)	Command added for FTD.

Usage Guidelines

Bootstrap settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can change most values in the application CLI configuration.

Example

The following example shows how to set the manager to FDM:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create bootstrap-key FIREWALL_MODE	Sets the firewall mode for the application.
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.

set value (create bootstrap-key PERMIT_EXPERT_MODE)

To permit Expert Mode from FTD SSH sessions for the threat defense, use the **set value** command.

set value {**yes** | **no**}

Syntax Description

no	Disallows Expert Mode from an SSH session to the threat defense.
yes	Allows an Expert Mode from an SSH session to the threat defense.

Command Modes

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key PERMIT_EXPERT_MODE/

Command Default

The default is no.

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

Expert Mode provides FTD shell access for advanced troubleshooting. By default for container instances, Expert Mode is only available to users who access the FTD CLI from the FXOS CLI. This limitation is only applied to container instances to increase isolation between instances. Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the expert command in the FTD CLI.

Example

The following example shows how to enable Expert Mode from SSH:

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Related Commands

Command	Description
create bootstrap-key FIREWALL_MODE	Sets the firewall mode for the application.
create logical-device	Creates the logical device.
create mgmt-bootstrap	Creates the bootstrap configuration for the application.

set vlan

To set the VLAN ID for a subinterface for use with container instances, use the **set vlan** command.

set vlan *id*

Syntax Description

id	Sets the VLAN ID between 1 and 4095.

Command Modes

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

You can add between 250 and 500 VLAN subinterfaces to the chassis, depending on your network deployment.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on *separate* interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

Example

The following example creates 3 subinterfaces on Ethernet 1/1, and sets them to be data-sharing interfaces.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Related Commands

Command	Description
create port-channel	Creates an EtherChannel (port channel).
create subinterface	Adds a subinterface.

Command	Description
scope interface	Enters the physical interface object.
set port-type	Sets the interface type.

sh Commands

show

To view information about operations and current configuration in various command modes, use the **show** command.

Many of the FXOS CLI command modes provide a general **show** command which displays a variety of information relevant to the current command mode. For example, use the **show** command in slot mode (scope ssa/scope slot) to view current SSP information.

Many of these commands are not explicitly documented in this guide. Use **show ?** to view available **show** options for the current command mode.

show app

To display a list of kickstart apps available on the system like ASA and FTD, use the **show app** command.

.

show app [**detail**]

Syntax Description		
	Detail	Displays list of detailed apps information.

Command Modes scope ssa

Command History	Release	Modification
	2.3.1	Command added.

Usage Guidelines This is a subcommand of the **show** command in scope ssa.

Example

This example shows how to display information of all kickstart apps:

```
Firepower /fabric-interconnect # scope ssa
Firepower /ssa # show app

  Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- ----------- ---
-----------
    asa        99.18.20.36     cisco      Native           Application Yes
    ftd        7.2.0.1784      cisco      Native, Container  Application  No
    ftd        7.2.0.83      cisco      Native, Container  Application No
    ftd        7.3.0.1258      cisco      Native, Container  Application No
    ftd        7.3.0.1402      cisco      Native, Container  Application Yes
                   In Cluster      Data Node
```

Example

This example shows how to display information of all the available apps:

```
firepower /ssa # show app detail
        Application:
Name: asa
    Version: 99.18.20.36
    Author: cisco
    Supported Deploy Types: Native
    Is Default App: Yes
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: No
    License Agreement has been Accepted: No
    Time Stamp: 2012-01-27T11:34:37.000
    Validation State: None
```

```
Validation Time Stamp: Never
Application Information:
    Deploy Type: Native
    Description: N/A
    Build Date: 12/16/2021
    Min OS: 92.12.0.122
    Data VNIC NR: 0
    Mgmt VNIC NR: 0
    Security Control: No
    Support Aggregated VNIC: No
    Can Upgrade: Yes
    Full Install: Yes
    Can Downgrade: Yes
    Is Secondary Data Disk Supported: No
    Installation Timeout (sec): 240
    Uninstallation Timeout (sec): 240
    Upgrade Timeout (sec): 360
    Recommended Data Disk (MB): 20481
    Recommended Cpu Cores: 0
    Recommended Ram (MB): 0
    Minimum Required Data Disk (MB): 20481
    Minimum Required Cpu Logical Cores: 16
    Minimum Required Ram (MB): 24576
    Required Binary Disk (MB): 171
    Net Management Bootstrap Type: Appagent
    Is App Agent Supported: Yes
    Is Clustering Supported: Yes
    Is Turbo Mode Supported: No
    Aggregator: Full
    Incompatible Apps: ftd
    Support Customized CCL IP Subnet: Yes
    Max Application Instance Count: 1
    Reboot Module On App Restart: Yes
    Hardware Crypto Version: Unsupported
Name: ftd
Version: 7.2.0.1784
Author: cisco
Supported Deploy Types: Native,Container
Is Default App: No
CSP Type: Application
Is Decorator: No
Has License Agreement: Yes
License Agreement has been Accepted: No
Time Stamp: 2012-01-26T11:16:15.000
Validation State: None
Validation Time Stamp: Never
Application Information:
    Deploy Type: Native
    Description: N/A
    Build Date: 02/28/2022
    Min OS: 92.12.0.122
    Data VNIC NR: 0
    Mgmt VNIC NR: 0
    Security Control: No
    Support Aggregated VNIC: No
    Can Upgrade: No
    Full Install: Yes
    Can Downgrade: No
    Is Secondary Data Disk Supported: Yes
    Installation Timeout (sec): 1800
    Uninstallation Timeout (sec): 600
    Upgrade Timeout (sec): 1800
    Recommended Data Disk (MB): 195313
    Recommended Secondary Disk (MB): 0
```

```
        Recommended Cpu Cores: 0
        Recommended Ram (MB): 0
        Minimum Required Data Disk (MB): 39063
        Minimum Required Secondary Disk (MB): 0
        Minimum Required Cpu Logical Cores: 4
        Minimum Required Ram (MB): 10
        Required Binary Disk (MB): 3907
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: asa
        Support Customized CCL IP Subnet: Yes
        Max Application Instance Count: 1
        Reboot Module On App Restart: Yes
        Hardware Crypto Version: Unsupported
        Deploy Type: Container
        Description: N/A
        Build Date: 02/28/2022
        Min OS: 92.12.0.122
        Data VNIC NR: 0
        Mgmt VNIC NR: 0
        Security Control: No
        Support Aggregated VNIC: No
        Can Upgrade: No
        Full Install: Yes
        Can Downgrade: No
        Is Secondary Data Disk Supported: Yes
        Installation Timeout (sec): 1800
        Uninstallation Timeout (sec): 600
        Upgrade Timeout (sec): 1800
        Recommended Data Disk (MB): 40960
        Recommended Secondary Disk (MB): 102400
        Recommended Cpu Cores: 10
        Recommended Ram (MB): 32768
        Minimum Required Data Disk (MB): 40960
        Minimum Required Secondary Disk (MB): 0
        Minimum Required Cpu Logical Cores: 6
        Minimum Required Ram (MB): 10
        Required Binary Disk (MB): 3907
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: asa
        Support Customized CCL IP Subnet: No
        Max Application Instance Count: 0
        Reboot Module On App Restart: No
        Hardware Crypto Version: 2
Name: ftd
Version: 7.2.0.83
Author: cisco
Supported Deploy Types: Native,Container
Is Default App: No
CSP Type: Application
Is Decorator: No
Has License Agreement: Yes
License Agreement has been Accepted: No
Time Stamp: 2012-01-22T07:04:58.000
Validation State: None
Validation Time Stamp: Never
```

Example

This example shows how to display detailed information of all the available apps:

```
Firepower /ssa # show app expand detail
 Application:
    Application:

    Name: asa
    Version: 99.18.20.36
    Author: cisco
    Supported Deploy Types: Native
    Is Default App: Yes
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: No
    License Agreement has been Accepted: No
    Time Stamp: 2012-01-27T11:34:37.000
    Validation State: None
    Validation Time Stamp: Never
    Application Information:
        Deploy Type: Native
        Description: N/A
        Build Date: 12/16/2021
        Min OS: 92.12.0.122
        Data VNIC NR: 0
        Mgmt VNIC NR: 0
        Security Control: No
        Support Aggregated VNIC: No
        Can Upgrade: Yes
        Full Install: Yes
        Can Downgrade: Yes
        Is Secondary Data Disk Supported: No
        Installation Timeout (sec): 240
        Uninstallation Timeout (sec): 240
        Upgrade Timeout (sec): 360
        Recommended Data Disk (MB): 20481
        Recommended Cpu Cores: 0
        Recommended Ram (MB): 0
        Minimum Required Data Disk (MB): 20481
        Minimum Required Cpu Logical Cores: 16
        Minimum Required Ram (MB): 24576
        Required Binary Disk (MB): 171
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: ftd
        Support Customized CCL IP Subnet: Yes
        Max Application Instance Count: 1
        Reboot Module On App Restart: Yes
        Hardware Crypto Version: Unsupported
        App Attribute Key for the Application:
            App Attribute Key: cluster-role
            Description: This is the role of the blade in the cluster
            App Attribute Key: mgmt-ip
            Description: This is the IP for the management interface
            App Attribute Key: mgmt-ip-virtual
            Description: This is the Virtual IP for cluster only
            App Attribute Key: mgmt-ipv6
            Description: This is the IPv6 for the management interface
            App Attribute Key: mgmt-ipv6-virtual
```

```
            Description: This is the Virtual IPv6 for cluster only
            App Attribute Key: mgmt-url
            Description: This is the management URL for this application
            App Attribute Key: mgmt-url-ipv6
            Description: This is the management IPv6 URL for this application
        Net Mgmt Bootstrap Key for the Application:
            Bootstrap Key: FIREWALL_MODE
            Key Data Type: enum:(routed, transparent)
            Mandatory: No
            Is the Key Secret: No
            Description: This is the mode to set the firewall (transparent routed)
            Key scope: Global
            Bootstrap Key: PASSWORD
            Key Data Type: string
            Mandatory: No
            Is the Key Secret: Yes
            Description: The admin user password.
            Key scope: Global
        Port Requirement for the Application:
            Port Type: Data
            Max Ports: 120
            Min Ports: 1
            Interchassis Supported Port Types: PORT_CHANNEL
            Port Type: Mgmt
            Max Ports: 1
            Min Ports: 0
            Interchassis Supported Port Types:
            Port Type: Cluster
            Max Ports: 1
            Min Ports: 0
            Interchassis Supported Port Types:

    Name: ftd
    Version: 7.3.0.1258
    Author: cisco
    Supported Deploy Types: Native,Container
    Is Default App: No
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: Yes
    License Agreement has been Accepted: No
    Time Stamp: 2012-03-18T13:06:33.000
    Validation State: None
    Validation Time Stamp: Never
    Application Information:
        Deploy Type: Native
        Description: N/A
        Build Date: 04/19/2022
        Min OS: 92.13.0.100
        Data VNIC NR: 0
        Mgmt VNIC NR: 0
        Security Control: No
        Support Aggregated VNIC: No
        Can Upgrade: No
        Full Install: Yes
        Can Downgrade: No
        Is Secondary Data Disk Supported: Yes
        Installation Timeout (sec): 1800
        Uninstallation Timeout (sec): 600
        Upgrade Timeout (sec): 1800
        Recommended Data Disk (MB): 195313
        Recommended Secondary Disk (MB): 0
        Recommended Cpu Cores: 0
        Recommended Ram (MB): 0
```

```
        Minimum Required Data Disk (MB): 39063
        Minimum Required Secondary Disk (MB): 0
        Minimum Required Cpu Logical Cores: 4
        Minimum Required Ram (MB): 10
        Required Binary Disk (MB): 3907
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: asa
        Support Customized CCL IP Subnet: Yes
        Max Application Instance Count: 1
        Reboot Module On App Restart: Yes
        Hardware Crypto Version: Unsupported
        App Attribute Key for the Application:
            App Attribute Key: cluster-role
            Description: This is the cluster role for this application instance
            App Attribute Key: firepower-mgmt-ip
            Description: This is the IP address used to initialize a tunnel with
 Firepower Management Center
            App Attribute Key: firepower-mgmt-ipv6
            Description: This is the IPv6 address used to initialize a tunnel wi
th Firepower Management Center
            App Attribute Key: mgmt-url
            Description: This is the management URL for Firepower Management Cen
ter
            App Attribute Key: NAT_ID
            Description: This is the token used to associate with Firepower Mana
gement Center
        Net Mgmt Bootstrap Key for the Application:
            Bootstrap Key: DNS_SERVERS
            Key Data Type: string
            Mandatory: No
            Is the Key Secret: No
            Description: Comma-separated DNS servers for the application
            Key scope: Global
            Bootstrap Key: FIREPOWER_MANAGER_IP
            Key Data Type: string
            Mandatory: No
            Is the Key Secret: No
            Description: The IP address of Cisco Firepower Management Center
            Key scope: Global
```

show (app-instance)

To display current application information, use the **show** command in app-instance mode.

show [**app** | **app-attri** | **detail** | **event** | **expand** | **fault** | **fsm** | **heartbeat** | **hotfix** | **resource**]

Syntax Description

app	(Optional) Displays list of application packages, such as ASA or FTD that are available for installation (blade).
app-attri	(Optional) Displays current application attributes.
detail	(Optional) Displays detailed information for the current application instance. This keyword is also available with many of the other command options to display detailed information about the specified option.
event	(Optional) Displays event management information for the application.
expand	(Optional) Displays expanded information for the current application instance. This keyword is also available with many of the other command options to display expanded information about the specified option.
fault	(Optional) Displays information about faults that have occurred in this application instance. The following options are also available: • *fault_ID*—Shows information for the specified fault. • **cause**—Shows information for only the specified cause type. • **detail**—Shows detailed fault information. • **severity**—Shows information for only the specified severity level. • **suppressed**—Lists suppressed faults. The **cause**, **detail** and **severity** keywords are available with this option.
fsm { **status** | **task** }	(Optional) Displays finite state machine information the current application, according to the specified keyword: • **status**—Displays FSM status information. • **task**—Displays FSM task information.
heartbeat	(Optional) Displays information about the last-received heartbeat.
hotfix	(Optional) Displays information about applied hotfixes. The following options are also available with this keyword: **detail**, **expand**, and *version* which you can use to display information for a specific hotfix.
resource	(Optional) Displays information about current resource allocations.

Command Modes

scope ssa/scope slot

Command History

Release	Modification
1.1(1)	Command added.
2.13(0)	The Cluster Role was changed from Master/Slave to Control Node/Data Node.

Usage Guidelines

By default, this command displays general application instance configuration information.

Example

This example shows how to display general application instance information:

```
firepower# scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # scope app-instance asa cluster1
firepower /ssa/slot/app-instance # show

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ -------------- ------------
    asa        cluster1   Enabled     Online           201.2.1.125     201.2.1.125
Native                   In Cluster      Data Node
```

Example

This example shows how to display general application information available for installation:

```
firepower# scope ssa
firepower# show app
firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default App

    ---------- --------------- ---------- ---------------------- ----------- --------------

    asa        9.12.3.12       cisco      Native                 Application No
    asa        9.12.3.140      cisco      Native                 Application No
    asa        9.12.3.9        cisco      Native                 Application No
    asa        9.14.1.150      cisco      Native                 Application No
    asa        9.16.2.3        cisco      Native                 Application Yes
    asa        9.9.2           cisco      Native                 Application No
    ftd        6.4.0.102       cisco      Native,Container       Application No
    ftd        6.5.0.115       cisco      Native,Container       Application No
    ftd        6.6.1.91        cisco      Native,Container       Application No
    ftd        6.6.4.59        cisco      Native,Container       Application Yes
    ftd        6.7.0.65        cisco      Native,Container       Application No
    ftd        7.0.0.94        cisco      Native,Container       Application No
```

Related Commands

Command	Description
scope app-instance	Enters application instance mode for a specific application.
show slot	Shows general configuration information for a specific SSP module.

show audit-logs

To display the user audit logs, use the **show audit-logs** command.

show audit-logs

Command Modes

scope security

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays the user audit logs information.

Example

This example displays the user audit logs information:

```
firepower# scope security
firepower # /security # show audit-logs
Audit trail logs:
    Creation Time        User       ID       Action           Description
    -------------------- ---------- -------- ---------------- -----------
    2021-10-11T21:42:30.885
                         admin      18405523 Creation         PreLoginBanner created
    2021-10-11T21:41:07.340
                         admin      18405498 Deletion         PreLoginBanner deleted
    2021-10-11T21:40:48.222
                         internal   18405486 Deletion         Web A: user admin terminated
 session id web_34771_A
    2021-10-11T21:39:52.703
                         internal   18405463 Creation         Fabric A: remote user test1
logged in from 192.0.2.1
    2021-10-11T21:39:44.351
                        internal   18405450 Deletion        Fabric A: user test1 terminated
 session id pts_1_1_5725
firepower# /security # show audit-logs 18405523 detail
Audit trail logs:
    Creation Time: 2021-10-11T21:42:30.885
    User: admin
    Session ID: pts_0_1_24360
    ID: 18405523
    Action: Creation
    Description: PreLoginBanner created
    Affected Object: sys/user-ext/pre-login-banner
    Trigger: Admin
    Modified Properties: message:TEST
, policyOwner:local
```

show auth-domain

To display current authentication domain information, use the **show auth-domain** command in security mode.

show auth-domain [**detail** | *domain_name*]

Syntax Description

detail	(Optional) Displays detailed information for all current authentication domains.
domain_name	(Optional) Displays information for the specified domain only. The **detail** keyword is available with this option.

Command Modes

scope security/

Command History

Release	Modification
1.4(1)	Command added.

Usage Guidelines

Authentication domains are created using the **create auth-domain** or **enter auth-domain** commands.

Example

This example shows how to display detailed authentication domain information for a specific domain:

```
firepower# scope security
firepower /security # show auth-domain test_domain detail

Authentication domain:
    Authentication domain name: test_domain
    Web session refresh period(in secs): 600
    Idle Session timeout(in secs) for web, ssh, telnet sessions: 600
    Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
    Serial Console Idle Session timeout(in secs): 600
    Serial Console Absolute Session timeout(in secs): 3600
    Default Realm: Local
    Authentication server group:
    Use of 2nd factor: No
firepower /security #
```

Command	Description
create auth-domain	Creates a new authentication domain.
scope auth-domain	Enters auth-domain mode for a specific authentication domain.

show auth-realm fsm status

To display the information of fsm status available on the system, use the **show-auth fsm status** command.

show auth-realm fsm status [**detail**]

Syntax Description		
	detail	(Optional) Displays expanded information for the current application instance. This keyword is also available with many of the other command options to display expanded information about the specified option.

Command Modes scope security

Command History	Release	Modification
	2.3.1	Command added.

Usage Guidelines This is a subcommand of the **show** command in scope security.

Example

This example shows how to display fsm status information

```
Firepower # scope security
Firepower /security # show auth-realm fsm status

FSM 1:
        Status: Nop
        Previous Status: Update Realm Success
        Timestamp: 2012-07-05T23:47:54.643
        Try: 0
        Progress (%): 100
        Current Task:
```

This example shows how to display the fsm status expand details:

```
Firepower # show auth-realm fsm status expand detail

    FSM Status:

        Affected Object: sys/auth-realm/fsm
        Current FSM: update Realm
        Status: Success
        Completion Time: 2012-07-05T23:47:54.643
        Progress (%): 100
        Description:
        Remote Result: Not Applicable
        Error Code: None
        Error Description:

        FSM Stage:

            Order: 1
            Stage Name: updateRealmSetRealmLocal
            Status: Success
            Try: 2
            Last Update Time: 2012-07-05T23:47:54.642
```

```
            Stage Description: realm configuration to primary (FSM-STAGE: Sam: dme:
AaaRealmUpdateRealm: SetRealmLocal)

            Order: 2
            Stage Name: updateRealmSetRealmPeer
            Status: Skip
            Try: 0
            Last Update Time: 2012-07-05T23:47:54.643
            Stage Description: realm configuration to secondary (FSM-STAGE: sam:dm e:
AaaRealmUpdateRealm: SetRealmPeer)
```

show authentication

To display the existing administrative configuration and operational status for the console and default authentication, use the **show authentication** command.

show authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

scope security

Command History

Release	Modification
2.10(1)	Command added.

Usage Guidelines

You can display the existing administrative configuration and operational status for the console and default authentication.

Example

This example shows how to enter security mode and show default authentication method:

```
firepower# scope security
firepower /security # show authentication
Console authentication: Local
Operational Console authentication: Local
Default authentication: Local
Operational Default authentication: Local
Role Policy For Remote Users: Assign Default Role
```

Related Commands

Command	Description
set authentication	Sets the default authentication service.

show breakout

To view information about interface port-breakout configurations, use the **show breakout** command in fabric mode.

show breakout [*slot_id port_id* | **detail** | **expand**]

Syntax Description

slot_id port_id	(Optional) Displays breakout information for a specific port. The **expand** and **expand** keywords are available with this option.
detail	(Optional) Displays detailed information for port breakouts. The **expand** keyword is available with this option.
expand	(Optional) Displays expanded information for port breakouts. The **detail** keyword is available with this option.

Command Modes

scope cabling/scope fabric a/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays breakout information for all ports.

Example

This example shows how to display expanded cabling information:

```
firepower# scope cabling
firepower /cabling # scope fabric a
firepower /cabling/fabric # show breakout

port breakout:
    Slot ID    Port ID    breakout type
    ---------- ---------- -------------
             3          1 10g 4x
             3          2 10g 4x
firepower /cabling/fabric #
```

Related Commands

Command	Description
create breakout	Creates a new interface breakout.

show callhome

To show Call Home configuration and status information, use the **show callhome** command.

show callhome [**detail** | **expand** | **fsm status**]

Syntax Description

detail	(Optional) Displays detailed Call Home information.
expand	(Optional) Displays expanded Call Home information.
fsm status	(Optional) Displays Call Home information and finite state machine status.

Command Modes

Monitoring mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display Call Home information:

```
FP9300-A /monitoring # show callhome

Callhome:
    Admin State: Off
    Throttling State: On
    Contact Information: admin
    Customer Contact Email:
    From Email:
    Reply To Email:
    Phone Contact e.g., +1-011-408-555-1212:
    Street Address:
    Contract Id:
    Customer Id:
    Site Id:
    Switch Priority: Debugging
    Enable/Disable HTTP/HTTPS Proxy: Off
    HTTP/HTTPS Proxy Server Address:
    HTTP/HTTPS Proxy Server Port: 80
    SMTP Server Address:
    SMTP Server Port: 25

DOC-FP9300-A /monitoring #
```

Related Commands

Command	Description
scope callhome	Enters Call Home configuration mode.

show (card)

To view current fabric card information, use the **show** command in card mode.

show [**beacon-led** | **detail** | **event** | **expand** | **fault** | **fsm task** | **port**]

Syntax Description

beacon-led	(Optional) Displays information about the card's beacon LEDs. The following options are also available: • **detail**—Shows detailed LED information. The **expand** keyword is available with this option. • **expand**—Shows expanded LED information. The **detail** keyword is available with this option. • **fsm status**—Shows finite state machine status information. The **expand** keyword is available with this option.
detail	(Optional) Displays detailed information for the fabric card. The **expand** keyword is available with this option.
event [*event_ID* | **detail** | **expand**]	(Optional) Displays event information for the fabric card. You can enter a numeric event ID to view information for only that event. The **detail** and **expand** keywords are also available with this option.
expand	(Optional) Displays expanded information for the fabric card. The **detail** keyword is available with this option.
fault	(Optional) Displays information about faults that have occurred on the fabric card. The following options are also available with this keyword: • *fault_ID*—Shows information for the specified fault. • **cause**—Shows information for only the specified cause type. • **detail**—Shows detailed fault information. • **severity**—Shows information for only the specified severity level. • **suppressed**—Lists suppressed faults. The **cause**, **detail** and **severity** keywords are available with this option.
fsm task	(Optional) Displays FSM task information for the card. The **detail** keyword is available with this option.
port	(Optional) Lists port information for the card.

Command Modes

scope fabric-interconnect/scope card

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays basic card status.

Example

This example shows how to display port information for a specific fabric card:

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # scope card 1
firepower /fabric-interconnect/card # show port

Ether Port:

Slot  Aggr Port  Port  Oper State       Mac                Role    Xcvr
----- ---------- ----- ---------------- ------------------ ------- ----
    1          0     1 Up               B0:AA:77:2F:F0:B0  Network 1000BASE T
    1          0     2 Up               B0:AA:77:2F:F0:B1  Network 1000BASE T
    1          0     3 Up               B0:AA:77:2F:F0:B2  Network 1000BASE T
    1          0     4 Up               B0:AA:77:2F:F0:B3  Network 1000BASE T
    1          0     5 Up               B0:AA:77:2F:F0:B4  Network 1000BASE T
    1          0     6 Up               B0:AA:77:2F:F0:B5  Network 1000BASE T
    1          0     7 Failed           B0:AA:77:2F:F0:B6  Network 1000BASE T
    1          0     8 Sfp Not Present  B0:AA:77:2F:F0:B7  Network N/A

firepower /fabric-interconnect/card #
```

Related Commands

Command	Description
scope card	Enters adminstrative mode for a specific fabric card.

show card detail

To view the card information, use the **show card detail** command.

show card [**detail** | **event** | **expand** | **card-config**]

Syntax Description

detail	Displays detailed information for the fabric card.
expand	(Optional) Displays expanded information for the fabric card
card-config	(Optional) Displays information about the current card configuration

Command Modes

scope fabric-interconnect a

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the command **show** in scope fabric-interconnect a.

Example

This example shows how to display information for a specific fabric card:

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # show card

Fabric Card:
    Id         State
    ---------- -----
             1 Online
             2 Online
             3 Online
```

This example shows how to display detailed information for a specific fabric card:

```
Firepower /fabric-interconnect # show card detail

Fabric Card:
    Id: 1
    Description: Firepower 9300 Supervisor
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-SUP
    HW Revision: 0
    Serial (SN): JSJ18250001
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 2
    Description: Firepower 8x10G SFP+ NM
```

```
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-8X10G
    HW Revision: 0
    Serial (SN): JAD19510ALL
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 3
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD21040C9U
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
```

This example shows how to display expanded information of the current fabric card:

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # show card detail expand

Fabric Card:
    Id: 1
    Description: Firepower 9300 Supervisor
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-SUP
    HW Revision: 0
    Serial (SN): JSJ18250001
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 2
    Description: Firepower 8x10G SFP+ NM
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-8X10G
    HW Revision: 0
    Serial (SN): JAD19510ALL
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 3
```

```
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD21040C9U
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
```

This example shows how to display the information about the current card configuration:

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # show card-config

Card Config:

Slot     Model            OperState    Presence ConfigState
-------- ---------------- ------------ -------- -----------
       1 FPR9K-SUP        Online       Yes      Ok
       2 FPR-NM-8X10G     Online       Yes      Ok
       3 FPR-NM-4X40G     Online       Yes      Ok
```

show cc-mode

To display current Common Criteria mode status information, use the **show cc-mode** command.

show cc-mode

Syntax Description

This command has no arguments or keywords.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Enabling certification compliance on a Firepower 4100/9300 chassis does not automatically propagate compliance to any of its attached logical devices.

Example

This example shows how to enter security mode and display current Common Criteria mode status information:

```
FP9300-A # scope security
FP9300-A /security # show cc-mode
Common Criteria Mode Admin State: Disabled
Common Criteria Mode Operational State: Disabled
FP9300-A /security #
```

Related Commands

Command	Description
disable cc-mode	Disables Common Criteria mode.
enable cc-mode	Enables Common Criteria mode.

show certreq

To display the certificate request for a specific RSA keyring, use the **show certreq** command.

Syntax Description

This command has no arguments or keywords.

Command Modes

Keyring mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to show the certificate request for the current keyring, which you can then copy and send to a trust anchor or certificate authority.

Example

This example shows how to enter an existing keyring and display its certificate request:

```
FP9300-A # scope security
FP9300-A # scope keyring test-ring
FP9300-A /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 198.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name:
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIDEzCCAbsCAQAwEDEOMAwGA1UEAwwFdGVzdDEwggFiMA0GCSqGSIb3DQEBAQUA
A4IBTwAwggFKAoIBQQCDnam/ZTgX8SYXeaYIMeVPeMLvOO7EemP7kEAHPpAqX9d6
3V5NIOLNnCfr7SL8gmLDFORanzZIYb9uxD7/z98xlrS3LdIB3GWCYw+IN1Hz5do/
uClI56thmN5nWgjEWGDwTnu+CD0tFn3qPg8wOpynutE+f43B4fyhWRpU5VO6I3Ma
SRrR4Cp9CKju6U9lttqiNkt5VH3+peM+3AgF6suFF96tN2G+caIlwwf3h6EpFJ1e
NE6CHUIQAdrKPtJVcmMYIYEmEogMYD1O0RXY+ionucK7id4JFAKLVFXPrzHGA3g7
n+xInFC84/2kM1TtapWHrMAOYcTiQ5UR6BJOpLT1V6yXTJrv/FrknJkZJUFKvOBX
9fvZ82UH9o+gWMD8rRBvsz94zGbjBm3SpKh1MLvXjR9af3koaiWMR45BSob0XwID
AQABoD4wEwYJKoZIhvcNAQkHMQYMBHRlc3QwJwYJKoZIhvcNAQkOMRowGDAWBgNV
HREEDzANggV0ZXN0MYcEAQEBATANBgkqhkiG9w0BAQsFAAOCAUEAClVpnjwB8KjD
Okw6k9PaBde07a1eSWwmMd99rR3F9SmnWQMvFXj07m3dEgNRoTCMyxZXH3diDd6/
0e9Ss91/FxORTI3ux+lXhKAOKjOJ5Urz1YLLjomHGrhGNpITQCm71r/fXIjPfUHx
fwaN5lbgImiLI6copKMPY+XMPSFNvIuM4dTAZLHhn5PG0jRAztMNBogw+Fb659BH
vad0QYrz2SHAiH7xETZXp3CTBX4jGhoCad8ffS4YdGQd73/jpu8Zy1nnd1jv7mEj
H9GkSm8sQQfTwQX8RgbzegZGHu3/LxLO6XQDIRj9bTo1aa6zTuhwPyPs4MtdYbpv
mGdEB8QAMHUChdPZdPC44XRPhjPyseig91j+Q1HUmFCMvzNGXksbY1rWj3T4G8gn
z/g7x+OXX/31dLJA2yLx9osUsshmqjs=
-----END CERTIFICATE REQUEST-----
```

```
FP9300-A /security/keyring #
```

Related Commands

Command	Description
create certreq	Creates a new keyring certificate request.
create keyring	Creates a new RSA keyring.
delete certreq	Deletes an existing keyring certificate request.
enter certreq	Enters a keyring certificate request.

show cfg-export-policy

To display the list of configured export policies, use the **show cfg-export-policy** command.

Syntax Description

detail	Displays detailed show configured export policies information.

Command Modes

scope org

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope org.

Example

This example shows how to display the schedule configured export policies information:

```
Firepower /fabric-interconnect # scope org
Firepower /org # show cfg-export-policy
Config Export policy:
    Name                 Description Admin State
    -------------------- ----------- -----------
    default              Configuration Export Policy
                                     Disable
```

Example

This example shows how to display the detailed information of all the available configured export policies

```
Firepower /org # show cfg-export-policy detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Disable
    Protocol: Ftp
    Hostname:
    User:
    Remote File:
    Schedule: Daily
    Port: Default
    Current Task:
```

Example

This example shows how to display detailed information of fsm status of all the available configured export policies:

```
Firepower /org # show cfg-export-policy fsm status
Name: default
```

```
FSM 1:
    Status: Nop
    Previous Status: Nop
    Timestamp: Never
    Try: 0
    Progress (%): 100
    Current Task:
```

show chassis

To display chassis information, use the **show chassis** command.

show chassis [**1**] [**decommissioned** | **detail** | **environment** | **fabric** | **fi-iom** | **firmware** | **fsm status** | **inventory** | **iom** | **psu** | **version**]

Syntax Description

1	(Optional) The chassis ID. There is only one chassis, so entering this ID is optional.
decommissioned	(Optional) Displays information about a decommissioned chassis.
detail	(Optional) Displays detailed information about the chassis.
environment	(Optional) Displays environment information. The keywords **detail**, **expand**, **fan**, **iom**, **psu**, and **server** are also available.
fabric	(Optional) Displays information about the fabric. The keyword **detail** is also available.
fi-iom	(Optional) Displays fabric-interconnect I/O module information. The keyword **detail** is also available.
firmware	(Optional) Displays information about the firmware. The keyword **detail** is also available.
fsm status	(Optional) Displays information about the finite state machine. The keyword **expand** is also available.
inventory	(Optional) Displays vendor and identification information about the chassis. The keywords **detail**, **expand**, **fabric**, **fan**, **fi-iom**, **iom**, **psu**, **server**, and **unspecified** are also available.
iom	(Optional) Displays information about the input/output module. The keyword **detail** is also available.
psu	(Optional) Displays power-supply unit status. The keyword **detail** is also available.
version	(Optional) Displays the version numbers of all the devices in the chassis. The keyword **detail** is also available.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use the **show chassis** command without any arguments or keywords to display basic chassis information.

Example

This example shows how to display basic chassis information:

```
FP9300-A# show chassis 1
Chassis:
Chassis    Overall Status           Admin State
---------- ------------------------ -----------
         1 Accessibility Problem    Acknowledged
FP9300-A#
```

Related Commands

Command	Description
show server environment	Shows server hardware information.

show cli

To display CLI command-related information, use the **show cli** command.

show cli { **command-status** | **history** | **mode-info** | **session-config** | **shell-type** }

Syntax Description

command-status	(Optional) Displays the status of the most-recent command. The optional keyword **detail** provides additional details for the previously entered command.
history	(Optional) Displays a list of commands entered during the current session.
mode-info	(Optional) Displays information about the current CLI mode.
session-config	(Optional) Displays information about the current session configuration.
shell-type	(Optional) Displays information about the current command shell type.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

This command does not require a license.

Example

This example shows how to display information about the current session configuration:

```
FP9300-A# show cli session-config
Suppress Headers: off
Suppress Field Spillover: off
Table Field Delimiter: none
Terminal Width: 61
Terminal Length: 31
Session Absolute Timeout: 3600 seconds
Session Timeout: 600 seconds

FP9300-A#
```

Related Commands

Command	Description
set cli	Specifies whether command output lines will wrap or truncate to fit the width of the terminal window, whether table headers are displayed, and whether commas or spaces will be used to separate fields in command output tables.

show clock

To display the current system date and time, use the **show clock** command.

show clock [**detail**]

Syntax Description

detail	(Optional) Displays detailed information in list form.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display the current system date and time:

```
FP9300-A# show clock
Tue Apr 20 13:24:33 PDT 2010
FP9300-A#
```

Related Commands

Command	Description
set clock	Sets the date and time manually.
show timezone	Shows currently set time zone.

show cloud-connector

To display cloud-connector status and configuration information, use the **show cloud-connector** command.

show cloud-connector [**detail** | **expand** | **fsm**]

Syntax Description

detail	(Optional) Shows additional cloud connector details.
expand	(Optional) Shows expanded cloud connector information.
fsm status	(Optional) Shows current Finite State Machine (FSM) status information.

Command Modes

Any command mode

Command History

Release	Modification
2.2(2)	Command added.

Example

This example shows how to display status information for the cloud connector FSM:

```
FP9300-A# show cloud-connector fsm status

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:
FP9300-A #
```

Related Commands

Command	Description
scope cloud-connector	Enters cloud connector mode.

show configuration

To display system configuration information, use the **show configuration** command.

show configuration [**all** | **no-diff-markers** | **no-pending** | **pending**]

Syntax Description

all	(Optional) Displays all current configuration information.
no-diff-markers	(Optional) Doesn't include diff-markers in the displayed configuration information.
no-pending	(Optional) Doesn't include pending (uncommitted) configuration commands.
pending	(Optional) Shows all pending configuration commands only.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display information about pending (uncommitted) configuration commands:

```
FP9300-A# show configuration pending
 scope services
+    create ntp-server 192.168.200.101
 exit
FP9300-A#
```

Related Commands

Command	Description
show cli	Shows CLI-related status information.

show connection

To show configuration information for the current IPSec connections, or for a single connection, use the **show connection** command.

show connection [**detail** | *name*]

Syntax Description

detail	(Optional) Show detailed IPSec connection information.
name	(Optional) The specific connection name; can be up to 16 alphanumeric characters.

Command Modes

IPSec mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to display current IPSec connection information.

Example

This example shows how to display IPSec connection information:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # show connection

IPSec Connection:
    Name       Admin State Local Address Remote Address ESP Mode  Keyring Name
    ---------- ----------- ------------- -------------- --------- ------------
    TEST       Disabled                                 Transport

FP9300-A /security/ipsec #
```

Related Commands

Command	Description
show ipsec-log	Shows IPSec connection logs.
show stats	Shows IPSec statistics.

show console-auth

To show the console authentication details, use the **show console-auth** command.

show console-auth [**detail**]

Syntax Description

detail	Detailed information of console authentication.

Command Modes

scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope security.

Example

This example shows how to display console authentication information:

```
Firepower # scope security
Firepower /security # show console-auth

Console authentication:
    Admin Realm                 Admin Authentication server group Use of 2nd factor
    --------------------------- --------------------------------- -------------
----
    Local                                                         No
```

show controller fsm status

To display a list of controllers fsm status available on the system, use the **show controller fsm status** command.

show controller fsm status [**expand**]

Syntax Description

expand	(Optional) Displays expanded information for the current application instance. This keyword is also available with many of the other command options to display expanded information about the specified option.

Command Modes

scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system.

Example

This example shows how to display system controller fsm status information:

```
Firepower # scope system
QP1 /system # show controller fsm status


    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:


    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:
Firepower /system # show controller fsm status expand


    FSM Status:
```

```
        Affected Object: sys/chassis-1/blade-1/adaptor-1/mgmt/fsm
        Current FSM: nop
        Status: Nop
        Completion Time:
        Progress (%): 100

        FSM Stage:


    FSM Status:
Affected Object: sys/chassis-1/blade-1/board Controller/mgmt/fsm
        Current FSM: nop
        Status: Nop
        Completion Time:
        Progress (%): 100

        FSM Stage:


    FSM Status:

        Affected Object: sys/chassis-1/blade-1/mgmt/fsm
        Current FSM: ExtMgmtIfConfig
        Status: Success
        Completion Time: 2012-07-27T00:42:51.248
        Progress (%): 100

        FSM Stage:

        Order Stage Name                                  Status       Try
        ------ ---------------------------------------- ------------ ---
        1      ExtMgmtIfConfigPrimary                    Success      1
        2      ExtMgmtIfConfigSecondary                  Skip         0

    FSM Status:

        Affected Object: sys/chassis-1/sw-slot-1/mgmt/fsm
        Current FSM: nop
        Status: Nop
        Completion Time:
        Progress (%): 100
                                                          No
```

show core-export-target

To display the information of core export target available on the system, use the **show core-export-target** command.

show connection [**detail** | **FSM**]

Syntax Description

detail	Lists detailed core export target information.
fsm	Displays finite state machine information of the current application according to the specified keyword: status —Displays FSM status information.

Command Modes

Scope monitoring and scope sysdebug

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope monitoring and scope sysdebug.

Example

This example shows how to display the information of all the system core export target:

```
Firepower # scope monitoring
Firepower /monitoring # scope sysdebug
Firepower /monitoring/sysdebug # show core-export-target

Core Export Target:
    Server Name Port       Path       Admin State
    ----------- ---------- ---------- -----------
                69                    Disabled
Firepower /monitoring/sysdebug # show core-export-target detail

Core Export Target:
Server Name:
    Port: 69
    Path:
    Admin State: Disabled
    Description:
    Current Task:
Firepower /monitoring/sysdebug # show core-export-target fsm status

Server Name:
Port: 69
Path:
Admin State: Disabled

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
```

```
Previous Status: Configure Success
Timestamp: 2012-08-04T12:24:44.253
Try: 0
Progress (%): 100
Current Task:
```

show cores-detail

To display the information of core files available on the system, use the show cores-detail command.

show cores detail

Syntax Description

detail	Lists detailed core information.

Command Modes

Scope monitoring and scope sysdebug

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope monitoring and scope sysdebug.

Example

This example shows how to display the information of all the system core export target:

```
Firepower # scope monitoring
Firepower /monitoring # scope sysdebug
Firepower /monitoring/sysdebug # show cores detail

Core Files:
    Name: 1339202710_SAM_QP1_svc_sam_portAG_log.10885.tar.gz
    Fabric ID: A
    Description: SAM/Fabric Interconnect Core Dump
    Size: 9928624
    Timestamp: 2012-06-09T00:45:23.000
    URI: corefile/1339202710_SAM_QP1_svc_sam_portAG_log.10885.tar.gz
    Current Task:

    Name: 1339202451_SAM_QP1_svc_sam_portAG_log.6740.tar.gz
    Fabric ID: A
    Description: SAM/Fabric Interconnect Core Dump
    Size: 9928180
    Timestamp: 2012-06-09T00:41:14.000
    URI: corefile/1339202451_SAM_QP1_svc_sam_portAG_log.6740.tar.gz
    Current Task:
```

show cpu

To display the details of a CPU, use the **show cpu** command.

show cpu [**detail**]

Syntax Description		
	detail	Shows detailed version information.

Command Modes

scope chassis/scope server

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope server 1 under scope chassis 1.

Example

This example shows how to display CPU information on a specific server:

```
Firepower # KSEC-FPR4115-3# scope chassis 1
Firepower /chassis # scope server 1
Firepower /chassis/server # show cpu
CPU:
    ID  Presence             Architecture      Socket Cores       Speed (GHz)
    --- -------------------- ----------------- ------ ----------- -----------
      1 Equipped             Xeon              CPU1   12          2.100000
       2 Equipped             Xeon              CPU2   12          2.100000
Firepower /chassis/server #
```

Example

This example shows how to display detailed information of CPU on a specific server:

```
Firepower# scope chassis 1
Firepower /chassis # scope server 1
Firepower /chassis/server # show cpu detail

CPU:
    ID: 1
    Presence: Equipped
    Architecture: Xeon
    Socket: CPU1
    Cores: 12
    Cores Enabled: 12
    Speed (GHz): 2.100000
    Stepping: 4
    Vendor: Intel(R) Corporation
    HW Revision: 0
    Thermal Status: OK
    Overall Status: Operable
    Operability: Operable
```

```
    ID: 2
    Presence: Equipped
    Architecture: Xeon
    Socket: CPU2
    Cores: 12
    Cores Enabled: 12
    Speed (GHz): 2.100000
    Stepping: 4
    Vendor: Intel(R) Corporation
    HW Revision: 0
    Thermal Status: OK
    Overall Status: Operable
    Operability: Operable
Firepower /chassis/server #
```

show domain-env-feature

To display the domain environment feature, use the **show domain-env-feature** command.

show domain-env-feature [**detail**]

Syntax Description

detail dns	Displays detailed information on the show domain environment feature.

Command Modes

scope system (scope environment-feature)

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope environment-feature

Example

This example shows how to display domain environment feature information:

```
Firepower /fabric-interconnect # scope system
Firepower /system/ # scope environment-feature
Firepower /system/environment-feature/ show domain-env-feature
Domain Environment Feature:
    Name                                Functional State
    ----------------------------------- ----------------
    DC_POWER_GROUP_FEATURE              Disabled
    ESTIMATE_IMPACT_ON_RECONNECT        Enabled
    HEALTH_REPORTING_FEATURE            Disabled
    POWER_GROUP_FEATURE                 Enabled
    REMOTE_OPERATION_FEATURE            Enabled
    UCS_REGISTRATION_FEATURE            Enabled
```

Example

```
Firepower /system/environment-feature # show domain-env-feature detail
Domain Environment Feature:
    Name: DC_POWER_GROUP_FEATURE
    Feature Type: Major
    Functional State: Disabled

    Name: ESTIMATE_IMPACT_ON_RECONNECT
    Feature Type: Major
    Functional State: Enabled

    Name: HEALTH_REPORTING_FEATURE
    Feature Type: Major
    Functional State: Disabled

    Name: POWER_GROUP_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: REMOTE_OPERATION_FEATURE
```

```
Feature Type: Major
Functional State: Enabled

Name: UCS_REGISTRATION_FEATURE
Feature Type: Major
Functional State: Enabled
```

show domain-nw-feature

To display the information of network features available in the system, use the **show domain-nw-feature** command.

show domain-nw-feature [**detail**]

Syntax Description

detail dns	Displays detailed network feature's information.

Command Modes

scope system, scope network-features

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope network-features.

Example

This example shows how to display the system network feature information:

```
Firepower /fabric-interconnect # scope system
Firepower /system/ # scope environment-feature
Firepower /system/environment-feature/ show domain-nw-feature
Domain Environment Feature:
    Domain Network Feature:
    Name: NETFLOW_FEATURE
    Feature Type: Major
    Functional State: Disabled
```

show domain-server-feature

To display the information of server features available in the system, use the **show domain-server-feature** command.

show domain-server-feature [**detail**]

Syntax Description		
	detail	Displays detailed network feature's information.

Command Modes Scope system, scope server-features

Command History	Release	Modification
	2.3.1	Command added.

Usage Guidelines This is a subcommand of the **show** command in scope system, scope server-features

Example

This example shows information for all system server features:

```
Firepower # scope system
Firepower /system # scope server-features
Firepower /system/server-features # show domain-server-feature detail
Domain Server Feature:
    Name: GLOBAL_SP_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: HEALTH_POLICY_FEATURE
    Feature Type: Major
    Functional State: Disabled

    Name: IN_BAND_MGMT_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: POLICY_MAP_FEATURE
    Feature Type: Major
    Functional State: Enabled
```

show domain-storage-feature

To list of system domain storage feature, use the **show show domain-storage-feature** command.

show domain-storage-feature [**detail** | **Name**]

Syntax Description

detail dns	Displays detailed show domain storage feature information.
Name	Displays information about the specific domain storage. The details keywords are also available with this option.

Command Modes

scope system/scope storage feature

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope storage feature.

Example

This example shows how to display domain storage feature policy information:

```
Firepower /fabric-interconnect # scope system
Firepower /system # scope storage-feature
Firepower /system/storage-feature # show domain-storage-feature
Domain Storage Feature:
    Name                               Functional State
    ---------------------------------- ----------------
    FC_ZONING_FEATURE                  Enabled
    ISCSI_IPV6_FEATURE                 Enabled
```

Example

This example shows how to display detailed information of the available domain storage feature:

```
Firepower /system/storage-feature # show domain-storage-feature detail
Domain Storage Feature:
    Name: FC_ZONING_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: ISCSI_IPV6_FEATURE
    Feature Type: Major
    Functional State: Enabled
  Firepower /system/storage-features # show domain-storage-feature FC_ZONING_FEATURE
Domain Storage Feature:
Name Functional State
---------------------------------- ----------------
FC_ZONING_FEATURE Enabled
```

show dns

To display the DNS name servers in FXOS, use the **show dns** command.

show dns

Syntax Description

show dns	This command is used to display a DNS name server in FXOS.

Command Modes

scope system/scope services

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays the DNS name server.

Example

The following example shows how to display a DNS name server

```
firepower# scope system; scope services
firepower /system /services # show dns
Domain Name Servers:
IP Address: 192.0.2.1
```

show download-task

To view information about firmware-package download operations, use the **show download-task** command in firmware mode.

To view information about logical device software-image download operations, use the **show download-task** command in application software (/ssa/app-software) mode.

show download-task [**detail** | **fsm** | *file_name*]

Syntax Description

detail	(Optional) Use this keyword to display a detailed list of all downloads, or if *file_name* is supplied, detailed download information for the specified file.
fsm status | **fsm task**	(Optional) Use this keyword to list finite state machine (FSM)-related information for all downloads, or if *file_name* is supplied, FSM-related information for the only the specified file. **Note** In firmware mode, this keyword is **fsm status**. In application software (/ssa/app-software) mode, this keyword is **fsm task**.
file_name	(Optional) To view information about a specific file download, provide the name of that file.

Command Modes

scope firmware/

scope ssa/scope app-software

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you do not provide a specific *file_name*, all downloads are listed.

Examples

This example shows how to show detailed firmware-download task information for a specific package:

```
firepower# scope firmware
firepower /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.16.SPA detail

Download task:
    File Name: fxos-k9-fpr9k-firmware.1.0.16.SPA
    Protocol: Scp
    Server: 172.23.32.21
    Port: 0
    Userid: admin2
    Path: /auto/sspdev/bios/MIO_Firmware/release_images/fpr9k/1.0.16
    Downloaded Image Size (KB): 2118
    Time stamp: 2018-05-14T09:30:01.047
    State: Downloaded
    Status: Successful unpack the image
```

```
    Transfer Rate (KB/s): 192.545456
    Current Task:
firepower /firmware #
```

This example shows how to list downloaded software image files:

```
firepower# scope ssa
firepower /ssa # scope app-software
firepower /ssa/app-software # show download-task
Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded
```

Related Commands

Command	Description
download image	Copies a firmware image, or a logical device software image, to the appliance.
install firmware	Installs a firmware package.
show firmware	Shows system firmware information.

show enforce-strong-password

To view the password strength check, use the **show enforce-strong-password** command.

show enforce-strong-password

Syntax Description

Enforce-strong-password	Displays the password strength check(yes/no).

Command Modes

scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope security.

Example

This example shows how to display the password strength check:

```
firepower# scope security
firepower /security # show enforce-strong-password
Password Strength Check: No
```

show environment

To view environmental status information about the chassis, use the **show environment** command in chassis, fxos, or local management mode.

show environment [**detail** | **expand** | **fan** | **iom** | **psu** | **server** | **summary** | **verbose** | **tech**]

Syntax Description

detail	(Optional) Use this keyword to display detailed environment information about the chassis.
expand	(Optional) Use this keyword to display expanded status information for each component on the chassis.
fan	(Optional) Displays extensive status information for each fan in each fan module. The keywords **detail**, **iom**, **psu**, and **server** are also available.
iom	(Optional) Displays information about the input/output module. The keywords **detail**, **fan**, **psu**, and **server** are also available.
psu	(Optional) Displays power-supply unit status. The keywords **detail**, **fan**, **iom**, and **server** are also available.
server	(Optional) Lists extension status information for each hardware component of each server. The keywords **detail**, **fan**, **iom**, and **psu** are also available.
summary	(Optional) Displays a status summary of each hardware component. The keyword **detail** is also available.
verbose | **tech**	(Optional) Use this keyword to display detailed debugging information for each component on the environment.

Command Modes

scope chassis/connect fxos/connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use this command without any arguments or keywords to display basic chassis environment information.

Example

This example shows how to view a summary of the chassis environment:

```
firepower# scope chassis
firepower /chassis # show environment summary

Chassis INFO :
    Total Power Consumption: 726.000000
    Inlet Temperature (C): 35.000000
    CPU Temperature (C): 46.000000
    Last updated Time: 2018-12-18T21:19:22.353

    PSU 1:
        Type: AC
        Input Feed Status: Ok
        12v Output Status: Ok
        Overall Status: Operable
    PSU 2:
        Type: AC
        Input Feed Status: Ok
        12v Output Status: Ok
        Overall Status: N/A

    FAN 1
        Fan Speed RPM (RPM): 4268
        Speed Status: Ok
        Overall Status: Operable
    FAN 2
        Fan Speed RPM (RPM): 4312
        Speed Status: Ok
        Overall Status: Operable
    FAN 3
        Fan Speed RPM (RPM): 4180
        Speed Status: Ok
        Overall Status: Operable
    FAN 4
        Fan Speed RPM (RPM): 4092
        Speed Status: Ok
        Overall Status: Operable

    BLADE 1:
        Total Power Consumption: 258.000000
        Processor Temperature (C): 61.000000
    BLADE 2:
        Total Power Consumption: 270.000000
        Processor Temperature (C): 65.500000

firepower /chassis #
```

Example

This example shows how to view the chassis environment information:

```
firepower# scope chassis
firepower /chassis # show environment expand

Chassis 1:
    Overall Status: Thermal Problem
    Operability: Operable
    Power State: Ok
    Thermal Status: Upper Critical   <<<---!!!

             CPU 1:
                Threshold Status: N/A
```

```
        Overall Status: Operable
        Operability: Operable
        Power State: N/A
        Thermal Status: OK
        Voltage Status: N/A

    CPU 2:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable
        Power State: N/A
        Thermal Status: UC   <<<---!!!
        Voltage Status: N/A
```

Note If the Thermal Status is UC or Upper Critical, then the device performs well without any performance loss. Whereas, if the Thermal Status shows UNR or Upper Non-Recoverable, it indicates that the device performance is getting degraded.

Example

This example shows how to view detailed debugging information:

```
firepower# connect fxos
firepower (fxos) # show environment verbose
***************  Chassis Temps  ***************
AD7416_INLET_TEMP is 34 degrees Celsius
AD7416_OUTLET_TEMP_1 is 31 degrees Celsius

***************  CPU Data  ***************
Core Temperature 0 is 46 degrees Celsius
Core Temperature 1 is 46 degrees Celsius
Core Temperature 2 is 46 degrees Celsius
Core Temperature 3 is 46 degrees Celsius
Core Temperature 4 is 46 degrees Celsius
Core Temperature 5 is 46 degrees Celsius
Core Temperature 6 is 46 degrees Celsius
Core Temperature 7 is 46 degrees Celsius
Core Temperature 8 is 46 degrees Celsius
Core Temperature 9 is 46 degrees Celsius
Core Temperature 10 is 46 degrees Celsius
Core Temperature 11 is 46 degrees Celsius
Core Temperature 12 is 46 degrees Celsius
Core Temperature 13 is 46 degrees Celsius
Core Temperature 14 is 46 degrees Celsius
Core Temperature 15 is 46 degrees Celsius

***************  Power Supplies  ***************
PSU 1 input is okay
PSU 1 output is okay


-- Power Supply 1
  Voltage In         : 0xf9ab Raw Hex
  Current In         : 0xc878 Raw Hex
  Power In           : 0x00c0 Raw Hex
  Temperature 1      : 0x0022 Raw Hex
  Temperature 2      : 0x0026 Raw Hex
```

```
  Temperature 3      : 0x001f Raw Hex
  Fan Speed          : 0x28c4 Raw Hex
  Fan Status         : 0x00 Raw Hex
  Voltage Out        : 0x0078 Raw Hex
  Current Out        : 0x008f Raw Hex
  Power Out          : 0x00ab Raw Hex

No detected PSU in PSU Slot 2


***************  PSEQ Data  ***************
  12V         Voltage Output     :  12.22 Volts
  3.3V        Voltage Output     :   3.37 Volts
  1.2V_FPGA   Voltage Output     :   1.23 Volts
  2.5V_FPGA   Voltage Output     :   2.56 Volts
  0.85V_KC    Voltage Output     :   0.87 Volts
  0.9V_KC     Voltage Output     :   0.93 Volts
  1.8V_KC     Voltage Output     :   1.85 Volts
  1.2V_KC     Voltage Output     :   1.23 Volts
  1.8V_SW     Voltage Output     :   1.84 Volts
  1.0V_SW     Voltage Output     :   1.01 Volts
  SW_CORE     Voltage Output     :   1.01 Volts
  1.8V_NIC    Voltage Output     :   1.84 Volts
  0.9V_CORE_NIC Voltage Output     :   0.93 Volts
  1.0V_NIC    Voltage Output     :   1.03 Volts
  VDD_18_S5   Voltage Output     :   1.84 Volts
  VDDCR_SOC_S5 Voltage Output     :   0.92 Volts
  VDD_18      Voltage Output     :   1.84 Volts
  VDD_33      Voltage Output     :   3.45 Volts
  VPP_CD      Voltage Output     :   2.55 Volts
  VPP_GH      Voltage Output     :   2.55 Volts
  VDDIO_MEM_CD Voltage Output     :   1.23 Volts
  VDDIO_MEM_GH Voltage Output     :   1.23 Volts
  1.2V_MGTAVTT_KC Voltage Output     :   1.23 Volts
  0.9V_NTX_EN Voltage Output     :   0.00 Volts
  1.5V_NTX_EN Voltage Output     :   0.00 Volts
  1.8V_PHY_EN Voltage Output     :   0.00 Volts
  1.0V_PHY_EN Voltage Output     :   0.00 Volts
  VDDCR_SOC_EN Voltage Output     :   0.00 Volts
  VDDCR_CPU_EN Voltage Output     :   0.00 Volts
  VDD_3.3_S5_EN Voltage Output     :   0.00 Volts
  3.3_NIC_EN  Voltage Output     :   0.00 Volts
  5V_EN       Voltage Output     :   0.00 Volts

 PSEQ log

Fault Info Reg (0xb5):
12 9a 00 00 4f a9 33 48 7f ff ff ff ff ff ff ff 7f ff

Fault Rails Warning Reg (0xb6):
20 00 00 00 00 00 00 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff


Rails Value Reg (0xb7) page 0:
07 00 d0 2f 00 00 00

Rails Value Reg (0xb7) page 1:
07 00 45 34 00 00 00

Rails Value Reg (0xb7) page 2:
07 00 54 4c 00 00 00

Rails Value Reg (0xb7) page 3:
```

```
07 00 7d 4f 00 00 00

Rails Value Reg (0xb7) page 4:
07 00 10 36 00 00 00

Rails Value Reg (0xb7) page 5:
07 00 6c 39 00 00 00

Rails Value Reg (0xb7) page 6:
07 00 44 39 00 00 00

Rails Value Reg (0xb7) page 7:
07 00 18 4c 00 00 00

Rails Value Reg (0xb7) page 8:
07 00 22 39 00 00 00

Rails Value Reg (0xb7) page 9:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 10:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 11:
07 00 12 39 00 00 00

Rails Value Reg (0xb7) page 12:
07 00 a0 39 00 00 00

Rails Value Reg (0xb7) page 13:
07 00 b8 3f 00 00 00

Rails Value Reg (0xb7) page 14:
07 00 36 39 00 00 00

Rails Value Reg (0xb7) page 15:
07 00 3c 39 00 00 00

Rails Value Reg (0xb7) page 16:
07 00 22 39 00 00 00

Rails Value Reg (0xb7) page 17:
07 00 74 35 00 00 00

Rails Value Reg (0xb7) page 18:
07 00 3e 4f 00 00 00

Rails Value Reg (0xb7) page 19:
07 00 37 4f 00 00 00

Rails Value Reg (0xb7) page 20:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 21:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 22:
07 00 74 4c 00 00 00

Rails Value Reg (0xb7) page 23:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 24:
07 00 00 00 00 00 00
```

```
Rails Value Reg (0xb7) page 25:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 26:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 27:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 28:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 29:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 30:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 31:
07 00 01 00 00 00 00

Logged Fault Reg (0xea):
25 03 00 00 08 02 82 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00

Fault Details Index Reg (0xeb):
00 64

Fault Details Reg (0xec) index 0:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 1:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 2:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 3:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 4:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 5:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 6:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 7:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 8:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 9:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 10:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 11:
```

```
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 12:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 13:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 14:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 15:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 16:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 17:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 18:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 19:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 20:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 21:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 22:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 23:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 24:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 25:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 26:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 27:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 28:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 29:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 30:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 31:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 32:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 33:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 34:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 35:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 36:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 37:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 38:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 39:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 40:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 41:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 42:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 43:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 44:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 45:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 46:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 47:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 48:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 49:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 50:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 51:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 52:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 53:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 54:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 55:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 56:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 57:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 58:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 59:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 60:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 61:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 62:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 63:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 64:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 65:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 66:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 67:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 68:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 69:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 70:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 71:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 72:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 73:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 74:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 75:
```

```
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 76:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 77:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 78:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 79:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 80:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 81:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 82:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 83:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 84:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 85:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 86:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 87:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 88:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 89:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 90:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 91:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 92:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 93:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 94:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 95:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 96:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 97:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 98:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 99:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Logged Page Peaks Reg (0xed) page 0:
05 00 4b 31 00

Logged Page Peaks Reg (0xed) page 1:
05 00 fa 35 00

Logged Page Peaks Reg (0xed) page 2:
05 00 08 4f 00

Logged Page Peaks Reg (0xed) page 3:
05 00 25 52 00

Logged Page Peaks Reg (0xed) page 4:
05 00 fc 37 00

Logged Page Peaks Reg (0xed) page 5:
05 00 58 3b 00

Logged Page Peaks Reg (0xed) page 6:
05 00 24 3b 00

Logged Page Peaks Reg (0xed) page 7:
05 00 e8 4e 00

Logged Page Peaks Reg (0xed) page 8:
05 00 06 3b 00

Logged Page Peaks Reg (0xed) page 9:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 10:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 11:
05 00 16 3b 00

Logged Page Peaks Reg (0xed) page 12:
05 00 d8 3b 00

Logged Page Peaks Reg (0xed) page 13:
05 00 dc 41 00

Logged Page Peaks Reg (0xed) page 14:
05 00 10 3b 00

Logged Page Peaks Reg (0xed) page 15:
05 00 1c 3b 00

Logged Page Peaks Reg (0xed) page 16:
05 00 2a 3b 00

Logged Page Peaks Reg (0xed) page 17:
05 00 3e 37 00
```

```
Logged Page Peaks Reg (0xed) page 18:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 19:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 20:
05 00 4c 4f 00

Logged Page Peaks Reg (0xed) page 21:
05 00 58 4f 00

Logged Page Peaks Reg (0xed) page 22:
05 00 44 4f 00

Logged Page Peaks Reg (0xed) page 23:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 24:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 25:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 26:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 27:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 28:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 29:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 30:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 31:
05 00 00 00 00

Fault Detail Enable Reg (0xef):
25 ff ff ff f7 fd 07 07 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00


*************** EPM Data ***************
EPM0 is present
EPM0 Card power is okay
EPM0 Card is ready
EPM0 temperature is 32 degrees Celsius

***************  Fans  ***************
FanMod 1 Fan 1 rotating
FanMod 1 Fan 1 RPM = 21720
FanMod 1 Fan 2 rotating
FanMod 1 Fan 2 RPM = 19380
FanMod 1 Fan 3 rotating
FanMod 1 Fan 3 RPM = 21900
FanMod 1 Fan 4 rotating
FanMod 1 Fan 4 RPM = 19320
FanMod 2 Fan 1 rotating
```

```
FanMod 2 Fan 1 RPM = 21720
FanMod 2 Fan 2 rotating
FanMod 2 Fan 2 RPM = 19200
FanMod 2 Fan 3 rotating
FanMod 2 Fan 3 RPM = 21540
FanMod 2 Fan 4 rotating
FanMod 2 Fan 4 RPM = 19440
Fan Controller Speed = automatic
```

Example

This example shows how to view debugging information:

```
firepower# connect fxos
firepower (fxos) # show environment tech
***************  Chassis Temps  ***************
AD7416_INLET_TEMP is 34 degrees Celsius
AD7416_OUTLET_TEMP_1 is 31 degrees Celsius

***************  CPU Data  ***************
Core Temperature 0 is 45 degrees Celsius
Core Temperature 1 is 45 degrees Celsius
Core Temperature 2 is 45 degrees Celsius
Core Temperature 3 is 45 degrees Celsius
Core Temperature 4 is 45 degrees Celsius
Core Temperature 5 is 45 degrees Celsius
Core Temperature 6 is 45 degrees Celsius
Core Temperature 7 is 45 degrees Celsius
Core Temperature 8 is 45 degrees Celsius
Core Temperature 9 is 45 degrees Celsius
Core Temperature 10 is 45 degrees Celsius
Core Temperature 11 is 45 degrees Celsius
Core Temperature 12 is 45 degrees Celsius
Core Temperature 13 is 45 degrees Celsius
Core Temperature 14 is 45 degrees Celsius
Core Temperature 15 is 45 degrees Celsius
Tdie is 45
Tctl is 45
Tccd3 is 45
Tccd5 is 38

***************  Power Supplies  ***************
PSU 1 input is okay
PSU 1 output is okay


-- Power Supply 1
  Voltage In         : 0xf9ab Raw Hex
  Current In         : 0xc878 Raw Hex
  Power In           : 0x00c0 Raw Hex
  Temperature 1      : 0x0022 Raw Hex
  Temperature 2      : 0x0026 Raw Hex
  Temperature 3      : 0x001f Raw Hex
  Fan Speed          : 0x28c5 Raw Hex
  Fan Status         : 0x00 Raw Hex
  Voltage Out        : 0x0078 Raw Hex
  Current Out        : 0x0091 Raw Hex
  Power Out          : 0x00ac Raw Hex

No detected PSU in PSU Slot 2
```

```
***************  PSEQ Data  ***************

Common PSEQ Regs
  CAPABILITY                    : 0xb0 Raw Hex
  STATUS_BYTE                   : 0x03 Raw Hex
  STATUS_WORD                   : 0x1003 Raw Hex
  Communication status          : 0x40 Raw Hex
  MFR_ID                        :  31 37 2d 31 30 32 30 7f ff ff ff ff ff ff ff 80 Raw Hex

  PMBus revision                : 0x12 Raw Hex
  MFR_MODEL                     :  46 50 52 2d 33 31 30 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_REVISION                  :  56 31 2e 35 a3 ff ff 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_LOCATION                  :  43 69 73 63 6f 6e ff 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_DATE                      :  30 35 32 31 32 31 db 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_SERIAL                    :  55 31 36 36 c5 ff ff 7f ff ff ff ff ff ff ff 80 Raw Hex

  Silicon device ID             :  55 43 44 39 30 33 32 7f ff ff ff ff ff ff ff 80 Raw Hex

  Silicon device revision       :  2e 30 2e 30 2e 33 30 7f ff ff ff ff ff ff ff 80 Raw Hex


  12V         Voltage Output    :  12.24 Volts
  Page                          : 0x00 Raw Hex
  OPERATION                     : 0x00 Raw Hex
  On Off Config                 : 0x14 Raw Hex
  VOUT mode                     : 0x16 Raw Hex
  VOUT command                  : 0x3000 Raw Hex
  VOUT margin hi                : 0x3266 Raw Hex
  VOUT margin lo                : 0x2d9a Raw Hex
  VOUT scale                    : 0xa2a8 Raw Hex
  VOUT OV fault limit           : 0x3733 Raw Hex
  VOUT OV warn limit            : 0x34cd Raw Hex
  VOUT UV warn limit            : 0x2b33 Raw Hex
  VOUT UV fault limit           : 0x28cd Raw Hex
  IOUT OC fault limit           : 0x8000 Raw Hex
  IOUT OC warn limit            : 0x8000 Raw Hex
  Power good on                 : 0x2b33 Raw Hex
  Power good off                : 0x28cd Raw Hex
  On delay                      : 0xba00 Raw Hex
  On time limit                 : 0x8000 Raw Hex
  Off delay                     : 0xba00 Raw Hex
  Off time limit                : 0x8000 Raw Hex
  STATUS_VOUT                   : 0x00 Raw Hex
  STATUS_IOUT                   : 0x00 Raw Hex
  Output voltage                : 0x30e5 Raw Hex
  Output current                : 0x8000 Raw Hex

  3.3V        Voltage Output    :   3.37 Volts
  Page                          : 0x01 Raw Hex
  OPERATION                     : 0x00 Raw Hex
  On Off Config                 : 0x14 Raw Hex
  VOUT mode                     : 0x14 Raw Hex
  VOUT command                  : 0x34cd Raw Hex
  VOUT margin hi                : 0x3771 Raw Hex
  VOUT margin lo                : 0x3229 Raw Hex
  VOUT scale                    : 0xb26d Raw Hex
  VOUT OV fault limit           : 0x3cb8 Raw Hex
  VOUT OV warn limit            : 0x3a14 Raw Hex
```

```
VOUT UV warn limit            : 0x2f85 Raw Hex
VOUT UV fault limit           : 0x2ce1 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x2f85 Raw Hex
Power good off                : 0x2ce1 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x35ea Raw Hex
Output current                : 0x8000 Raw Hex

1.2V_FPGA   Voltage Output    :   1.23 Volts
Page                          : 0x02 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x4ccd Raw Hex
VOUT margin hi                : 0x50a4 Raw Hex
VOUT margin lo                : 0x48f6 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x5852 Raw Hex
VOUT OV warn limit            : 0x547b Raw Hex
VOUT UV warn limit            : 0x451f Raw Hex
VOUT UV fault limit           : 0x4148 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x451f Raw Hex
Power good off                : 0x4148 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x4ec0 Raw Hex
Output current                : 0x8000 Raw Hex

2.5V_FPGA   Voltage Output    :   2.56 Volts
Page                          : 0x03 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
VOUT command                  : 0x5000 Raw Hex
VOUT margin hi                : 0x5400 Raw Hex
VOUT margin lo                : 0x4c00 Raw Hex
VOUT scale                    : 0xb333 Raw Hex
VOUT OV fault limit           : 0x5c00 Raw Hex
VOUT OV warn limit            : 0x5800 Raw Hex
VOUT UV warn limit            : 0x4800 Raw Hex
VOUT UV fault limit           : 0x4400 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x4800 Raw Hex
Power good off                : 0x4400 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
```

```
Output voltage                 : 0x5207 Raw Hex
Output current                 : 0x8000 Raw Hex

0.85V_KC    Voltage Output     :   0.87 Volts
Page                           : 0x04 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x3666 Raw Hex
VOUT margin hi                 : 0x3927 Raw Hex
VOUT margin lo                 : 0x33b6 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x3e87 Raw Hex
VOUT OV warn limit             : 0x3bd7 Raw Hex
VOUT UV warn limit             : 0x30f6 Raw Hex
VOUT UV fault limit            : 0x2e35 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x30f6 Raw Hex
Power good off                 : 0x2e35 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x37c8 Raw Hex
Output current                 : 0x8000 Raw Hex

0.9V_KC     Voltage Output     :   0.93 Volts
Page                           : 0x05 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x399a Raw Hex
VOUT margin hi                 : 0x3c7b Raw Hex
VOUT margin lo                 : 0x36b8 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x423d Raw Hex
VOUT OV warn limit             : 0x3f5c Raw Hex
VOUT UV warn limit             : 0x33d7 Raw Hex
VOUT UV fault limit            : 0x30f6 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x33d7 Raw Hex
Power good off                 : 0x30f6 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x3b38 Raw Hex
Output current                 : 0x8000 Raw Hex

1.8V_KC     Voltage Output     :   1.85 Volts
Page                           : 0x06 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x13 Raw Hex
VOUT command                   : 0x399a Raw Hex
VOUT margin hi                 : 0x3c7b Raw Hex
VOUT margin lo                 : 0x36b8 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
```

```
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3b1a Raw Hex
Output current                : 0x8000 Raw Hex

1.2V_KC     Voltage Output    :   1.23 Volts
Page                          : 0x07 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x4ccd Raw Hex
VOUT margin hi                : 0x50a4 Raw Hex
VOUT margin lo                : 0x48f6 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x5852 Raw Hex
VOUT OV warn limit            : 0x547b Raw Hex
VOUT UV warn limit            : 0x451f Raw Hex
VOUT UV fault limit           : 0x4148 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x451f Raw Hex
Power good off                : 0x4148 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x4e84 Raw Hex
Output current                : 0x8000 Raw Hex

1.8V_SW     Voltage Output    :   1.84 Volts
Page                          : 0x08 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xeb20 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
```

```
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x3af2 Raw Hex
Output current                 : 0x8000 Raw Hex

1.0V_SW     Voltage Output     :   1.01 Volts
Page                           : 0x09 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x4000 Raw Hex
VOUT margin hi                 : 0x4333 Raw Hex
VOUT margin lo                 : 0x3ccd Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x499a Raw Hex
VOUT OV warn limit             : 0x4666 Raw Hex
VOUT UV warn limit             : 0x399a Raw Hex
VOUT UV fault limit            : 0x3666 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x399a Raw Hex
Power good off                 : 0x3666 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x409c Raw Hex
Output current                 : 0x8000 Raw Hex

SW_CORE     Voltage Output     :   1.01 Volts
Page                           : 0x0a Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x4000 Raw Hex
VOUT margin hi                 : 0x4333 Raw Hex
VOUT margin lo                 : 0x3ccd Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x499a Raw Hex
VOUT OV warn limit             : 0x4666 Raw Hex
VOUT UV warn limit             : 0x399a Raw Hex
VOUT UV fault limit            : 0x3666 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x399a Raw Hex
Power good off                 : 0x3666 Raw Hex
On delay                       : 0xca80 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x4094 Raw Hex
Output current                 : 0x8000 Raw Hex

1.8V_NIC    Voltage Output     :   1.84 Volts
Page                           : 0x0b Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x13 Raw Hex
VOUT command                   : 0x399a Raw Hex
VOUT margin hi                 : 0x3c7b Raw Hex
```

```
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3ae8 Raw Hex
Output current                : 0x8000 Raw Hex

0.9V_CORE_NIC Voltage Output     :   0.93 Volts
Page                          : 0x0c Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3bc4 Raw Hex
Output current                : 0x8000 Raw Hex

1.0V_NIC    Voltage Output    :   1.03 Volts
Page                          : 0x0d Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x4000 Raw Hex
VOUT margin hi                : 0x4333 Raw Hex
VOUT margin lo                : 0x3ccd Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x499a Raw Hex
VOUT OV warn limit            : 0x4666 Raw Hex
VOUT UV warn limit            : 0x399a Raw Hex
VOUT UV fault limit           : 0x3666 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x399a Raw Hex
Power good off                : 0x3666 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
```

```
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x41a0 Raw Hex
Output current                  : 0x8000 Raw Hex

VDD_18_S5   Voltage Output      :   1.84 Volts
Page                            : 0x0e Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x13 Raw Hex
VOUT command                    : 0x399a Raw Hex
VOUT margin hi                  : 0x3c7b Raw Hex
VOUT margin lo                  : 0x36b8 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x423d Raw Hex
VOUT OV warn limit              : 0x3f5c Raw Hex
VOUT UV warn limit              : 0x33d7 Raw Hex
VOUT UV fault limit             : 0x30f6 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x33d7 Raw Hex
Power good off                  : 0x30f6 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x3b02 Raw Hex
Output current                  : 0x8000 Raw Hex

VDDCR_SOC_S5 Voltage Output     :   0.92 Volts
Page                            : 0x0f Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x12 Raw Hex
VOUT command                    : 0x399a Raw Hex
VOUT margin hi                  : 0x3c7b Raw Hex
VOUT margin lo                  : 0x36b8 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x423d Raw Hex
VOUT OV warn limit              : 0x3f5c Raw Hex
VOUT UV warn limit              : 0x33d7 Raw Hex
VOUT UV fault limit             : 0x30f6 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x33d7 Raw Hex
Power good off                  : 0x30f6 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x3b08 Raw Hex
Output current                  : 0x8000 Raw Hex

VDD_18      Voltage Output      :   1.84 Volts
Page                            : 0x10 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x13 Raw Hex
```

```
VOUT command                    : 0x399a Raw Hex
VOUT margin hi                  : 0x3c7b Raw Hex
VOUT margin lo                  : 0x36b8 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x423d Raw Hex
VOUT OV warn limit              : 0x3f5c Raw Hex
VOUT UV warn limit              : 0x33d7 Raw Hex
VOUT UV fault limit             : 0x30f6 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x33d7 Raw Hex
Power good off                  : 0x30f6 Raw Hex
On delay                        : 0xb39a Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x3aee Raw Hex
Output current                  : 0x8000 Raw Hex

VDD_33      Voltage Output      :   3.45 Volts
Page                            : 0x11 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x14 Raw Hex
VOUT command                    : 0x34cd Raw Hex
VOUT margin hi                  : 0x3771 Raw Hex
VOUT margin lo                  : 0x3229 Raw Hex
VOUT scale                      : 0xb266 Raw Hex
VOUT OV fault limit             : 0x3cb8 Raw Hex
VOUT OV warn limit              : 0x3a14 Raw Hex
VOUT UV warn limit              : 0x2f85 Raw Hex
VOUT UV fault limit             : 0x2ce1 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x2f85 Raw Hex
Power good off                  : 0x2ce1 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x372a Raw Hex
Output current                  : 0x8000 Raw Hex

VPP_CD      Voltage Output      :   2.55 Volts
Page                            : 0x12 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x13 Raw Hex
VOUT command                    : 0x5000 Raw Hex
VOUT margin hi                  : 0x5400 Raw Hex
VOUT margin lo                  : 0x4c00 Raw Hex
VOUT scale                      : 0xb333 Raw Hex
VOUT OV fault limit             : 0x5c00 Raw Hex
VOUT OV warn limit              : 0x5800 Raw Hex
VOUT UV warn limit              : 0x4800 Raw Hex
VOUT UV fault limit             : 0x4400 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x4800 Raw Hex
Power good off                  : 0x4400 Raw Hex
```

```
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x51c1 Raw Hex
Output current                  : 0x8000 Raw Hex

VPP_GH      Voltage Output      :   2.55 Volts
Page                            : 0x13 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x13 Raw Hex
VOUT command                    : 0x5000 Raw Hex
VOUT margin hi                  : 0x5400 Raw Hex
VOUT margin lo                  : 0x4c00 Raw Hex
VOUT scale                      : 0xb333 Raw Hex
VOUT OV fault limit             : 0x5c00 Raw Hex
VOUT OV warn limit              : 0x5800 Raw Hex
VOUT UV warn limit              : 0x4800 Raw Hex
VOUT UV fault limit             : 0x4400 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x4800 Raw Hex
Power good off                  : 0x4400 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x51bc Raw Hex
Output current                  : 0x8000 Raw Hex

VDDIO_MEM_CD Voltage Output     :   1.23 Volts
Page                            : 0x14 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x12 Raw Hex
VOUT command                    : 0x4ccd Raw Hex
VOUT margin hi                  : 0x50a4 Raw Hex
VOUT margin lo                  : 0x48f6 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x5852 Raw Hex
VOUT OV warn limit              : 0x547b Raw Hex
VOUT UV warn limit              : 0x451f Raw Hex
VOUT UV fault limit             : 0x4148 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x451f Raw Hex
Power good off                  : 0x4148 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x4ef4 Raw Hex
Output current                  : 0x8000 Raw Hex

VDDIO_MEM_GH Voltage Output     :   1.23 Volts
Page                            : 0x15 Raw Hex
OPERATION                       : 0x00 Raw Hex
```

```
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x12 Raw Hex
VOUT command                    : 0x4ccd Raw Hex
VOUT margin hi                  : 0x50a4 Raw Hex
VOUT margin lo                  : 0x48f6 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x5852 Raw Hex
VOUT OV warn limit              : 0x547b Raw Hex
VOUT UV warn limit              : 0x451f Raw Hex
VOUT UV fault limit             : 0x4148 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x451f Raw Hex
Power good off                  : 0x4148 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x4ef4 Raw Hex
Output current                  : 0x8000 Raw Hex

1.2V_MGTAVTT_KC Voltage Output     :   1.23 Volts
Page                            : 0x16 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x12 Raw Hex
VOUT command                    : 0x4ccd Raw Hex
VOUT margin hi                  : 0x50a4 Raw Hex
VOUT margin lo                  : 0x48f6 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x5852 Raw Hex
VOUT OV warn limit              : 0x547b Raw Hex
VOUT UV warn limit              : 0x451f Raw Hex
VOUT UV fault limit             : 0x4148 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x451f Raw Hex
Power good off                  : 0x4148 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x4ee0 Raw Hex
Output current                  : 0x8000 Raw Hex

0.9V_NTX_EN Voltage Output      :   0.00 Volts
Page                            : 0x17 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x14 Raw Hex
VOUT command                    : 0x0000 Raw Hex
VOUT margin hi                  : 0x0000 Raw Hex
VOUT margin lo                  : 0x0000 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x0000 Raw Hex
VOUT OV warn limit              : 0x0000 Raw Hex
VOUT UV warn limit              : 0x0000 Raw Hex
VOUT UV fault limit             : 0x0000 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
```

```
Power good on                  : 0x0000 Raw Hex
Power good off                 : 0x0000 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x0000 Raw Hex
Output current                 : 0x8000 Raw Hex

1.5V_NTX_EN Voltage Output     :   0.00 Volts
Page                           : 0x18 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x14 Raw Hex
VOUT command                   : 0x0000 Raw Hex
VOUT margin hi                 : 0x0000 Raw Hex
VOUT margin lo                 : 0x0000 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x0000 Raw Hex
VOUT OV warn limit             : 0x0000 Raw Hex
VOUT UV warn limit             : 0x0000 Raw Hex
VOUT UV fault limit            : 0x0000 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x0000 Raw Hex
Power good off                 : 0x0000 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x0000 Raw Hex
Output current                 : 0x8000 Raw Hex

1.8V_PHY_EN Voltage Output     :   0.00 Volts
Page                           : 0x19 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x14 Raw Hex
VOUT command                   : 0x0000 Raw Hex
VOUT margin hi                 : 0x0000 Raw Hex
VOUT margin lo                 : 0x0000 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x0000 Raw Hex
VOUT OV warn limit             : 0x0000 Raw Hex
VOUT UV warn limit             : 0x0000 Raw Hex
VOUT UV fault limit            : 0x0000 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x0000 Raw Hex
Power good off                 : 0x0000 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x0000 Raw Hex
Output current                 : 0x8000 Raw Hex

1.0V_PHY_EN Voltage Output     :   0.00 Volts
```

```
Page                           : 0x1a Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x14 Raw Hex
VOUT command                   : 0x0000 Raw Hex
VOUT margin hi                 : 0x0000 Raw Hex
VOUT margin lo                 : 0x0000 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x0000 Raw Hex
VOUT OV warn limit             : 0x0000 Raw Hex
VOUT UV warn limit             : 0x0000 Raw Hex
VOUT UV fault limit            : 0x0000 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x0000 Raw Hex
Power good off                 : 0x0000 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x0000 Raw Hex
Output current                 : 0x8000 Raw Hex

VDDCR_SOC_EN Voltage Output     :   0.00 Volts
Page                           : 0x1b Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x14 Raw Hex
VOUT command                   : 0x0000 Raw Hex
VOUT margin hi                 : 0x0000 Raw Hex
VOUT margin lo                 : 0x0000 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x0000 Raw Hex
VOUT OV warn limit             : 0x0000 Raw Hex
VOUT UV warn limit             : 0x0000 Raw Hex
VOUT UV fault limit            : 0x0000 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x0000 Raw Hex
Power good off                 : 0x0000 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x0000 Raw Hex
Output current                 : 0x8000 Raw Hex

VDDCR_CPU_EN Voltage Output     :   0.00 Volts
Page                           : 0x1c Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x14 Raw Hex
VOUT command                   : 0x0000 Raw Hex
VOUT margin hi                 : 0x0000 Raw Hex
VOUT margin lo                 : 0x0000 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x0000 Raw Hex
VOUT OV warn limit             : 0x0000 Raw Hex
VOUT UV warn limit             : 0x0000 Raw Hex
VOUT UV fault limit            : 0x0000 Raw Hex
```

```
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

VDD_3.3_S5_EN Voltage Output     :   0.00 Volts
Page                          : 0x1d Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x14 Raw Hex
VOUT command                  : 0x0000 Raw Hex
VOUT margin hi                : 0x0000 Raw Hex
VOUT margin lo                : 0x0000 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x0000 Raw Hex
VOUT OV warn limit            : 0x0000 Raw Hex
VOUT UV warn limit            : 0x0000 Raw Hex
VOUT UV fault limit           : 0x0000 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

3.3_NIC_EN  Voltage Output     :   0.00 Volts
Page                          : 0x1e Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x14 Raw Hex
VOUT command                  : 0x0000 Raw Hex
VOUT margin hi                : 0x0000 Raw Hex
VOUT margin lo                : 0x0000 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x0000 Raw Hex
VOUT OV warn limit            : 0x0000 Raw Hex
VOUT UV warn limit            : 0x0000 Raw Hex
VOUT UV fault limit           : 0x0000 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex
```

```
  5V_EN       Voltage Output     :   0.00 Volts
  Page                           : 0x1f Raw Hex
  OPERATION                      : 0x00 Raw Hex
  On Off Config                  : 0x14 Raw Hex
  VOUT mode                      : 0x14 Raw Hex
  VOUT command                   : 0x0000 Raw Hex
  VOUT margin hi                 : 0x0000 Raw Hex
  VOUT margin lo                 : 0x0000 Raw Hex
  VOUT scale                     : 0xba00 Raw Hex
  VOUT OV fault limit            : 0x0000 Raw Hex
  VOUT OV warn limit             : 0x0000 Raw Hex
  VOUT UV warn limit             : 0x0000 Raw Hex
  VOUT UV fault limit            : 0x0000 Raw Hex
  IOUT OC fault limit            : 0x8000 Raw Hex
  IOUT OC warn limit             : 0x8000 Raw Hex
  Power good on                  : 0x0000 Raw Hex
  Power good off                 : 0x0000 Raw Hex
  On delay                       : 0xba00 Raw Hex
  On time limit                  : 0xda80 Raw Hex
  Off delay                      : 0xba00 Raw Hex
  Off time limit                 : 0x8000 Raw Hex
  STATUS_VOUT                    : 0x00 Raw Hex
  STATUS_IOUT                    : 0x00 Raw Hex
  Output voltage                 : 0x0001 Raw Hex
  Output current                 : 0x8000 Raw Hex


 PSEQ log

Fault Info Reg (0xb5):
12 9a 00 00 4f a9 33 48 7f ff ff ff ff ff ff ff 7f ff

Fault Rails Warning Reg (0xb6):
20 00 00 00 00 00 00 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff


Rails Value Reg (0xb7) page 0:
07 00 d0 2f 00 00 00

Rails Value Reg (0xb7) page 1:
07 00 45 34 00 00 00

Rails Value Reg (0xb7) page 2:
07 00 54 4c 00 00 00

Rails Value Reg (0xb7) page 3:
07 00 7d 4f 00 00 00

Rails Value Reg (0xb7) page 4:
07 00 10 36 00 00 00

Rails Value Reg (0xb7) page 5:
07 00 6c 39 00 00 00

Rails Value Reg (0xb7) page 6:
07 00 44 39 00 00 00

Rails Value Reg (0xb7) page 7:
07 00 18 4c 00 00 00

Rails Value Reg (0xb7) page 8:
07 00 22 39 00 00 00
```

```
Rails Value Reg (0xb7) page 9:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 10:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 11:
07 00 12 39 00 00 00

Rails Value Reg (0xb7) page 12:
07 00 a0 39 00 00 00

Rails Value Reg (0xb7) page 13:
07 00 b8 3f 00 00 00

Rails Value Reg (0xb7) page 14:
07 00 36 39 00 00 00

Rails Value Reg (0xb7) page 15:
07 00 3c 39 00 00 00

Rails Value Reg (0xb7) page 16:
07 00 22 39 00 00 00

Rails Value Reg (0xb7) page 17:
07 00 74 35 00 00 00

Rails Value Reg (0xb7) page 18:
07 00 3e 4f 00 00 00

Rails Value Reg (0xb7) page 19:
07 00 37 4f 00 00 00

Rails Value Reg (0xb7) page 20:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 21:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 22:
07 00 74 4c 00 00 00

Rails Value Reg (0xb7) page 23:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 24:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 25:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 26:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 27:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 28:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 29:
07 00 00 00 00 00 00
```

```
Rails Value Reg (0xb7) page 30:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 31:
07 00 01 00 00 00 00

Logged Fault Reg (0xea):
25 03 00 00 08 02 82 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00

Fault Details Index Reg (0xeb):
00 64

Fault Details Reg (0xec) index 0:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 1:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 2:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 3:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 4:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 5:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 6:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 7:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 8:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 9:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 10:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 11:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 12:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 13:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 14:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 15:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 16:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 17:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 18:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 19:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 20:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 21:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 22:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 23:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 24:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 25:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 26:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 27:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 28:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 29:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 30:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 31:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 32:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 33:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 34:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 35:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 36:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 37:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 38:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 39:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 40:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 41:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 42:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 43:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 44:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 45:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 46:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 47:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 48:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 49:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 50:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 51:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 52:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 53:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 54:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 55:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 56:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 57:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 58:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 59:
```

```
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 60:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 61:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 62:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 63:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 64:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 65:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 66:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 67:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 68:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 69:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 70:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 71:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 72:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 73:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 74:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 75:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 76:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 77:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 78:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 79:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 80:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 81:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 82:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 83:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 84:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 85:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 86:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 87:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 88:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 89:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 90:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 91:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 92:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 93:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 94:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 95:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 96:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 97:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 98:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 99:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Logged Page Peaks Reg (0xed) page 0:
05 00 4b 31 00

Logged Page Peaks Reg (0xed) page 1:
05 00 fa 35 00
```

```
Logged Page Peaks Reg (0xed) page 2:
05 00 08 4f 00

Logged Page Peaks Reg (0xed) page 3:
05 00 25 52 00

Logged Page Peaks Reg (0xed) page 4:
05 00 fc 37 00

Logged Page Peaks Reg (0xed) page 5:
05 00 58 3b 00

Logged Page Peaks Reg (0xed) page 6:
05 00 24 3b 00

Logged Page Peaks Reg (0xed) page 7:
05 00 e8 4e 00

Logged Page Peaks Reg (0xed) page 8:
05 00 06 3b 00

Logged Page Peaks Reg (0xed) page 9:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 10:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 11:
05 00 16 3b 00

Logged Page Peaks Reg (0xed) page 12:
05 00 d8 3b 00

Logged Page Peaks Reg (0xed) page 13:
05 00 dc 41 00

Logged Page Peaks Reg (0xed) page 14:
05 00 10 3b 00

Logged Page Peaks Reg (0xed) page 15:
05 00 1c 3b 00

Logged Page Peaks Reg (0xed) page 16:
05 00 2a 3b 00

Logged Page Peaks Reg (0xed) page 17:
05 00 3e 37 00

Logged Page Peaks Reg (0xed) page 18:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 19:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 20:
05 00 4c 4f 00

Logged Page Peaks Reg (0xed) page 21:
05 00 58 4f 00

Logged Page Peaks Reg (0xed) page 22:
05 00 44 4f 00

Logged Page Peaks Reg (0xed) page 23:
```

```
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 24:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 25:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 26:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 27:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 28:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 29:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 30:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 31:
05 00 00 00 00

Fault Detail Enable Reg (0xef):
25 ff ff ff f7 fd 07 07 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00


*************** EPM Data ***************
EPM0 is present
EPM0 Card power is okay
EPM0 Card is ready
EPM0 temperature is 32 degrees Celsius

***************  Fans  ***************
FanMod 1 Fan 1 rotating
FanMod 1 Fan 1 RPM = 21720
FanMod 1 Fan 2 rotating
FanMod 1 Fan 2 RPM = 19380
FanMod 1 Fan 3 rotating
FanMod 1 Fan 3 RPM = 21900
FanMod 1 Fan 4 rotating
FanMod 1 Fan 4 RPM = 19320
FanMod 2 Fan 1 rotating
FanMod 2 Fan 1 RPM = 21720
FanMod 2 Fan 2 rotating
FanMod 2 Fan 2 RPM = 19260
FanMod 2 Fan 3 rotating
FanMod 2 Fan 3 RPM = 21540
FanMod 2 Fan 4 rotating
FanMod 2 Fan 4 RPM = 19440

Environmental Fan FPGA Control   : 0x00000107
Environmental Fan Status         : 0x00000003
Environmental Fan Enable Control : 0x00110700
Fanmod1 PWM Slope                : 0x00000108
Fanmod1 Speed                    : 0x000003e8
Fanmod1 Smartfan Control         : 0x00000000
Fanmod1 Smartfan Status          : 0x00540000
Fanmod1 Smartfan PWM             : 0x000000f0
```

```
Fanmod1 Smartfan Debug           : 0x00003aee
Fanmod2 PWM Slope                : 0x00000108
Fanmod2 Speed                    : 0x000003e8
Fanmod2 Smartfan Control         : 0x00000000
Fanmod2 Smartfan Status          : 0x00540000
Fanmod2 Smartfan PWM             : 0x000000f0
Fanmod2 Smartfan Debug           : 0x00003b14
T2/T1 Temp                       : 0x0088007c
T4/T3 Temp                       : 0x0098008c
T6/T5 Temp                       : 0x00a8009c
T8/T7 Temp                       : 0x00b800ac
Level 1 Speed                    : 0x000004b0
Level 2 Speed                    : 0x00000550
Level 3 Speed                    : 0x000005b4
Level 4 Speed                    : 0x00000640
Level 5 Speed                    : 0x000007d0
Minimal Speed Threshold          : 0x00000054
Fan Controller Speed = automatic

***************  Disks  ***************

***************  SSD Data  ***************
```

Related Commands

Command	Description
show server environment	Shows server hardware information.

show eth-uplink

To display Ethernet uplink information, use the **show eth-uplink** command.

show eth-uplink [**detail** | **expand** | **fsm**]

Syntax Description

detail	(Optional) Displays details about the Ethernet uplink.
expand	(Optional) Displays expanded information about the Ethernet uplink.
fsm status	(Optional) Displays the finite state machine status.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Unidirectional link detection (UDLD) is not supported by FXOS; ignore any references to UDLD.

Example

This example shows how to display expanded Ethernet uplink information:

```
firepower# show eth-uplink expand

Ethernet Uplink:
    Mode          MAC Table Aging Time (dd:hh:mm:ss) VLAN Port Count Optimization
    ------------ ---------------------------------- ----------------------------
    Security Node 00:04:01:40                        Disabled
firepower# show eth-uplink expand

Ethernet Uplink:
    Mode: Security Node
    MAC Table Aging Time (dd:hh:mm:ss): 00:04:01:40
    VLAN Port Count Optimization: Disabled

    Ethernet Link Profile:
        Name       UDLD link policy name Oper UDLD link policy name
        ---------- --------------------- --------------------------
        default    default               fabric/lan/udld-link-pol-default

    Fabric:
        Fabric ID: A

        Interface:
            Port Name: Ethernet1/1
            Port Type: Mgmt
            Admin State: Enabled
            Oper State: Link Down
            State Reason: Link failure or not-connected

    <--- intevening lines removed for brevity --->

            Port Name: Ethernet2/6
```

```
            Port Type: Data
            Admin State: Disabled
            Oper State: Admin Down
            State Reason: Administratively down

            Port Name: Ethernet2/7
            Port Type: Data
            Admin State: Disabled
            Oper State: Sfp Not Present
            State Reason: Unknown

            Port Name: Ethernet2/8
            Port Type: Data
            Admin State: Disabled
            Oper State: Sfp Not Present
            State Reason: Unknown

        Port Channel:
            Port Channel Id: 48
            Name: Port-channel48
            Port Type: Cluster
            Admin State: Enabled
            Oper State: Failed
            State Reason: No operational members

            Member Port:
                Port Name       Membership         Oper State       State Reason
                --------------- ------------------ ---------------- ------------
                Ethernet1/5     Down               Link Down        Link failure or
not-connected
                Ethernet1/6     Down               Link Down        Link failure or
not-connected

    Stats Threshold Policy:
        Name: default
        Full Name: fabric/lan/thr-policy-default
        Policy Owner: Local

    UDLD link policy:
        Name       Admin State UDLD mode
        ---------- ----------- ---------
        default    Disabled    Normal
firepower#
```

Related Commands

Command	Description
scope eth-uplink	Enters Ethernet uplink mode.

show event

To display FSM event information, use the **show event** command.

show event [*event_id* | **detail**]

Syntax Description

event_id	(Optional) Displays information for a specific event.
detail	(Optional) Displays detailed information for all events.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use the **show event** command without any arguments or keywords to display a list of events.

Example

This example shows how to display a list of events:

```
FP9300-A# show event
Creation Time              ID       Code     Description
-------------------------- -------- -------- -----------
2025-12-23T04:17:00.678    176144 E4195253 [FSM:STAGE:SKIP]: keyring configuration on
secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingPeer)
2025-12-23T04:17:00.678    176145 E4195253 [FSM:STAGE:END]: keyring configuration on
secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingPeer)
2025-12-23T04:17:00.678    176146 E4197130 [FSM:STAGE:SKIP]: post processing after keyring
 configration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingLocal)
2025-12-23T04:17:00.678    176147 E4197130 [FSM:STAGE:END]: post processing after keyring
configration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingLocal)
2025-12-23T04:17:00.678    176148 E4197131 [FSM:STAGE:SKIP]: post processing after keyring
 configuration on secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingPeer)
2025-12-23T04:17:00.678    176149 E4197131 [FSM:STAGE:END]: post processing after keyring
configuration on secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingPeer)
2025-12-23T04:17:00.678    176150 E4195525 [FSM:END]: keyring
configuration(FSM:sam:dme:PkiEpUpdateEp)
2025-12-23T04:17:00.677    176142 E4195252 [FSM:STAGE:STALE-SUCCESS]: keyring configuration
 on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal)

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
show sel	Shows the contents of the system event log (SEL) of a server.

show fabric

To view fabric cabling information, use the **show fabric** command in cabling mode.

show fabric [**breakout** | **detail** | **expand**]

Syntax Description

a	(Optional) Displays cabling information specific to Fabric A. **Note** There is no Fabric B.
detail	(Optional) Displays detailed cabling information. The **expand** keyword is available with this option.
expand	(Optional) Displays expanded cabling information including port breakouts. The **detail** keyword is available with this option.

Command Modes

scope cabling/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays general fabric cabling information.

Example

This example shows how to display expanded cabling information:

```
firepower# scope cabling
firepower /cabling # show fabric expand

cabling on switch:
    Id: A

    port breakout:
        Slot ID    Port ID    breakout type
        ---------- ---------- -------------
                 3          1 10g 4x
                 3          2 10g 4x
firepower /cabling #
```

Related Commands

Command	Description
create breakout	Creates a new interface breakout.

show fabric-interconnect

To display fabric interconnect information, use the **show fabric-interconnect** command.

show fabric-interconnect [**a** | **b** | **detail** | **environment** | **firmware** | **fsm** | **inventory** | **mac-aging** | **mode** | **version**]

Syntax Description

a	(Optional) Displays fabric interconnect information for Fabric A. Use the optional **detail** keyword to show detailed information for the fabric. **Note** There is only one fabric; it is labeled A. Thus, there is no need to enter this keyword.
b	(Optional) Do not use: there is no Fabric B.
detail	(Optional) Displays detailed fabric interconnect information.
environment	(Optional) Displays information about installed fabric cards. These optional keywords are available: • **a** —Displays information for only Fabric A. This keyword is optional—there is only one fabric. • **b** —Do not use: there is no Fabric B. • **detail** —Displays detailed environment information. • **expand** —Displays expanded environment information. The **detail** keyword is available with this option. • **fan** —Displays fan-specific information. The keywords **detail** and **psu**available with this option. • **psu** —Displays power-supply-unit-specific information. The keywords **detail** and **fan**available with this option.
firmware	(Optional) Displays firmware information.
fsm status	(Optional) Displays finite state machine status information.
inventory	(Optional) Displays basic hardware information about the fabric. The keywords **detail**, **expand** and **id**available with this option.
mac-aging	(Optional) Displays MAC table aging time.
mode	(Optional) Displays fabric interconnect mode information.
version	(Optional) Displays firmware version information.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

This command does not require a license.

Example

This example shows how to display base fabric interconnect information:

```
FP9300-A# show fabric-interconnect

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    10.201.153.14   10.201.153.1    255.255.255.0   ::               ::
 64     Operable
FP9300-A#
```

Related Commands

Command	Description
scope fabric-interconnect	Enters fabric interconnect mode.

show fan-module

To view information about installed fan modules, use the **show fan-module** command in chassis mode.

show fan-module [[**1** *module_id*] | **detail** | **expand**]

Syntax Description

tray_id module_id	(Optional) To display information for a specific module, use *tray_id module_id* to identify the module. The *tray_id* is always 1; the *module_id* can be 1 through 8.
detail	(Optional) Use this keyword to display detailed status information about each fan module.
expand	(Optional) Use this keyword to display overall status information for each fan module.

Command Modes

scope chassis/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use this command without any arguments or keywords to display basic fan module information.

Example

This example shows how to show detailed information for a specific fan module:

```
firepower# scope chassis
firepower /chassis # show fan-module 1 2 detail

Fan Module:
    Tray: 1
    Module: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Product Name: Cisco Firepower 9000 Series Fan
    PID: FPR9K-FAN
    VID: 01
    Part Number: 73-17509-01
    Vendor: Cisco Systems Inc
    Serial (SN): NWG194500D8
    HW Revision: 0
    Mfg Date: 2015-11-07T00:00:00.000
firepower /chassis #
```

Related Commands

Command	Description
scope fan	Scopes into a specific fan.

show fault

To display fault information, use the **show fault** command.

show fault [*ID* | **cause** | **detail** | **severity** | **suppressed**]

Syntax Description

ID	(Optional) Display information for the specified fault only.
cause *label*	(Optional) Display faults with the specifed cause label; for example, `set-user-local-failed`.
detail	(Optional) Display detailed information about each fault.
severity {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	(Optional) Displays all faults of the specified severity: • **cleared** • **condition** • **critical** • **info** • **major** • **minor** • **warning**
suppressed	(Optional) Displays all suppressed faults. You also can optionally append the **cause** , **detail** , or **severity** keyword.

Command Modes

Any command mode

Command History

Release	Modification
1.0(1)	This command was introduced.

Example

This example shows how to display the fault list:

```
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0276    2025-12-16T07:08:08.542     52605 ether port 1/1 on fabric interconnect
 A oper state: link-down, reason: Link failure or not-connected
Major     F0276    2025-12-16T07:08:08.542     78300 ether port 1/5 on fabric interconnect
 A oper state: link-down, reason: Link failure or not-connected
Major     F0276    2025-12-16T07:08:08.542     78301 ether port 1/6 on fabric interconnect
 A oper state: link-down, reason: Link failure or not-connected
Warning   F16683   2025-12-16T07:08:00.670     78430 [FSM:STAGE:FAILED]: internal system
backup(FSM-STAGE:sam:dme:MgmtBackupBackup:upload)
```

```
Warning   F78123   2025-12-16T07:08:00.670     78428 [FSM:STAGE:REMOTE-ERROR]: Result:
end-point-failed Code: unspecified
Message: End point timed out. Check for IP, port, password, disk space or network access
related issues.#(sam:dme:MgmtBackupBackup:upload)

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
show server status	Shows information on the status of a server.

show fc

To display the information of fc class available on the system, use the **show fc** command.

show fc [**detail**]

Syntax Description

detail	Lists detailed fc class information.

Command Modes

scope eth-server, scope qos

Command History

Release	Modification
2.3.1	This command was introduced.

Usage Guidelines

This is a subcommand of the **show** command in scope eth-server, scope qos

Example

This example shows how tpo display system fc class information:

```
Firepower # scope eth-server
Firepower /eth-server # scope qos
Firepower /eth-server/qos # show fc

FC Class:
    Priority: Fc
    Cos: 3
    Weight: 5
    Bw Percent: 50
    Drop: No Drop
    Mtu: Fc
    Admin State: Enabled
```

This example shows howto displau detailed information of ethernet classified class:

```
Firepower /eth-server/qos # show eth-classified

Ethernet Classified Class:
    Priority: Platinum
    CoS: 5
    Weight: 10
    BW Percent: Not Applicable
    Drop: No Drop
    MTU: Normal
    Multicast Optimize: No
    Admin State: Disabled

    Priority: Gold
    CoS: 4
    Weight: 9
    BW Percent: Not Applicable
    Drop: Drop
    MTU: Normal
    Multicast Optimize: No
    Admin State: Disabled
```

```
    Priority: Silver
    CoS: 2
    Weight: 8
    BW Percent: Not Applicable
    Drop: Drop
    MTU: Normal
    Multicast Optimize: No
    Admin State: Disabled
```

This example shows how to display detailed information of ethernet best effort class:

```
Firepower /eth-server/qos # show eth-best-effort

Ethernet Best-Effort Class:
    Priority: Best Effort
    Cos: Any
    Weight: 5
    Bw Percent: 50
    Drop: Drop
    Mtu: 9198
    Multicast Optimize: No
    Admin State: Enabled
```

This example shows how to display the detailed information of ethernet best effort class:

```
Firepower /eth-server/qos # show eth-best-effort detail

Ethernet Best-Effort Class:
    Priority: Best Effort
    Cos: Any
    Weight: 5
    Bw Percent: 50
    Drop: Drop
    Mtu: 9198
    Multicast Optimize: No
    Admin State: Enabled
```

show fips-mode

To display current FIPS (Federal Information Processing Standard) mode status information, use the **show fips-mode** command.

show fips-mode

Syntax Description

This command has no arguments or keywords.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Enabling certification compliance on a Firepower 4100/9300 chassis does not automatically propagate compliance to any of its attached logical devices.

Example

This example shows how to enter security mode and display current FIPS mode status information:

```
FP9300-A # scope security
FP9300-A /security # show fips-mode
FIPS Mode Admin State: Disabled
FIPS Mode Operational State: Disabled
FP9300-A /security #
```

Related Commands

Command	Description
disable fips-mode	Disables FIPS mode.
enable fips-mode	Enables FIPS mode.

show firmware

To view system firmware information, use the **show firmware** command.

show firmware [**detail** | **expand** | **monitor** | **package-version**]

Syntax Description

detail	(Optional) Use this keyword to display the current firmware and start-up versions for the device, as well as the running version, its activate status, and the start-up version for the service manager.
expand	(Optional) Use this keyword to list an extensive list of version and status information for the various system components.
monitor	(Optional) Use this keyword to display current package version and upgrade status for the device manager, fabric interconnect, and chassis server(s).
package-version	(Optional) Use this keyword to display current package version for the device manager.

Command Modes

System mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use **show firmware monitor** repeatedly to monitor the status of a firmware upgrade download and activation.

Example

This example shows how to monitor firmware version and upgrade status:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.4(1.52)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.4(1.52)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.4(1.52)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.4(1.52)
        Upgrade-Status: Ready

FP9300-A /system #
```

Related Commands

Command	Description
activate firmware	Activates a firmware package.
show server firmware	Shows server firmware versions and status information.

show (firmware-install)

To display current firmware package information, use the **show** command in firmware-install mode.

show [**detail** | **event** | **fsm**]

Syntax Description

detail	(Optional) Use this keyword to display detailed firmware package information.
event [*event_ID* | **detail**]	(Optional) Use this keyword to display events logged during firmware upgrade; the **detail** keyword is available. Provide a specific *event_ID* to view information for only that event.
fsm {**status** | **task**}	(Optional) Use these keywords to show firmware upgrade-related finite state machine (FSM) status- or task-related information.

Command Modes

Firmware installation mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command shows information about the most-recently installed firmware package.

Example

This example shows how to display detailed information about the installed firmware package:

```
FP9300-A# scope firmware
FP9300-A /firmware # scope firmware-install
FP9300-A /firmware-install # show detail

Firmware Pack Install:
    Upgrade Package Version: 1.0.16
    Oper State: Ready
    Upgrade Status: Upgrade Complete Successful
    Current Task:
FP9300-A /firmware-install #
```

Related Commands

Command	Description
install firmware	Installs a firmware package.
show download-task	Shows information about firmware-package download operations
show firmware	Shows system firmware information.

show fsm status

To display contents of fsm details available on the system, use the **show fsm status** command.

show fsm status [**expand**]

Syntax Description

expand	Displays expanded information for fsm status. The expand keyword is available with this option.

Command Modes

scope fabric-interconnect a

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope fabric-interconnect a.

Example

This example shows how to display fsm status information:

```
Firepower # scope fabric-interconnect a
QP1 /fabric-interconnect # show fsm status

ID: A

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Update Switch Success
        Timestamp: 2012-07-05T23:47:10.032
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:

    FSM 2:
        Status: Nop
        Previous Status: SW Mgmt Oob Ipv6 If Config Success
        Timestamp: 2012-07-05T23:47:10.017
        Try: 0
        Progress (%): 100
        Current Task:

    FSM 3:
        Status:
        Previous Status:
        Timestamp:
        Try:
        Progress (%):
        Current Task:
```

This example shows how to display detailed information of fsm status:

```
Firepower /fabric-interconnect # show fsm status expand detail

ID: A

    FSM Status:

        Affected Object: sys/switch-A/mgmt/fsm
        Current FSM: Update Switch
        Status: Success
        Completion Time: 2012-07-05T23:47:10.033
        Progress (%): 100
        Description:
        Remote Result: Not Applicable
        Error Code: None
        Error Description:

        FSM Stage:

            Order: 1
            Stage Name: UpdateSwitchCopyToLocal
            Status: Skip
            Try: 0
            Last Update Time: 2012-07-05T23:46:54.941
            Stage Description: copying image from external repository to local repository
(FSM-STAGE: sam: dme: MgmtControllerUpdateSwitch: copyToLocal)

            Order: 2
            Stage Name: UpdateSwitchCopyToPeer
            Status: Skip
            Try: 0
            Last Update Time: 2012-07-05T23:46:54.942
            Stage Description: copying image from external repository to local repository
of peer (FSM-STAGE: sam: dme: MgmtControllerUpdateSwitch: copyToPeer

            Order: 3
            Stage Name: UpdateSwitchUpdateLocal
            Status: Success
            Try: 1
            Last Update Time: 2012-07-05T23:47:10.016
            Stage Description: updating local fabric interconnect (FSM-STAGE: sam:
dme: MgmtControllerUpdateSwitch: update Local)

            Order: 4
            Stage Name: UpdateSwitchVerifyLocal
            Status: Success
            Try: 1
            Last Update Time: 2012-07-05T23:47:10.027
```

show fw-infra-pack

To view a list of firmware infrastructure package available on the system, use the **show fw-infra-pack** command.

show fw-infra-pack [**detail**]

Syntax Description		
	detail	Lists detailed firmware package infrastructure information.

Command Modes scope org

Command History	Release	Modification
	2.3.1	Command added.

Usage Guidelines This is a subcommand of the **show** command in scope org.

Example

This example shows how to display information of all the system firmware infrastructure packages:

```
Firepower /fabric-interconnect # scope org
Firepower /org # show fw-infra-pack
Infra Pack:
    Name                 Description Infrastructure Bundle Version
    -------------------- ----------- ------------------------------
    default              Infrastructure Pack
                                     92.14(0.0808g_libtirpc)
```

Example

This example shows how to display detailed information of all the available system firmware infrastructure packages:

```
Firepower /org # show fw-infra-pack expand detail
Infra Pack:
    Name: default
    Description: Infrastructure Pack
    Infrastructure Bundle Version: 92.14(0.0808g_libtirpc)

    Pack Image:
HW Vendor: Cisco Systems
        HW Model: FPR-Manager
        Type: System
        Version: 92.13(0.0808g)
        Presence: Present

        HW Vendor: Cisco Systems
        HW Model: MGMTEXT
        Type: 17
        Version: 92.13(0.107g)
        Presence: Present
```

```
HW Vendor: Cisco Systems, Inc.
HW Model: F9K-C9300-SUP-K9
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: F9K-C9300-SUP-K9
Type: Fabric Interconnect System
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4110-SUP
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4110-SUP
Type: Fabric Interconnect System
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4112-SUP
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4112-SUP
Type: Fabric Interconnect System
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4115-SUP
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present
```

show hardware-bypass-ports

To display hardware bypass ports information, use the **show hardware-bypass-ports** command.

show hardware-bypass-ports

Syntax Description

show hardware-bypass-ports	(Optional) Displays hardware bypass information.

Command Modes

Any command mode

Command History

Release	Modification
2.6(1)	Command added.

Usage Guidelines

This command does not require a license.

Example

This example shows how to display bypass port pairs information:

```
FPR # scope fabric-interconnect
FPR /fabric-interconnect # show hardware-bypass-ports

hardware-bypass port pairs:

Port1                Port2                Mode              Oper Mode      WDT      WDT Val
---------------- ---------------- ---------------- ---------------- -------- -------
Ethernet2/1      Ethernet2/2      Standby          Standby          Enabled  1000 <-------Pair
 Ethernet 2/1-2 is in standby mode
Ethernet2/3      Ethernet2/4      Disabled         Disabled         Disabled 0
Ethernet2/5      Ethernet2/6      Disabled         Disabled         Disabled 0
Ethernet2/7      Ethernet2/8      Disabled         Disabled         Disabled 0
Ethernet3/1      Ethernet3/2      Disabled         Disabled         Disabled 0
Ethernet3/3      Ethernet3/4      Switch Bypass    Switch Bypass    Enabled  1000
<-------Pair Ethernet 3/3-4 is in bypass mode (bypass is active)
Ethernet3/5      Ethernet3/6      Switch Bypass    Switch Bypass    Enabled  1000 <-------Pair
 Ethernet 3/5-6 is in bypass mode (bypass is active)
```

Related Commands

Command	Description
scope fabric-interconnect	Enters fabric interconnect mode.

show https

To display the current HTTPS service configuration, use the **show https** command.

show https

Syntax Description

This command has no arguments or keywords.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display the current HTTPS service configuration:

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # show https
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: default
    Cipher suite mode: Medium Strength
    Cipher suite: ALL:!EDH-RSA-DES-CBC3-SHA:!EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:
    !ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
    Https authentication type: Cred Auth
    Crl mode: Relaxed
FP9300-A /system/services #
```

Related Commands

Command	Description
set https auth-type	Specifies the type of authentication for HTTPS access.

show hw-crypto

To show the status of TLS crypto acceleration, use the **show hw-crypto** command. For more information about TLS crypto acceleration, see the *Management Center Configuration Guide*.

show hw-crypto

Command Modes

connect module

Command History

Release	Modification
2.7.1	This command was introduced.

Usage Guidelines

This command displays the status of TLS crypto acceleration for a container instance.

Examples

Following is an example of showing the status of TLS crypto acceleration:

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ---------- ------------ ---------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                    Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # show hw-crypto

Hardware Crypto:
    Admin State Hardware Crypto Size Hardware Crypto Version
    ----------- -------------------- ------------------------
    Enabled     13%                  2
```

Related Commands

Command	Description
create hw-crypto	Create a TLS crypto acceleration configuration for a container instance.
delete hw-crypto	Delete a TLS crypto acceleration configuration for a container instance.
scope hw-crypto	Enable or disable TLS crypto acceleration configuration on a container instance.

show image

To display a list of images available on the system, use the **show image** command.

show image [**detail** | **type** | **version**]

Syntax Description

detail	Lists detailed image information.
type	(Optional) Displays information about the current image type.
version	(Optional) Displays firmware version information.

Command Modes

scope firmware

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope firmware.

.

Example

This example shows information of all the system images:

```
Firepower # scope firmware
Firepower /firmware# show image

Name                                        Type                Version
------------------------------------------- ------------------- -------
fxos-b200-m5-brdprog.11.0.bin               Board Controller    11.0
fxos-b200-m5-brdprog.5.0.bin                Board Controller    5.0
fxos-k9-compatibility.2.10.1. 1102.json      FXOS CSP Compatibility
                                                                2.10(1.1102)
fxos-k9-compatibility.2.10.1. 159.json       FXOS CSP Compatibility
                                                                2.10(1.159)
fxos-k9-compatibility.2.10.1.175_r. json     FXOS CSP Compatibility
                                                                2.10(1.175_r)
fxos-k9-compatibility.2.10.1. 177.json       FXOS CSP Compatibility
                                                                2.10(1.177)
fxos-k9-compatibility.2.10.1. 179.json       FXOS CSP Compatibility
                                                                2.10(1.179)
fxos-k9-compatibility.2.10.1.192_fix. json   FXOS CSP Compatibility
                                                                2.10(1.192_fi
x)
fxos-k9-compatibility.2.10.1. 193.json       FXOS CSP Compatibility
                                                                2.10(1.193)
fxos-k9-compatibility.2.10.1.198_rf. json    FXOS CSP Compatibility
                                                                2.10(1.198_rf
)
fxos-k9-compatibility.2.10.1. 199.json       FXOS CSP Compatibility
                                                                2.10(1.199)
fxos-k9-compatibility.2.10.1. 207.json       FXOS CSP Compatibility
                                                                2.10(1.207)
```

```
fxos-k9-compatibility.2.11.1. 156.json         FXOS CSP Compatibility
                                                                    2.11(1.156)
fxos-k9-compatibility.2.11.1.1922f_dpipev. json
                                               FXOS CSP Compatibility
                                                                    2.11(1.1922f_
dpipev)
fxos-k9-compatibility.2.11.1.2022f_cpio. json FXOS CSP Compatibility
                                                                    2.11(1.2022f_
cpio)
fxos-k9-compatibility.2.11.1.2022f_modsec. json
                                               FXOS CSP Compatibility
```

This example shows detailed information of images:

```
Firepower/firmware# show image detail

Image fxos-b200-m5-brdprog.11.0.bin:
    Type: Board Controller
    Version: 11.0
    Size: 1391730
    Supported Models:
        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-12S

        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-24S

        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-32S

        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-44S

        Vendor: Cisco Systems Inc
        Model: FPR9K-SM-40

        Vendor: Cisco Systems Inc
        Model: FPR9K-SM-48

        Vendor: Cisco Systems Inc
```

show image detail

To display a list of kick-start and system images available on the system, use the **show image** command.

show image detail

Syntax Description

detail	Lists detailed image information.

Command Modes

scope fabric-interconnect

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope fabric-interconnect mode.

.

Example

This example shows information of all the kickstart and system images:

```
firepower# /system/services # scope fabric-interconnect
firepower# /fabric-interconnect # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
fxos-k9-kickstart.5.0.3.N2.4.111.85.SPA    Fabric Interconnect Kernel
                                                                 5.0(3)N2(4.11
1.85)
fxos-k9-kickstart.5.0.3.N2.92.130.257g.gSSB   Fabric Interconnect Kernel
                                                                 5.0(3)N2(92.1
30.257g)
fxos-k9-system.5.0.3.N2.4.111.85.SPA       Fabric Interconnect System
                                                                 5.0(3)N2(4.11
1.85)
fxos-k9-system.5.0.3.N2.92.130.257g.gSSB   Fabric Interconnect System
                                                                 5.0(3)N2(92.1
30.257g)
Mahendra-QPD /fabric-interconnect #
```

show identity

To display a variety of system information, use the **show identity** command.

show identity {**ip-addr** | **ipv6-addr** | **iqn** | **mac-addr** | **uuid** | **wwn**}

Syntax Description

ip-addr	(Optional) Lists information for all available IP addresses. The following optional keywords are available: • *IPv4_address*—Displays identity information for the specified IPv4 address. • **detail** —Displays detailed IPv4 address identity information. • **pool-info** —Displays IPv4 address information for the pool. The **detail** keyword is also available. • **profile-info** —Displays IPv4 address information for the profile. The **detail** keyword is also available.
ipv6-addr	(Optional) Lists information for all available IPv6 addresses. The following optional keywords are available: • **detail** —Displays detailed IPv6-address identity information. • **pool-info** —Displays IPv6-address information for the pool. The **detail** keyword is also available. • **profile-info** —Displays IPv6-address information for the profile. The **detail** keyword is also available. • *IPv6_address*—Displays identity information for the specified IPv6 address.

iqn	(Optional) Displays information on the iSCSI Qualified Name (IQN) identities for a system. The following optional keywords are also available: • **detail** —Displays details about the identity information in list format. • **pool-info** —Displays IQN identity information for the pool. The **detail** keyword is also available. • **profile-info** —Displays IQN identity information for the profile. The **detail** keyword is also available. • *prefix* —Displays information for the specified IQN prefix. • *name* —Displays information for the named IQN identity; can be a maximum of 510 characters. By default, this command lists information on all IQN identities configured for an IQN pool.
mac-addr	(Optional) Displays MAC-address identity information for a system. The following optional keywords are also available: • *id* —Displays identity information for a specific MAC address. Specify a MAC address in the format AA:BB:CC:DD:EE:FF. • **detail** —Displays details about the identity information in list format. • **pool-info** —Displays MAC-address identity information for the pool. The **detail** keyword is also available. • **profile-info** —Displays MAC-address identity information for the profile. The **detail** keyword is also available.
uuid	(Optional) Displays the universally unique identifier (UUID) identity information for a system. The following optional keywords are also available: • **derived** *id*—Displays derived identity information for the specified UUID; entered in the form `FFFF-FFFFFFFFFFFF`. • **detail** —Displays detailed UUID identity information. • *uuid_prefix* —Displays identity information for the specified UUID prefix; entered in the form `FFFFFFFF-FFFF-FFFF`. • *uuid* —Displays identity information for the specified UUID; entered in the form `FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF`. • **pool-info** —Displays UUID identity information for the pool. The **detail** keyword is also available. • **profile-info** —Displays UUID identity information for the profile. The **detail** keyword is also available.

wwn	(Optional) Displays the world-wide name (WWN) information for a system. The following optional keywords are also available: • **detail** —Displays details about the identity information in list format. • *id* —Displays identity information for a specific WWN; provide a unique WWN identifier in the form `FF:FF:FF:FF:FF:FF:FF:FF`. • **pool-info** —Displays identity information for the pool. The **detail** keyword is also available. • **profile-info** —Displays identity information for the profile. The **detail** keyword is also available.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

IQN pools and prefixes must be configured in order to use the **show identity iqn** command.

Example

This example shows how to display detailed identity information for the device's IPv4 addresses:

```
FP9300-A# show identity ip-addr detail
IP Address: 192.0.2.9
    Assigned: No
    Assigned Service Profile:
    Owner: Pool
IP Address: 192.0.2.10
    Assigned: No
    Assigned Service Profile:
    Owner: Pool
IP Address: 192.0.2.11
    Assigned: No
    Assigned Service Profile:
    Owner: Pool
IP Address: 192.0.2.12
    Assigned: No
    Assigned Service Profile:
    Owner: Pool

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
show server identity	Shows identity information for a servers, adapters and interfaces.

show interface

To view Ethernet interface status, use the **show interface** command.

show interface [**detail** | **expand** | **fsm status** | *interface_id*]

Syntax Description

detail	Shows detailed interface information.
expand	Shows information about interfaces in a non-tabular view, as well as information about subinterfaces.
fsm status	Shows Finite State Machine (FSM) status.
interface_id	Shows information about a particular Ethernet interface, for example, Ethernet1/4.

Command Modes

scope eth-uplink/scope fabric a/

Command History

Release	Modification
2.4(1)	Additional fields were added for VLAN subinterfaces.
1.1(1)	Command added.

Usage Guidelines

This command only applies to Ethernet interfaces. For EtherChannels, see the **show port-channel** command. For subinterfaces, see the **show subinterface** command.

Note Unidirectional link detection (UDLD) is not supported by FXOS; ignore any references to UDLD.

Example

The following is sample output from the **show interface** command.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       Allowed Vlan State
Reason
    --------------- ------------------ ----------- ---------------- ------------ ------------

    Ethernet1/2     Data               Enabled     Up               All
    Ethernet1/4     Mgmt               Enabled     Up               All
    Ethernet1/5     Data               Enabled     Up               Untagged
    Ethernet1/7     Firepower Eventing Enabled     Up               All
    Ethernet1/8     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/1     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/2     Data               Disabled    Sfp Not Present  All          Unknown
```

```
    Ethernet2/3     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/4     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/5     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/6     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/7     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/8     Data               Disabled    Sfp Not Present  All          Unknown
```

The following is sample output from the **show interface detail** command.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # show interface detail

Interface:
    Port Name: Ethernet1/2
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:

    Port Name: Ethernet1/4
    User Label:
    Port Type: Mgmt
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:

[...]
```

The following is sample output from the **show interface expand** command.

```
firepower# scope eth-uplink
```

```
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # show interface expand

Interface:
    Port Name: Ethernet1/2
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    Allowed Vlan: All
    State Reason:

    Port Name: Ethernet1/4
    Port Type: Mgmt
    Admin State: Enabled
    Oper State: Up
    Allowed Vlan: All
    State Reason:

    Port Name: Ethernet1/5
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    Allowed Vlan: Untagged
    State Reason:

    Sub Interface:
        Sub-If Id  Sub-Interface Name VLAN        Port Type
        ---------- ------------------ ----------- ---------
               100 Ethernet1/5.100    500         Data Sharing
```

Related Commands

Command	Description
show port-channel	Shows EtherChannel status.
show subinterface	Shows subinterface status.

show interface counter errors (connect fxos)

To view the interface counter errors, use the **show interface counter errors** command.

show interface counter errors

Syntax Description

Align-Err	Alignment errors are a count of the number of frames received that don't end with an even number of octets and have a bad Cyclic Redundancy Check (CRC). Common Causes: Alignment errors are usually the result of a duplex mismatch or a physical problem (such as cabling, a bad port, or a bad NIC). When the cable is first connected to the port, some of these errors can occur. Also, if there is a hub connected to the port, collisions between other devices on the hub can cause these errors.
FCS-Err	The number of valid size frames with Frame Check Sequence (FCS) errors but no framing errors. Common Causes: This is typically a physical issue (such as cabling, a bad port, or a bad Network Interface Card (NIC)) but can also indicate a duplex mismatch.
Xmit-Err	This is an indication that the internal send (Tx) buffer is full. Common Causes: A common cause of Xmit-Err can be traffic from a high-bandwidth link that is switched to a lower bandwidth link, or traffic from multiple inbound links that are switched to a single outbound link. For example, if a large amount of bursty traffic comes in on a gigabit interface and is switched out to a 100Mbps interface, this can cause Xmit-Err to increment on the 100Mbps interface. This is because the output buffer of the interface is overwhelmed by the excess traffic due to the speed mismatch between the inbound and outbound bandwidths.
Rcv-Err	A receive error (that is, Rcv-Err) occurs when a port receives buffer overflows. Congestion on a switch's backplane could cause the receive buffer on a port to fill to capacity, as frames await access to the switch's backplane. However, most likely, an Rcv-Err is indicating a duplex mismatch.
Undersize	The frames received that are smaller than the minimum IEEE 802.3 frame size of 64 bytes (which excludes framing bits but includes FCS octets) that are otherwise well formed. Common Causes: Check the device that sends out these frames.
Out-Discard	The number of outbound packets chosen to be discarded even though no errors have been detected. Common Causes: One possible reason to discard such a packet can be to free up buffer space.

Single-Col	The number of times one collision occurred before the interface transmitted a frame to the media successfully. Common Causes: Collisions are normal for interfaces configured as half duplex but must not be seen on full duplex interfaces. If collisions increase dramatically, this points to a highly utilized link or possibly a duplex mismatch with the attached device.
Multi-Col	The number of times multiple collisions occurred before the interface transmitted a frame to the media successfully. Common Causes: Collisions are normal for interfaces configured as half duplex but must not be seen on full duplex interfaces. If collisions increase dramatically, this points to a highly utilized link or possibly a duplex mismatch with the attached device.
Late-Col	The number of times a collision is detected on a particular interface late in the transmission process. For a 10 Mbit/s port this is later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. Common Causes: This error can indicate a duplex mismatch among other things. For the duplex mismatch scenario, the late collision is seen on the half duplex side. As the half duplex side is transmitting, the full duplex side does not wait its turn and transmits simultaneously which causes a late collision. Late collisions can also indicate an Ethernet cable or segment that is too long. Collisions must not be seen on interfaces configured as full duplex.
Excess-Col	A count of frames for which transmission on a particular interface fails due to excessive collisions. An excessive collision happens when a packet has a collision 16 times in a row. The packet is then dropped. Common Causes: Excessive collisions are typically an indication that the load on the segment needs to be split across multiple segments but can also point to a duplex mismatch with the attached device. Collisions must not be seen on interfaces configured as full duplex.
Carri-Sen	The Carri-Sen (carrier sense) counter increments every time an Ethernet controller wants to send data on a half-duplex connection. The controller senses the wire and checks if it is not busy before transmitting. Common Causes: This is normal on a half-duplex Ethernet segment.

Runts	The frames received that are smaller than the minimum IEEE 802.3 frame size (64 bytes for Ethernet), and with a bad CRC. Common Causes: This can be caused by a duplex mismatch and physical problems, such as a bad cable, port, or NIC on the attached device. Platform Exceptions: Catalyst 4000 Series that run Cisco IOS Previous to software Version 12.1(19)EW, a runt = undersize. Undersize = frame < 64bytes. The runt counter only incremented when a frame less than 64 bytes was received. After 12.1(19EW, a runt = a fragment. A fragment is a frame < 64 bytes but with a bad CRC. The result is the runt counter now increments in show interfaces, along with the fragments counter in show interfaces counters errors when a frame <64 bytes with a bad CRC is received. Cisco Catalyst 3750 Series Switches In releases prior to Cisco IOS 12.1(19)EA1, when dot1q is used on the trunk interface on the Catalyst 3750, runts can be seen on show interfaces output because valid dot1q encapsulated packets, which are 61 to 64 bytes and include the q-tag, are counted by the Catalyst 3750 as undersized frames, even though these packets are forwarded correctly. In addition, these packets are not reported in the appropriate category (unicast, multicast, or broadcast) in receive statistics. This issue is resolved in Cisco IOS release 12.1(19)EA1 or 12.2(18)SE or later.
Giants	Frames received that exceed the maximum IEEE 802.3 frame size (1518 bytes for non-jumbo Ethernet) and have a bad Frame Check Sequence (FCS). Common Causes: In many cases, this is the result of a bad NIC. Try to find the offending device and remove it from the network. Platform Exceptions: Catalyst Cat4000 Series that run Cisco IOS Previous to software Version 12.1(19)EW, the giants counter incremented for a frame > 1518bytes. After 12.1(19)EW, a giant in show interfaces increments only when a frame is received >1518bytes with a bad FCS.
IntMacTx-Er	Interface mac TX - Transmission error
IntMacRx-Er	Interface mac RX - Reception error
Symbol-Err	Symbol-Err is seen when the Mac sees "invalid" symbols. In most cases, this is a physical problem - Gbics, fiber, etc. These errors also increment when the link is not up because the Mac isn't synchronized and receives noise. Small amounts of symbol errors can be ignored. Large amounts of symbol errors can indicate a bad device, cable, or hardware.
Deferred-tx	Deferred-tx increments every sec. Number of first transmission attempts delayed because the medium was busy.

SQETest-Err	SQE stands for "Signal Quality Error" and may also be referred to the Ethernet "heartbeat". With early Ethernet cards that required transceivers, the transceiver would send a "Signal Quality Error" back to the Ethernet card after each frame was transmitted to insure that the collision detection circuitry was working. With modern network cards, this SQE test can cause network cards to believe that an actual collision occurred, and a collision is sent out on the network when a SQE test is detected. This can seriously degrade network performance, as each frame successfully transmitted on the network is followed by a collision caused by the SQE test. Cause 1: SQE Test Errors can be caused by a transceiver that have the "SQE test" dip switch turned on (it should be turned off). Check the switch settings on all transceivers on the segment. Cause 2: SQE Test errors can be caused by broken transceivers. Check for failed transceivers on the segment.

Command Modes

connect fxos

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This command displays the interface counter errors.

Example

This example shows how to display the interface counter errors information:

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show interface counters errors
-------------------------------------------------------------------------------
Port          Align-Err    FCS-Err   Xmit-Err    Rcv-Err  UnderSize OutDiscards
-------------------------------------------------------------------------------
Eth1/1                0          0          0          0          0           0
Eth1/2                0          0          0          0          0           0
Eth1/3                0          0          0          0          0           0
Eth1/4                0          0          0          0          0           0
Eth1/5                0          0          0          0          0           0
Eth1/6                0          0          0          0          0           0
Eth1/7                0          0          0          0          0           0
Eth1/8                0          0          0          0          0           0
Eth1/9                0 1378344622          0 1384807633          0           0
Eth1/10               0          0          0          0          0           0
Eth1/11               0          0          0          0          0           0
Eth1/12               0          0          0          0          0           0
Eth2/1                0          0          0          0          0           0
Eth2/2                0          0          0          0          0           0
Eth2/3                0          0          0          0          0           0
Eth2/4                0          0          0          0          0           0
Eth2/5                0          0          0          0          0           0
Eth2/6                0          0          0          0          0           0
Eth2/7                0          0          0          0          0           0
Eth2/8                0          0          0          0          0           0
Po1                   0          0          0          0          0           0
Po48                  0          0          0          0          0           0
Veth687              --         --         --         --         --           0
```

```
Veth688               --         --         --         --         --           0
Veth689               --         --         --         --         --           0
Veth690               --         --         --         --         --           0
Veth691               --         --         --         --         --           0
Veth692               --         --         --         --         --           0
Veth693               --         --         --         --         --           0
Veth694               --         --         --         --         --           0
Veth695               --         --         --         --         --           0
Veth696               --         --         --         --         --           0
Veth697               --         --         --         --         --           0
Veth698               --         --         --         --         --           0
Veth718               --         --         --         --         --           0
Veth736               --         --         --         --         --           0
Veth737               --         --         --         --         --           0
Veth772               --         --         --         --         --           0
Veth773               --         --         --         --         --           0
Veth774               --         --         --         --         --           0
Veth775               --         --         --         --         --           0
Veth776               --         --         --         --         --           0
Veth777               --         --         --         --         --           0
Veth855               --         --         --         --         --           0
Veth856               --         --         --         --         --           0
Veth857               --         --         --         --         --           0
Veth858               --         --         --         --         --           0
Veth859               --         --         --         --         --           0
Veth860               --         --         --         --         --           0
Veth861               --         --         --         --         --           0
Veth862               --         --         --         --         --           0

--------------------------------------------------------------------------------
Port          Single-Col  Multi-Col   Late-Col  Exces-Col  Carri-Sen        Runts
--------------------------------------------------------------------------------
Eth1/1                 0          0          0          0          0            0
Eth1/2                 0          0          0          0          0            0
Eth1/3                 0          0          0          0          0            0
Eth1/4                 0          0          0          0          0            0
Eth1/5                 0          0          0          0          0            0
Eth1/6                 0          0          0          0          0            0
Eth1/7                 0          0          0          0          0            0
Eth1/8                 0          0          0          0          0            0
Eth1/9                 0          0          0          0          0            0
Eth1/10                0          0          0          0          0            0
Eth1/11                0          0          0          0          0            0
Eth1/12                0          0          0          0          0            0
Eth2/1                 0          0          0          0          0            0
Eth2/2                 0          0          0          0          0            0
Eth2/3                 0          0          0          0          0            0
Eth2/4                 0          0          0          0          0            0
Eth2/5                 0          0          0          0          0            0
Eth2/6                 0          0          0          0          0            0
Eth2/7                 0          0          0          0          0            0
Eth2/8                 0          0          0          0          0            0
Po1                    0          0          0          0          0            0
Po48                   0          0          0          0          0            0
Veth687               --         --         --         --         --           --
Veth688               --         --         --         --         --           --
Veth689               --         --         --         --         --           --
Veth690               --         --         --         --         --           --
Veth691               --         --         --         --         --           --
Veth692               --         --         --         --         --           --
Veth693               --         --         --         --         --           --
Veth694               --         --         --         --         --           --
Veth695               --         --         --         --         --           --
Veth696               --         --         --         --         --           --
```

```
Veth697              --         --         --         --         --         --
Veth698              --         --         --         --         --         --
Veth718              --         --         --         --         --         --
Veth736              --         --         --         --         --         --
Veth737              --         --         --         --         --         --
Veth772              --         --         --         --         --         --
Veth773              --         --         --         --         --         --
Veth774              --         --         --         --         --         --
Veth775              --         --         --         --         --         --
Veth776              --         --         --         --         --         --
Veth777              --         --         --         --         --         --
Veth855              --         --         --         --         --         --
Veth856              --         --         --         --         --         --
Veth857              --         --         --         --         --         --
Veth858              --         --         --         --         --         --
Veth859              --         --         --         --         --         --
Veth860              --         --         --         --         --         --
Veth861              --         --         --         --         --         --
Veth862              --         --         --         --         --         --

--------------------------------------------------------------------------------
Port          Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err
--------------------------------------------------------------------------------
Eth1/1             0         --           0           0           0          0
Eth1/2             0         --           0           0           0          0
Eth1/3             0         --           0           0           0          0
Eth1/4             0         --           0           0           0          0
Eth1/5             0         --           0           0           0          0
Eth1/6             0         --           0           0           0          0
Eth1/7             0         --           0           0           0          0
Eth1/8             0         --           0           0           0          0
Eth1/9             0         --           0     6463011           0          0
Eth1/10            0         --           0           0           0          0
Eth1/11            0         --           0           0           0          0
Eth1/12            0         --           0           0           0          0
Eth2/1             0         --           0           0           0          0
Eth2/2             0         --           0           0           0          0
Eth2/3             0         --           0           0           0          0
Eth2/4             0         --           0           0           0          0
Eth2/5             0         --           0           0           0          0
Eth2/6             0         --           0           0           0          0
Eth2/7             0         --           0           0           0          0
Eth2/8             0         --           0           0           0          0
Po1                0         --           0           0           0          0
Po48               0         --           0           0           0          0
Veth687           --         --          --          --          --         --
Veth688           --         --          --          --          --         --
Veth689           --         --          --          --          --         --
Veth690           --         --          --          --          --         --
Veth691           --         --          --          --          --         --
Veth692           --         --          --          --          --         --
Veth693           --         --          --          --          --         --
Veth694           --         --          --          --          --         --
Veth695           --         --          --          --          --         --
Veth696           --         --          --          --          --         --
Veth697           --         --          --          --          --         --
Veth698           --         --          --          --          --         --
Veth718           --         --          --          --          --         --
Veth736           --         --          --          --          --         --
Veth737           --         --          --          --          --         --
Veth772           --         --          --          --          --         --
Veth773           --         --          --          --          --         --
Veth774           --         --          --          --          --         --
Veth775           --         --          --          --          --         --
```

```
Veth776           --          --          --          --          --          --
Veth777           --          --          --          --          --          --
Veth855           --          --          --          --          --          --
Veth856           --          --          --          --          --          --
Veth857           --          --          --          --          --          --
Veth858           --          --          --          --          --          --
Veth859           --          --          --          --          --          --
Veth860           --          --          --          --          --          --
Veth861           --          --          --          --          --          --
Veth862           --          --          --          --          --          --
firepower(fxos)#
```

show interface transceiver (connect fxos)

To view the transceiver details and calibrations, use the **show interface transceiver** command.

show interface transceiver | **details** | **calibrations**

Syntax Description

details	Shows detailed interface transceiver information.
calibrations	Shows detailed calibration information.

Command Modes

connect fxos

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

This command is a subcommand of the **show interface** command in the **connect fxos** shell.

Example

This example shows how to display a brief set of interface transceiver-related information:

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show interface transceiver calibrations
Ethernet1/1
    transceiver is present
    type is 1000base-T
    name is CISCO-METHODE
    part number is SP7041-R
    revision is
    serial number is ABCD1234
    nominal bitrate is 1300 MBit/sec
    Link length supported for copper is 100 m
    cisco id is --
    cisco extended id number is 4

firepower(fxos)# show interface transceiver details
Ethernet1/1
    transceiver is present
    type is 1000base-T
    name is CISCO-METHODE
    part number is SP7041-R
    revision is
    serial number is ABCD1234
    nominal bitrate is 1300 MBit/sec
    Link length supported for copper is 100 m
    cisco id is --
    cisco extended id number is 4

DOM is not supported
```

show interface brief (connect fxos)

To view or save a reduced set of interface status and other other information, use the **show interface brief** command.

show interface brief

Syntax Description

This command has no arguments or keywords.

Command Modes

connect fxos/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

This command is a subcommand of the **show interface** command in the **connect fxos** shell.

Example

This example shows how to display a brief set of interface-related information:

```
firepower # connect fxos
firepower(fxos)# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth1/1        1       eth  1qtunl up      none                      1000(D) 48
Eth1/2        1       eth  1qtunl up      none                      1000(D) --
Eth1/3        1       eth  1qtunl down    suspended(no LACP PDU)    1000(D) 1
Eth1/4        1       eth  1qtunl up      none                      1000(D) --
Eth1/5        1       eth  1qtunl up      none                      1000(D) --
Eth1/6        1       eth  1qtunl up      none                      1000(D) 2
Eth1/7        1       eth  1qtunl up      none                      1000(D) --
Eth1/8        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth1/9        1       eth  vntag  up      none                       40G(D) --
Eth1/10       1       eth  vntag  up      none                       40G(D) --
Eth1/11       1       eth  vntag  up      none                       40G(D) --
Eth1/12       1       eth  vntag  up      none                       40G(D) --
Eth1/13       1       eth  access down    Administratively down      40G(D) --
Eth1/14       1       eth  access down    Administratively down      40G(D) --
Eth1/15       1       eth  access down    Administratively down     1000(D) --
Eth1/16       1       eth  access down    Administratively down     1000(D) --
Eth2/1        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/2        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/3        1       eth  1qtunl down    SFP not inserted          1000(D) --
Eth2/4        1       eth  1qtunl down    SFP not inserted          1000(D) --
Eth2/5        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/6        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/7        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/8        1       eth  1qtunl down    SFP not inserted           10G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN    Type Mode   Status  Reason                     Speed   Protocol
```

```
Interface
--------------------------------------------------------------------------------
Po1          1       eth  1qtunl down    No operational members      1000(D)  lacp
Po2          1       eth  1qtunl up      none                      a-1000(D)  lacp
Po48         1       eth  1qtunl up      none                      a-1000(D)  lacp

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           down   --                                      --       1500

--------------------------------------------------------------------------------
Vethernet     VLAN   Type Mode   Status  Reason                     Speed
--------------------------------------------------------------------------------
Veth721       4047   virt trunk  up      none                     auto
Veth722       1      virt trunk  up      none                     auto
Veth723       1      virt trunk  up      none                     auto
Veth724       1      virt trunk  up      none                     auto
Veth725       1      virt trunk  up      none                     auto
Veth726       4047   virt trunk  up      none                     auto
Veth727       4047   virt trunk  up      none                     auto
Veth728       4047   virt trunk  up      none                     auto
Veth736       1      virt trunk  up      none                     auto
Veth737       1      virt trunk  down    Administratively down    auto
Veth738       1      virt trunk  down    Administratively down    auto
Veth739       4047   virt trunk  up      none                     auto
Veth740       4047   virt trunk  up      none                     auto
Veth741       4047   virt trunk  up      none                     auto
Veth757       4047   virt trunk  up      none                     auto
Veth758       1      virt trunk  up      none                     auto
Veth759       1      virt trunk  up      none                     auto
Veth760       1      virt trunk  up      none                     auto
Veth761       1      virt trunk  up      none                     auto
Veth762       4047   virt trunk  up      none                     auto
Veth763       4047   virt trunk  up      none                     auto
Veth764       4047   virt trunk  up      none                     auto
Veth772       1      virt trunk  down    Administratively down    auto
Veth773       1      virt trunk  down    Administratively down    auto
Veth774       1      virt trunk  down    Administratively down    auto
Veth775       4047   virt trunk  up      none                     auto
Veth776       4047   virt trunk  up      none                     auto
Veth777       4047   virt trunk  up      none                     auto
Veth792       1      virt trunk  up      none                     auto
Veth793       1      virt trunk  up      none                     auto
Veth794       1      virt trunk  up      none                     auto
Veth797       1      virt trunk  up      none                     auto
Veth798       1      virt trunk  up      none                     auto
Veth800       1      virt trunk  up      none                     auto
Veth801       1      virt trunk  up      none                     auto
Veth802       1      virt trunk  up      none                     auto
Veth805       1      virt trunk  up      none                     auto
Veth806       1      virt trunk  up      none                     auto
Veth2182      1      virt trunk  up      none                     auto
Veth2328      1      virt trunk  up      none                     auto
Veth2482      1      virt trunk  up      none                     auto
Veth2502      1      virt trunk  up      none                     auto
Veth2503      1      virt trunk  down    nonParticipating         auto
Veth2504      1      virt trunk  up      none                     auto
Veth2636      1      virt trunk  up      none                     auto
Veth2637      1      virt trunk  up      none                     auto
Veth2638      1      virt trunk  down    nonParticipating         auto
Veth2639      1      virt trunk  up      none                     auto
Veth2640      1      virt trunk  up      none                     auto
Veth2660      1      virt trunk  up      none                     auto
```

```
Veth2661      1      virt trunk  down    nonParticipating         auto
Veth2662      1      virt trunk  up      none                     auto
Veth2788      1      virt trunk  up      none                     auto
Veth2789      1      virt trunk  down    nonParticipating         auto
Veth2790      1      virt trunk  up      none                     auto
Veth2791      1      virt trunk  up      none                     auto
firepower(fxos)#
```

The following table describes the columns displayed by the `show interface brief` command.

Table 5: show interface brief Fields

Field	Description
Interface ID	*Interface or port identifier*
VLAN	*VLAN identifier*
Type	**Interface type:** `eth` – dedicated Ethernet interface `virt` – virtual interface
Mode	**Operational port mode:** `layer3` – Layer 3 interface `access` – access port `trunk` – trunk port `pvlan` – private VLAN `fabric` – fabric port (F_port) `1qtunl` – 1q-tunnel (802.1Q tunnel) port `f-path` – fabric path
Status	**Interface state:** `up` – port is operationally up `down` – port is operationally down `testing` – interface is in test mode; no operational packets can be passed `trunking` – trunking is enabled `link up` – link is up, but port is not yet fully operational for traffic to the data plane, although it is operational for control protocols

Field	Description
Reason	

Field	Description
	Detailed interface state reason:
	Transceiver Initializing
	Other
	None
	Hardware failure
	Diag failure
	Error disabled
	Port Software failure
	Link failure or not connected
	offline
	Non participating
	Initializing
	Inactive
	Administratively down
	Channel admin down
	Suspended (interface)
	Suspended (port)
	Channel membership update in progress
	RCF is in progress
	Isolation due to ELP failure
	Isolation due to ESC failure
	Isolation due to domain overlap
	Isolation due to domain id assignment failure
	Isolation due to domain other side eport isolated
	Isolation due to invalid fabric reconfiguration
	Isolation due to domain manager disabled
	Isolation due to zone merge failure
	Isolation due to vsan not configured on peer
	Parent Interface Admin Down
	Tunnel port src interface unbound
	Interface is removed
	SFP not present
	Error disabled due to SFP vendor not supported

Field	Description
	Error disabled due to incompatible admin port mode
	Error disabled due to incompatible admin port speed
	Suspended due to incompatible mode
	Suspended due to incompatible speed
	Suspended due to incompatible remote switch WWN
	Isolation due to domain manager other side not responding
	Error Disabled due to EPP Failure
	Isolation due to port vsan mismatch
	Isolation due to port loopback to same switch
	Linecard upgrade in progress
	Error disabled due to incompatible admin port rxbbcredit
	Error disabled due to incompatible admin port rxbufsize
	No operational members
	Isolation due to remote zone server not responding
	Error disabled due to first interface in this group is E
	Error disabled due to other interfaces in this group are not shut
	TCP connection closed by peer
	TCP connection rest by peer
	TCP max retransmission reached
	TCP keep alive timer expired
	TCP persist timer expired
	Parent ethernet link down
	Parent ethernet down
	Admin config change
	Tunnel src port removed
	Tunnel source module not online
	Possible port channel misconfiguration
	Isolation due to port security failure
	Isolation due to fabric bind failure
	Isolation due to no common vsans with peer on trunk
	Ficon vsan down
	Invalid attachment Ficon not configured on peer
	Port blocked due to Ficon

Field	Description
	Error disabled due to incompatible admin port rxbbcredit performance buffers
	Suspended due to too many invalid flogis
	Suspended due to port security
	Isolation due to ELP failure revision mismatch
	Isolation due to ELP failure class F param error
	Isolation due to ELP failure class N param error
	Isolation due to ELP failure invalid flow control code
	Isolation due to ELP failure invalid flow control param
	Isolation due to ELP failure invalid port name
	Isolation due to ELP failure invalid switch name
	Isolation due to ELP failure R_A_TOV or E_D_TOV mismatch
	Isolation due to ELP failure loopback detected
	Isolation due to ELP failure invalid transmit B2B credit
	Isolation due to ELP failure invalid payload size
	Error Disabled due to portchannel misconfiguration
	Link failure Port unusable
	Link failure loss of signal
	Link failure loss of sync
	Link failure NOS received
	Link failure OLS received
	Link failure renegotiation failed
	Link failure Link Reset failed nonempty recv queue
	Link failure Excessive credit loss indications
	Link failure receive queue overflow
	Error disabled due to excessive port interrupts
	Link failure Loop initialization failed nonempty recv queue
	Link failure Link reset failed queue not empty
	Link failure OPNy timeout while receive queue not empty
	Link failure OPNy returned while receive queue not empty
	Link failure Link reset failed queue not empty
	Link failure or notconnected
	Isolation due to FCSP failure
	SFP checksum error

Field	Description
	Suspended due to external Loopback diagnostics failure Invalid fabric binding exchange Isolation due to TOV Mismatch Error disabled due to ficon not enabled Error disabled due to no ficon portnumber for logical interface Ficon being enabled Port down because prohibit mask in place for E TE port Gracefully shutdown Not all VSANs UP on the trunk Isolation due to fabric binding peer switch WWN not found Isolation due to fabric binding peer domain mismatch Isolation due to fabric binding database mismatch Isolation due to fabric binding no response from peer Suspended due to dynamic vsan suspension Suspended due to dynamic vsan not found All tracked ports down Suspended as extended credit mode not allowed for loop ports Isolation due to portchannel misconfiguration Peer device does not support portchannels Isolation during port bringup Isolation due to domain not allowed Isolation due to virtual IVR domain overlap Out of service Authentication failed Unidirectional UDLD detected **Note** Unidirectional link detection (UDLD) is not supported by FXOS; ignore any references to UDLD. UDLD Tx Rx loop UDLD neighbor mismatch UDLD empty echo UDLD detected link failure in aggressive mode Port connector type error Error disabled due to reinit limit reached

Field	Description
	Duplicate port num in VSAN
	Internal RCF in progress
	Duplicate WWN
	Invalid other princ epp req received
	Isolated due to unknown reason
	Incomplete tunnel configuration
	Hardware programming failed
	No route to tunnel destination address
	Module removed
	MTU allocation failed
	All parameters have not been configured
	SFP is not inserted
	Transceiver is not inserted
	SFP is not Cisco certified
	Transceiver is not Cisco certified
	Bit error rate threshold exceeded
	Link failure link reset
	Link failure port initialization failed
	ELP failure, all zero peer WWN received
	Isolation due to preferred path
	FC redirect isolation
	Port activity license not available
	SDM isolation
	FCID allocation failed
	Externally disabled
	Authorization pending
	Hot standby in bundle
	Channel error-disabled
	Port capabilities not known
	Mismatch in source and transport VRF
	Forward referencing transport VRF
	two tunnel interface with same configuration is not allowed
	Too many link flaps in a short interval

Field	Description
	Primary vlan is down.
	VRF Unusable
	Internal handshake failure
	BPDUGuard triggered error disable
	Port is disabled
	error disabled due to security violation
	tunnel interface is down because mode is not configured
	tunnel interface is down because source is not configured
	tunnel interface is down because destination is not configured
	tunnel interface is down because could not resolved ip-address associated with tunnel source interface
	tunnel interface is down because could not resolved ip-address associated with tunnel destination
	tunnel interface is down because vrf configured to tunnel interface is down
	Interface is error disabled becasue of STP inconsistency on VPC peer-link
	Interface is error disabled becasue of STP set port state failure
	port channel is down because it was suspended by vpc
	vpc configuration is in progress
	vpc peer-link is down
	vpc down because failed to receive response from peer
	vpc down because compatibility check failed
	Not enough free entries in TCAM bank
	tunnel interface is down because tunnel source interface is down
	Error disabled due to IP address conflict
	Pinned fabric port is down
	Invalid fabric port
	FEX fabric sfp invalid
	SDP timeout/SFP Mismatch
	FEX identity mismatch
	FEX ID not configured on fabric port
	Error disabled due to IP QoS policy application failure
	Router mac allocation failed
	VLAN/BD does not exist
	VLAN/BD is down

Field	Description
	VLAN type is invalid DCX Multiple MSAP IDs recieved for the port DCX Recieved 100 PDUs without ACK IP QOS DCBXP compat check failed Suspended due to minlinks parent interface down Inactive - M1 port not allowed in FabricPath-mode VLAN The speed supported by the transceiver does not match the speed configured on the port Transceiver authentication failed on the port Failed to bring up vPC+ peer link Fabric Path switch ID not configured Failed to bring up vPC+ peer link port is not configured as a Fabric Path port The transceiver has failed ethernet compliance Speed-Group config does not match type of transceiver Suspended due to no LACP PDUs received from peer
Speed	**Interface speed:** `Auto` – auto-negotiated `10` – 10 Mbps `100` – 100 Mbps `Auto110` – auto-negotiated between 10 and 100 Mbps `1000` – 1 Gbps `10G` – 10 Gbps `a-10` – auto-negotiated, 16 Mbps `a-100` – auto-negotiated, 106 Mbps `a-1000` – auto-negotiated, 1006 Mbps `a-10G` – auto-negotiated, 10006 Mbps `40G` – 40000 Mbps `100G` – 100000 Mbps `a-40G` – auto-negotiated, 40006 Mbps `a-100G` – auto-negotiated, 100006 Mbps **Note** A `(D)` appended to a speed entry indicates a dedicated interface, while `(S)` indicates it is shared.
Port channel #	ID number of the port channel to which interface is assigned, if any.

Field	Description
Protocol	**Port channel protocol:** `none` – Link Aggregation Control Protocol (LCAP) is not enabled `lcap` – LCAP is enabled
VRF	Name of virtual routing and forwarding (VRF) instance to which port is assigned, if any.
IP Address	Port IP address
MTU	Port MTU (maximum transmission unit) size

Related Commands

Command	Description
show port	In connect fxos mode, shows port information.
show vlan	In connect fxos mode, shows VLAN information.

show inventory

To view information about the chassis and its installed modules, use the **show inventory** command in chassis mode.

show inventory [**detail** | **expand** | **fabric** | **fan** | **fi-iom** | **iom** | **psu** | **server** | **unspecified**]

Syntax Description

detail	(Optional) Use this keyword to display detailed information about the chassis itself.
expand	(Optional) Use this keyword to display expanded information for each component on the chassis.
fabric	(Optional) Use this keyword to display fabric transport information. The keyword **detail** is also available.
fan	(Optional) Displays information about each fan module on the chassis. The keyword **detail** is also available.
fi-iom	(Optional) Displays information about fabric-interconnect switch I/O modules. The keyword **detail** is also available.
iom	(Optional) Displays information about chassis input/output modules. The keyword **detail** is also available.
psu	(Optional) Displays information about installed power-supply units. The keyword **detail** is also available.
server	(Optional) Lists information for each server component. The keyword **detail** is also available.
unspecified	(Optional) Lists information for the chassis component. The keyword **detail** is also available.

Command Modes

scope chassis/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use this command without any arguments or keywords to display basic chassis information.

Example

This example shows how to view expanded chassis inventory information:

```
firepower# scope chassis
firepower /chassis # show inventory expand
Chassis 1:
    Servers:
        Server 1/1:
            Equipped Product Name: Cisco Firepower 9000 Series Security Module
            Equipped PID: FPR9K-SM-24
            Equipped VID: V01
            Equipped Serial (SN): FCH19057S0L
            Slot Status: Equipped
            Acknowledged Product Name: Cisco Firepower 9000 Series Security Module
            Acknowledged PID: FPR9K-SM-24
            Acknowledged VID: V01
            Acknowledged Serial (SN): FCH19057S0L
            Acknowledged Memory (MB): 262144
            Acknowledged Effective Memory (MB): 262144
            Acknowledged Cores: 24
            Acknowledged Adapters: 2

        Server 1/2:
            Equipped Product Name: Cisco Firepower 9000 Series Security Module
            Equipped PID: FPR9K-SM-24
            Equipped VID: V01
            Equipped Serial (SN): FCH19057RTY
            Slot Status: Equipped
            Acknowledged Product Name: Cisco Firepower 9000 Series Security Module
            Acknowledged PID: FPR9K-SM-24
            Acknowledged VID: V01
            Acknowledged Serial (SN): FCH19057RTY
            Acknowledged Memory (MB): 262144
            Acknowledged Effective Memory (MB): 262144
            Acknowledged Cores: 24
            Acknowledged Adapters: 2

        Server 1/3:
            Equipped Product Name:
            Equipped PID:
            Equipped VID:
            Equipped Serial (SN):
            Slot Status: Empty
            Acknowledged Product Name:
            Acknowledged PID:
            Acknowledged VID:
            Acknowledged Serial (SN):
            Acknowledged Memory (MB):
            Acknowledged Effective Memory (MB):
            Acknowledged Cores:
            Acknowledged Adapters:

    PSU 1:
        Presence: Equipped
        Product Name: Cisco Firepower 9000 Series  AC Power Supply
        PID: FPR9K-PS-AC
        VID: V00
        Vendor: Cisco Systems Inc
        Serial (SN): DTM190705G3
        HW Revision: 0

    PSU 2:
        Presence: Equipped
        Product Name: Cisco Firepower 9000 Series  AC Power Supply
        PID: FPR9K-PS-AC
        VID: V00
        Vendor: Cisco Systems Inc
```

```
        Serial (SN): DTM190705J8
        HW Revision: 0

    Fan Modules:
        Tray 1 Module 1:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200LD 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200LD 0

        Tray 1 Module 2:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200ML 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200ML 0

        Tray 1 Module 3:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200KZ 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200KZ 0

        Tray 1 Module 4:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200L8 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200L8 0

    Switch IOCard 1:
        Side: Left
        Fabric ID: A
        Product Name: Cisco FPR9K-SUP
        PID: FPR9K-SUP
        VID: V01
        Vendor: Cisco Systems, Inc.
        Serial (SN): JAD190800VU
        HW Revision: 0

Fabric Card 1:
    Description: Firepower 9300 Supervisor
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-SUP
    HW Revision: 0
    Serial (SN): JAD190800VU
    Perf: N/A
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A


Fabric Card 2:
    Description: Firepower 4x100G QSFP28 NM
    Number of Ports: 4
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X100G
    HW Revision: 0
```

```
    Serial (SN): JAD2151037Z
    Perf: N/A
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A


Fabric Card 3:
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DK
    Perf: N/A
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A


firepower /chassis #
```

Related Commands

Command	Description
show environment	Shows chassis hardware status information.

show inventory (connect fxos)

To view information about chassis inventory including the name, description, PID, and serial number of the supervisor and network modules, use the **show inventory** command in connect fxos mode.

show inventory

Syntax Description

This command has no arguments or keywords.

Command Modes

connect fxos

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use this command without any arguments or keywords to display chassis or module information.

Example

This example shows how to view chassis inventory or module information:

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show inventory
NAME: "Chassis", DESCR: "Cisco Firepower 9300 Security Appliance"
PID: FPR9K-SUP         , VID: V08 , SN: ABCD123456

NAME: "Module 1", DESCR: "Firepower 9300 Supervisor"
PID: FPR9K-SUP         , VID: V08 , SN: CBDA123456

NAME: "Module 2", DESCR: "Firepower 4x40G QSFP NM"
PID: FPR-NM-4X40G      , VID: V01 , SN: CBDA654321
```

show ip-block

To display a list of IPv4 address blocks currently defined for service access, use the **show ip-block** command.

show ip-block [[*ip_address prefix_length* { **https** | **snmp** | **ssh** }] | **detail**]

Syntax Description

ip_address prefix_length { **https** | **snmp** | **ssh** }	(Optional) To display a specific IPv4 address block, enter that address information: • The starting address for the IPv4 address block. • The prefix length; determines the number of addresses in the block. Value can be 0 to 32. • The service (HTTPS, SNMP, or SSH) to which the address block is assigned.
detail	(Optional) Appending the **detail** keyword displays the address, prefix and service for each IPv4 block as separate lines.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to list the currently permitted blocks of IPv4 addresses. Up to 25 different blocks can be configured for each service.

Example

This example shows how to display detailed IPv4 address block information:

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # show ip-block detail

    IP Address: 209.165.201.1
    Prefix Length: 24
    Protocol: https

Permitted IP Block:
    IP Address: 0.0.0.0
    Prefix Length: 0
    Protocol: snmp

    IP Address: 209.165.202.129
    Prefix Length: 24
    Protocol: ssh
FP9300-A /system/services #
```

Related Commands

Command	Description
create ip-block	Creates an IPv4 block.
delete ip-block	Deletes an existing IPv4 block.

show ip-pool

To display a list of IP pool available on the system, use the **show ip-pool** command.

show ip-pool [*detail* | *expand* | *name*]

Syntax Description

detail	(Optional) Displays IP pool information of a specific pool. The **expand** and **expand** keywords are available with this option.
expand	(Optional) Displays expanded information of IP pool. The **detail** keyword is available with this option.
name	Lists detailed IP pool information.

Command Modes

scope org

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope org.

Example

This example shows how to display IP pool information:

```
Firepower /fabric-interconnect # scope org
Firepower /org # show ip-pool
IP Pool:
    Name                 Size       Assigned   Management mode
    -------------------- ---------- ---------- ---------------
    ext-mgmt                      0          0 Internal
    iscsi-initiator-pool          0          0 Internal
    ssp-ippool-app-ccl          126          0 Internal
    ssp-ippool-inter-mgmt
                                117          0 Internal
```

Example

This example shows how to display detailed information of all the available IP pools:

```
Firepower /org # show ip-pool expand detail

IP Pool:
    Name: ext-mgmt
    Size: 0
    Assigned: 0
    IPv4 Size: 0
    IPv4 Assigned: 0
    IPv6 Size: 0
    IPv6 Assigned: 0
    Descr:
```

```
Assignment Order: Default
Management mode: Internal
Guid: 00000000-0000-0000-0000-000000000000
Net bios enabled or disabled: Not Active
DHCP enaled or disabled: Not Supported
Name: iscsi-initiator-pool
Size: 0
Assigned: 0
IPv4 Size: 0
IPv4 Assigned: 0
IPv6 Size: 0
IPv6 Assigned: 0
Descr:
Assignment Order: Default
Management mode: Internal
Guid: 00000000-0000-0000-0000-000000000000
Net bios enabled or disabled: Not Active
DHCP enaled or disabled: Not Supported
Name: ssp-ippool-app-ccl
Size: 126
Assigned: 0
IPv4 Size: 126
IPv4 Assigned: 0
IPv6 Size: 0
IPv6 Assigned: 0
Descr: SSP service profile IP Pool for app ccl vlan
Assignment Order: Default
Management mode: Internal
Guid: 00000000-0000-0000-0000-000000000000
Net bios enabled or disabled: Not Active
DHCP enaled or disabled: Not Supported
```

show ipsec-log

To view IPSec connection logs, use the **show ipsec-log** command.

show ipsec-log

Syntax Description

This command has no arguments or keywords.

Command Modes

IPSec mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use the **set log-level** command to change the amount of information displayed by these logs.

Example

This example shows how to display the contents of the IPSec log file:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # show ipsec-log
Feb 10 23:40:02 15[CFG] <test-connection|69>   using trusted ca certificate "C=US, ST=CA,
L=SJC, O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   reached self-signed root ca with a path
length of 0
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl correctly signed by "C=US, ST=CA, O=CA1,
 OU=ca1, CN=InterCA1, E=ca1@ca.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl is valid: until Mar 12 22:30:51 2017
Feb 10 23:40:02 15[CFG] <test-connection|69>   using cached crl
Feb 10 23:40:02 15[CFG] <test-connection|69> certificate status is good
Feb 10 23:40:02 15[CFG] <test-connection|69>   using trusted ca certificate "C=US, ST=CA,
L=SJC, O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69> checking certificate status of "C=US, ST=CA,
O=CA1, OU=ca1, CN=InterCA1, E=ca1@ca.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   fetching crl from
'file:///opt/certstore/ssp2-tp.crl' ...
Feb 10 23:40:02 15[CFG] <test-connection|69> issuer of fetched CRL 'C=US, ST=CA, O=CA1,
OU=ca1, CN=InterCA1, E=ca1@ca.net' does not match CRL issuer
'56:71:f1:d9:b1:62:fd:c3:2b:4d:cb:6b:01:85:ea:75:e5:0e:99:0d'
Feb 10 23:40:02 15[CFG] <test-connection|69>   fetching crl from
'http://192.168.0.81/interca_inuse.crl.pem' ...
Feb 10 23:40:02 15[CFG] <test-connection|69>   using trusted certificate "C=US, ST=CA,
L=SJC, O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl correctly signed by "C=US, ST=CA, L=SJC,
 O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl is valid: until Mar 12 22:30:49 2017
Feb 10 23:40:02 15[CFG] <test-connection|69> certificate status is good
Feb 10 23:40:02 15[CFG] <test-connection|69>   reached self-signed root ca with a path
length of 1
Feb 10 23:40:02 15[IKE] <test-connection|69> authentication of 'C=US, ST=CA, O=Cisco,
OU=STBU, CN=SSP, E=ssp@ssp.net' with RSA signature successful
Feb 10 23:40:02 15[IKE] <test-connection|69> IKE_SA test-connection[69] established between
 192.168.0.174[C=US, ST=CA, O=Cisco, OU=STBU, CN=SSP]
```

```
FP9300-A /security/ipsec #
```

Related Commands

Command	Description
set log-level	Sets the IPSec log verbosity.

show ipv6-block

To display a list of IPv6 address blocks currently defined for service access, use the **show ipv6-block** command.

show ipv6-block [[*ipv6_address prefix_length* { **https** | **snmp** | **ssh** }] | **detail**]

Syntax Description

ipv6_address prefix_length { **https** | **snmp** | **ssh** }	(Optional) To display a specific IPv6 address block, enter that address information: • The starting address for the IPv6 address block. • The prefix length; determines the number of addresses in the block. Value can be 0 to 128. • The service (HTTPS, SNMP, or SSH) to which the address block is assigned.
detail	(Optional) Appending the **detail** keyword displays the address, prefix and service for each IPv6 block as separate lines.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to list the currently permitted blocks of IPv6 addresses. Up to 25 different blocks can be configured for each service.

Example

This example shows how to display detailed IPv4 address block information:

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # show ip-block detail

    IP Address: 2001:DB8:1::1
    Prefix Length: 64
    Protocol: https

Permitted IP Block:
    IP Address: 0:0:0:0:0:0:0:0
    Prefix Length: 0
    Protocol: snmp

    IP Address: 2001:DB8:0:ABCD::1
    Prefix Length: 64
    Protocol: ssh
FP9300-A /system/services #
```

Related Commands

Command	Description
create ipv6-block	Creates an IPv6 block.
delete ipv6-block	Deletes an existing IPv6 block.

show ipv6-if

To view current IPv6 management-interface information, use the **show ipv6-if** command.

Syntax Description

detail	Lists detailed IPv6 management-interface information.
fsm status	Lists finite state machine (FSM) status information related to the IPv6 management interface.

Command Modes

IPv6 configuration (fabric-interconnect/ipv6-config) mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays only IPv6 management-interface information.

Example

This example shows how to display IPv6 management-interface information:

```
FP9300-A# scope fabric-interconnect
FP9300-A# scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address                       Prefix     IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998                         64         2001::1
FP9300-A /fabric-interconnect/ipv6-config #


FP9300-A# scope fabric-interconnect
FP9300-A# scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
    IPv6 Address                              Prefix     IPv6 Gateway
       AutoCfg-method  ReadyCfg-method IPv6 state      ND state
    ------------------------------------- ----------
---------------------------------------- --------------- --------------- ---------------
--------
    ::                                        64         2008::1
       Stablesec       Notset          Enable          Enable
```

Related Commands

Command	Description
scope fabric-interconnect	Enters fabric interconnect mode.
scope ipv6-config	Enters IPv6 configuration mode.

show keyring

To view the imported certificate information, use the **show keyring** command.

show keyring [**detail** | **name**]

Syntax Description

detail	Displays the imported certificates information.
name	(Optional) Displays content for the specified imported certificate.

Command Modes

scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

show keyring is a subcommand of the **show** command in scope security.

Example

This example shows how to display imported certificates and verifies the certificate status value:

```
Firepower# scope security
Firepower# show keyring
Name            Key pair type   RSA key modulus Elliptic Curve TrustpointCA
--------------- --------------- --------------- --------------- -------------
default         Rsa             Mod2048         Ec              invalid
```

This example shows how to display the contents of the imported certificates.

```
Firepower /security # show keyring detail
Keyring default:
    RSA key modulus: Mod2048
    Trustpoint CA:
    Certificate status: Self Signed Certificate
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6f:fe:83:56:a2:60:da:fd:66:f9:50:75:47:bd:48:da:86:dc:81:81
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = MOIO-2
        Validity
            Not Before: May 26 12:14:42 2012 GMT
            Not After : May 26 12:14:42 2014 GMT
        Subject: CN = MOIO-2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d0:78:39:a6:c3:b7:dd:f3:c8:8c:90:5e:6c:43:
                    9b:a0:d3:40:15:06:c9:cc:3b:d8:6c:f1:51:fc:5a:
                    09:2c:7c:eb:f7:74:25:aa:1d:94:5c:d7:6e:95:61:
                    6b:8d:d7:52:23:c8:6c:c7:86:ef:a9:cf:f4:41:65:
                    2a:7f:9d:f9:b5:d3:1e:15:91:6e:b5:3d:4a:a7:49:
                    d5:a0:cb:4e:8e:1a:e7:55:f3:aa:f9:f3:2a:e8:36:
```

```
                    b6:e8:a8:15:ad:54:b2:8a:f8:f3:b1:2f:ab:8f:df:
                    c8:28:a6:1d:08:df:25:bd:58:8c:e0:8e:8f:ce:db:
                    5a:68:68:ce:9a:37:37:66:a8:fa:8c:50:4f:54:0e:
                    e8:cf:10:a3:70:6a:f9:08:c5:45:5d:38:4f:70:2f:
                    7a:85:ca:37:e6:67:bf:63:77:c1:24:89:8f:d0:7f:
                    1d:a2:db:08:ad:33:33:53:ee:95:a9:2f:a3:d6:c1:
                    bf:d7:de:cd:ac:60:e6:db:2c:1f:20:81:14:c8:f5:
                    ce:3b:ea:aa:ed:c6:d9:c3:32:5f:f7:e7:36:ce:79:
                    31:19:18:43:42:62:4a:fa:f6:77:36:85:04:49:e2:
                    e7:40:0e:f6:9f:a9:a3:9c:c5:23:5e:c8:bc:50:fd:
                    f6:36:7f:e0:46:59:70:3d:82:84:45:a7:59:23:35:
                    80:bd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:MOIO-2, IP Address:10.0.0.6
    Signature Algorithm: sha256WithRSAEncryption
         cb:b6:f5:2a:96:4d:b9:a9:18:9f:00:fa:b6:e0:c0:0e:50:51:
         79:74:ca:21:25:e5:ae:e1:fe:03:dc:0b:9b:f7:c0:02:d2:72:
         e7:da:fd:f2:76:25:12:27:5f:bc:38:14:80:31:8c:e1:8b:5f:
         f8:7b:14:28:7a:be:2a:22:b8:b5:ea:90:1d:69:af:38:1b:ae:
         5e:c3:3c:95:f3:9b:32:0b:af:cb:2a:0b:5d:d7:57:77:25:df:
         26:ef:5b:ec:fb:09:6e:87:60:fb:3a:14:de:09:5e:13:f6:a8:
         10:70:50:e0:dd:cf:6d:78:4f:5e:27:d0:ad:92:db:65:fe:d7:
         81:cf:fb:93:d3:1f:21:e1:3f:20:50:62:5b:d3:7d:80:49:82:
         99:fc:74:9a:c3:d8:29:bf:2a:cb:a5:33:4d:dd:04:d2:fe:2c:
         1d:81:27:cc:56:70:9d:3e:f0:5c:ef:3a:86:ef:21:0a:6b:da:
         6c:7a:aa:1a:43:86:8c:f0:89:92:38:71:83:d9:8a:6c:47:22:
         03:4d:84:05:69:57:e9:a4:e5:2b:e2:3c:de:63:a9:10:3c:19:
         f2:2e:55:de:04:3a:6f:f1:e4:20:1b:2f:2f:38:b6:96:9f:7a:
         6b:18:09:f5:89:cd:8a:bc:95:59:b0:91:e9:61:46:7f:6e:6a:
         7c:0e:95:d7
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUb/6DVqJg2v1m+VB1R71I2obcgYEwDQYJKoZIhvcNAQEL
BQAwETEPMA0GA1UEAwwGTU9JTy0yMB4XDTEyMDUyNjEyMTQ0MloXDTE0MDUyNjEy
MTQ0MlowETEPMA0GA1UEAwwGTU9JTy0yMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0Hg5psO33fPIjJBebEOboNNAFQbJzDvYbPFR/FoJLHzr93Qlqh2U
XNdulWFrjddSI8hsx4bvqc/0QWUqf535tdMeFZFutT1Kp0nVoMtOjhrnVfOq+fMq
6Da26KgVrVSyivjzsS+rj9/IKKYdCN8lvViM4I6PzttaaGjOmjc3Zqj6jFBPVA7o
zxCjcGr5CMVFXThPcC96hco35me/Y3fBJImP0H8dotsIrTMzU+6VqS+j1sG/197N
rGDm2ywfIIEUyPXOO+qq7cbZwzJf9+c2znkxGRhDQmJK+vZ3NoUESeLnQA72n6mj
nMUjXsi8UP32Nn/gRllwPYKERadZIzWAvQIDAQABoxswGTAXBgNVHREEEDAOggZN
T0lPLTKHBAoAAAYwDQYJKoZIhvcNAQELBQADggEBAMu29SqWTbmpGJ8A+rbgwA5Q
UXl0yiEl5a7h/gPcC5v3wALScufa/fJ2JRInX7w4FIAxjOGLX/h7FCh6vioiuLXq
kB1przgbrl7DPJXzmzILr8sqC13XV3cl3ybvW+z7CW6HYPs6FN4JXhP2qBBwUODd
z214T14n0K2S22X+14HP+5PTHyHhPyBQYlvTfYBJgpn8dJrD2Cm/KsulM03dBNL+
LB2BJ8xWcJ0+8FzvOobvIQpr2mx6qhpDhozwiZI4cYPZimxHIgNNhAVpV+mk5Svi
PN5jqRA8GfIuVd4EOm/x5CAbLy84tpafemsYCfWJzYq8lVmwkelhRn9uanwOldc=
-----END CERTIFICATE-----

    Zeroized: No
```

show lacp (connect fxos)

To display Link Aggregation Control Protocol (LACP) information, use the **show lacp** command.

show lacp { **counters** | **interface** | **internal** | **issu-impact** | **neighbor** [**port-channel**] | **system-identifier** }

Syntax Description

counters [**interface** **port-channel** *number*]	Displays LACP traffic statistics. (Optional) You can specify a particular port-channel to view statistics for only that port-channel; valid port-channel numbers are 1 to 4096.
interface [**br-ethernet** *slot/chassis_num* | **ethernet** *slot/chassis_num*]	Displays LACP information for the Ethernet interfaces. (Optional) You can specify a break-out Ethernet interface, or an Ethernet interface, to view information about the specific interface.

internal { **debug buffer** | **event-history** | **info** | **mem-stats** }	Displays internal LCAP information and statistics, according to the provided keyword:
	• **debug buffer** – Shows LACP debug information.
	• **event-history** – Shows LACP event logs; one of the following event-type keywords is required:
	  • **errors** – Displays LCP error logs.
	  • **global** – Displays global event tranactions.
	  • **ifindex** *index_ID* – Displays LACP interface logs for the specified interface index; valid values are 0 to 2147483647.
	  • **interface** { **br-ethernet** *slot/chassis_num* | **ethernet** *slot/chassis_num* } – Displays LACP events for the specified Ethernet interface.
	  • **lock** – Displays LACP lock logs.
	  • **msgs** – Displays LACP event-message logs.
	• **info** – Shows general internal LACP information. The following optional keywords are available to specify specific types of information:
	  • **all** – Displays all internal LACP information.
	  • **global** – Displays global LACP information.
	  • **ifindex** *index_ID* – Displays LACP statistics for the specified interface index; valid values are 0 to 2147483647.
	  • **interface** { **br-ethernet** *slot/chassis_num* | **ethernet** *slot/chassis_num* } – Displays LACP information for the specified Ethernet interface.
	  • **log** – Displays LACP information logs.
	  • **pc-db interface port-channel** *number* – Displays virtual-port-channel database (2lvpc) status for the specified port-channel.
	  • **pss** – Displays global Persistent Storage Service (PSS) information.
	• **mem-stats** – Shows LACP memory allocation statistics.

issu-impact	The in-service software upgrade (ISSU) option does not apply to FXOS.
neighbor [**interface port-channel** *number*]	Displays information about LACP neighbors. (Optional) You can specify a particular port-channel to view information for only that port-channel; valid port-channel numbers are 1 to 4096.
port-channel [**interface port-channel** *number*]	Displays information about all port-channels. (Optional) You can specify a particular port-channel to view the information for only that port-channel; valid port-channel numbers are 1 to 4096.

system-identifier	Displays the LACP system identification. This is a combination of the port priority and the MAC address of the device.

Command Modes

connect fxos/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

Use this command to troubleshoot problems related to LACP in a network.

Note When you connect to the FXOS command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to the default prompt with (fxos) appended; see the following example.

Examples

This example shows how to display the LACP counters:

```
firepower# connect fxos
firepower(fxos)# show lacp counters                    LACPDUs         Marker      Marker
Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel1
Ethernet1/3        20552782218005  0      0        0      0        0

port-channel2
Ethernet1/6        671621 724750   0      0        0      0        0

port-channel48
Ethernet1/1        23974772587653  0      0        0      0        0

firepower(fxos)#
```

This example shows how to display the LACP information for a particular port-channel:

```
firepower# connect fxos
firepower(fxos)# show lacp port-channel interface port-channel 48
port-channel48
  System Mac=b0-aa-77-2f-f0-af
  Local System Identifier=0x8000,b0-aa-77-2f-f0-af
  Admin key=0x2f
  Operational key=0x2f
  Partner System Identifier=0x8000,78-ba-f9-e2-60-c0
  Operational key=0x30
  Max delay=0
  Aggregate or individual=1
  Member Port List=
firepower(fxos)#
```

Related Commands

Command	Description
clear lacp counters	Clears LACP counters.

show license

To display the usage of some or all license packages, use the **show license** command.

show license { **all** | **resvcode** | **status** | **summary** | **techsupport** | **udi** | **usage** }

Syntax Description

all	Displays the Smart Licensing status and usage information for all licenses.
resvcode	Displays generated reservation-code information.
status	Displays Smart Licensing status information.
summary	Displays Smart Licensing summary information.
techsupport	Displays a complete set of Smart Licensing information for transmission to Cisco TAC.
udi	Displays the FXOS universal device identifier (UDI).
usage	Displays current license usage.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You must purchase permanent licenses so they are available in Smart Software Manager. Not all accounts are approved for permanent license reservation.

Example

This example shows how to display current status and usage of all license packages:

```
FP9300-A# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Cisco SVS temp
  Virtual Account: Escalations
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Feb 10 18:55:08 2016 CST
  Last Renewal Attempt: SUCCEEDED on Jun 27 06:11:11 2017 CDT
  Next Renewal Attempt: Jul 28 03:02:49 2017 CDT
  Registration Expires: Jun 27 06:05:09 2018 CDT

License Authorization:
  Status: AUTHORIZED on Jul 05 18:19:38 2017 CDT
  Last Communication Attempt: SUCCESS on Jul 05 18:19:38 2017
```

```
 CDT
  Next Communication Attempt: Aug 08 14:50:41 2017 CDT

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
scope license	Enters license mode.

show load-stats

To display the list of load stats capabilities available on the system, use the**show load-stats** command.

show load-stats detail

Syntax Description

detail	Lists detailed load stats capabilities information.

Command Modes

scope system, scope capability

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope capability

Example

This example shows how to display load stats capabilities:

```
Firepower # scope system
Firepower /system # scope capability
Firepower /system/capability # show load-stats

Capability:
    Load Errors: 0
    Load Warnings: 4
    Providers Loaded: 128
    Provider Load Failures: 0
    Files Parsed: 17
    File Parse Failures: 0

Firepower /system/capability # show load-stats detail
Capability:
    Load Errors: 0
    Load Warnings: 4
    Providers Loaded: 126
    Provider Load Failures: 0
    Files Parsed: 17
    File Parse Failures: 0
```

show local-user

To display information about a specific user or all local users, use the**show local-user** command.

show local-user [**detail** | *user_name*]

Syntax Description

detail	(Optional) Displays detailed local user information.
user_name	(Optional) Displays information for the specified local user.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

In security mode, information for all local users is listed by default unless you enter a specific *user_name*.

In local user mode, you can use the **show** command to display information for the connected user.

Example

This example shows how to display detailed user information for a specific local user:

```
FP9300-A /security # show local-user test_user detail
Local User test_user:
    First Name: test
    Last Name: user
    Email: test_user@testuser.com
    Phone:
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
FP9300-A /security #
```

Related Commands

Command	Description
create local-user	Creates a new local user account.
delete local-user	Deletes an existing local user account.
enter local-user	Enters an existing local user account.

show local-user tech-support

To display the local user admin, use the**show local-user tech-support** command.

show local-user tech-support detail

Syntax Description

detail	Detailed information of local user tech support.

Command Modes

scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope security.

Example

This example shows how to display the local user admin information:

```
Firepower # scope security
Firepower /security # show local-user-tech support

Local User admin:
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
```

show logical-device

To display the information of logical devices available on the system, use the **show** command.

show [**expand**] [**detail**] [**fsm**]

Syntax Description

detail	Displays detailed network feature's information.
expand	(Optional) Displays expanded information for the current application instance. This keyword is also available with many of the other command options to display expanded information about the specified option.
fsm	It displays the information of fsm status.

Command Modes

Scope ssa

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope ssa:

Example

This example shows information for all available logical devices:

```
firepower # scope ssa
firepower /ssa # show logical-device

Logical Device:
    Name       Description Slot ID    Mode       Oper State                Template Name
    ---------- ----------- ---------- ---------- ------------------------ -------------
    ftd                    1          Standalone Incomplete Configuration ftd
```

This example shows detailed information of logical devices:

```
firepower /ssa # show logical-device detail
Logical Device:
    Name: ftd
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Incomplete Configuration
    Template Name: ftd
    Error Msg: Missing bootstrap keys MANAGEMENT_TYPE in ftd mgmt bootstrap
    Switch Configuration Status: Ok
    Current Task:
```

This example shows expand detailed information of logical devices:

```
firepower /ssa # show logical-device expand detail

Logical Device:
```

```
Name: ftd
Description:
Slot ID: 1
Mode: Standalone
Oper State: Incomplete Configuration
Template Name: ftd
Error Msg: Missing bootstrap keys MANAGEMENT_TYPE in ftd mgmt bootstrap
Switch Configuration Status: Ok
Current Task:

External-Port Link:
    Name: Ethernet11_ftd
    Port or Port Channel Name: Ethernet1/1
    Port Type: Mgmt
    App Name: ftd
    Description:
    Link Decorator:

    Name: Ethernet12_asa
    Port or Port Channel Name: Ethernet1/2
    Port Type: Data
```

show logical-device-template

To display the template of logical devices like ASA and FTD available on the system, use the**show logical-device-template** command.

show logical-device-template [**detail** | *expand* | *name*]

Syntax Description

detail	Displays the list of detailed logical device template information.
name	Displays logical device template information for a specific logical device. The expand and expand keywords are available with this option.
expand	(Optional) Displays expanded information of the logical device template.

Command Modes

scope ssa

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope ssa.

Example

This example shows how to display template information of all the logical device:

```
Firepower /fabric-interconnect # scope ssa
Firepower /ssa # show logical-device-template

Logical Device Template:
    Name       Version    Description
    ---------- ---------- -----------
    asa        1
    ftd        1
Firepower /ssa # show logical
```

Example

This example shows how to display the detailed template information of all the available logical devices in the system:

```
Firepower /ssa # show logical-device-template detail
 Logical Device Template:
    Name: asa
    Version: 1
    Description:
    Name: ftd
    Version: 1
    Description:
```

Example

This example shows how to display the detailed template information of all available logical device expand detail in system:

```
Firepower /ssa # show logical-device-template expand detail
   QP1 /ssa # show logical-device-template expand detail
Logical Device Template:
    Name: asa
    Version: 1
    Description:
    Template Applications:
        App Name: asa
        Application can be a decorator: No
    Name: ftd
    Version: 1
    Description:
    Template Applications:
        App Name: ftd
        Application can be a decorator: No
```

show mac-address

To view MAC address assignments for container instance interfaces, use the **show mac-address** command.

show mac-address [**detail** | *mac_address*]

Syntax Description

detail	Shows the MAC addresses in a non-table format.
mac_address	Shows information about a specific MAC address.

Command Modes

scope ssa/scope auto-macpool/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

This command only applies to container instance interfaces, and it does not show MAC addresses for native instances.

Example

The following is sample output from the **show mac-address** command.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
    Mac Address          Owner Profile            Owner Name
    -------------------- ------------------------ ----------
    A2:46:C4:00:00:1E    ftd13                    Port-channel14
    A2:46:C4:00:00:20    ftd14                    Port-channel15
    A2:46:C4:00:01:7B    ftd1                     Ethernet1/3
    A2:46:C4:00:01:7C    ftd12                    Port-channel11
    A2:46:C4:00:01:7D    ftd13                    Port-channel14
    A2:46:C4:00:01:7E    ftd14                    Port-channel15
    A2:46:C4:00:01:7F    ftd1                     Ethernet1/2
    A2:46:C4:00:01:80    ftd12                    Ethernet1/2
    A2:46:C4:00:01:81    ftd13                    Ethernet1/2
    A2:46:C4:00:01:82    ftd14                    Ethernet1/2
    A2:46:C4:00:01:83    ftd2                     Ethernet3/1/4
    A2:46:C4:00:01:84    ftd2                     Ethernet3/1/1
    A2:46:C4:00:01:85    ftd2                     Ethernet3/1/3
    A2:46:C4:00:01:86    ftd2                     Ethernet3/1/2
    A2:46:C4:00:01:87    ftd2                     Ethernet1/2
    A2:46:C4:00:01:88    ftd1                     Port-channel21
    A2:46:C4:00:01:89    ftd1                     Ethernet1/8
```

The following is sample output from the **show mac-address detail** command.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool #  show mac-address detail
```

```
Mac Address Item:
    Mac Address: A2:F0:B0:00:00:16
    Owner Profile: ftd1
    Owner Name: Ethernet1/5

    Mac Address: A2:F0:B0:00:00:17
    Owner Profile: ftd1
    Owner Name: Port-channel1

    Mac Address: A2:F0:B0:00:00:18
    Owner Profile: ftd1
    Owner Name: Ethernet1/4

    Mac Address: A2:F0:B0:00:00:19
    Owner Profile: ftd1
    Owner Name: Ethernet1/4
```

Related Commands

Command	Description
create port-channel	Creates an EtherChannel (port channel).
create subinterface	Adds a subinterface.
scope interface	Enters the physical interface object.
set port-type	Sets the interface type.

show member-port

To display status information for the port channel's member port(s), use the **show member-port** command.

show member-port [*slot_id port_id* | **detail** | **Ethernet***slot_id*/*port_id* | **expand** | **fsm status**]

Syntax Description

slot_id port_id	(Optional) You can view status information for a single member port by specifying its slot and port number. The **detail** and **expand** keywords are available with this option.
detail	(Optional) Use this keyword to view detailed information for all member ports. The **expand** keyword is available with this option.
Ethernet*slot_id*/*port_id*	(Optional) You can view status information for a single member port by specifying its Ethernet port label. The **detail** keyword is available with this option.
expand	(Optional) Use this keyword to view an expanded list of information for all member ports. The **detail** keyword is available with this option.
fsm status	(Optional) Use this keyword to view finite state machine (FSM) status information for the member ports. You can add a slot and port number (*slot_id port_id*) to limit the information display to the specified member port. The **expand** keyword is available with this option.

Command Modes

scope eth-uplink/scope fabric a/port-channel

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

You must create or enter a port-channel before you can use this command.

This is a subcommand of the **show** command in scope eth-uplink/scope fabric/port-channel mode.

Example

This example shows expanded member port information for a specific port-channel:

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter port-channel 3
firepower /eth-uplink/fabric/port-channel # show member-port expand

Member Port:
    Port Name       Membership         Oper State       State Reason
    --------------- ------------------ ---------------- ------------
    Ethernet1/1     Up                 Up
    Ethernet2/3     Suspended          Failed           Suspended
    Ethernet2/4     Down               Sfp Not Present  Unknown
```

```
firepower /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create member-port	Creates a port-channel member port.
create port-channel	Creates a new port-channel.

show mac-pool

To view the list of mac pool available on the system, use the **show mac-pool** command.

show mac-pool [**detail** | **expand** | **name**]

Syntax Description

detail	Lists detailed mac-pool information.
expand	(Optional) Displays mac-pool information for a specific pool. The **expand** and **expand** keywords are available with this option.
name	(Optional) Displays expanded information of mac pool. The **detail** keyword is available with this option.

Command Modes

scope org

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope org.

Example

This example shows how to display information of available mac pool:

```
Firepower /fabric-interconnect # scope org
Firepower /org # show mac-pool

MAC Pool:
    Name                 Size       Assigned
    -------------------- ---------- --------
    default                       0          0
    ssp-macpool-ccl             200          0
    ssp-macpool-inter-vnics
                                300         81
    ssp-macpool-mio-external-ports

                                 76          3
```

Example

This example shows how to display detailed information of the mac pool expand detail:

```
Firepower /org # show mac-pool expand detail

MAC Pool:
    Name: default
    Size: 0
    Assigned: 0
    Descr:
    Assignment Order: Default
```

```
Name: ssp-macpool-ccl
Size: 200
Assigned: 0
Descr: SSP service profile MAC Pool for ccl
Assignment Order: Default

Block of MAC Addresses:
    From: 00:15:C5:00:00:00
    To: 00:15:C5:00:00:C7

Pooled:
    Id: 00:15:C5:00:00:00
    Assigned: No
Assigned To Dn:
    Poolable Dn: mac/00:15:C5:00:00:00/pool-31022
    Prev Assigned To Dn:

    Id: 00:15:C5:00:00:01
    Assigned: No
    Assigned To Dn:
    Poolable Dn: mac/00:15:C5:00:00:01/pool-31025
    Prev Assigned To Dn:

    Id: 00:15:C5:00:00:02
    Assigned: No
    Assigned To Dn:
    Poolable Dn: mac/00:15:C5:00:00:02/pool-31028
    Prev Assigned To Dn:
```

show memory

To display the information of a memory module, use the **show memory** command.

show memory [*details*]

Syntax Description

detail	You can view detailed version information.

Command Modes

scope chassis/scope server

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope server 1 under scope chassis 1.

Example

This example shows how to display the available memory module information for a specific server:

```
firepower# scope chassis 1
firepower /chassis # scope server 1
firepower /chassis/server # show memory
DIMM Location   Presence         Overall Status           Type         Capacity (MB) Clock
---- ---------- ---------------- ----------------------- ------------ ------------- -----
   1 DIMM_A1    Equipped         Operable                 DDR4         16384         2666
   2 DIMM_A2    Missing          Removed                 Undisc       Unknown       Unknown

   3 DIMM_B1    Equipped         Operable                 DDR4         16384         2666
   4 DIMM_B2    Missing          Removed                 Undisc       Unknown       Unknown

   5 DIMM_C1    Equipped         Operable                 DDR4         16384         2666
   6 DIMM_C2    Missing          Removed                 Undisc       Unknown       Unknown

   7 DIMM_D1    Equipped         Operable                 DDR4         16384         2666
   8 DIMM_D2    Missing          Removed                 Undisc       Unknown       Unknown

   9 DIMM_E1    Equipped         Operable                 DDR4         16384         2666
  10 DIMM_E2    Missing          Removed                 Undisc       Unknown       Unknown

  11 DIMM_F1    Equipped         Operable                 DDR4         16384         2666
  12 DIMM_F2    Missing          Removed                 Undisc       Unknown       Unknown

  13 DIMM_G1    Equipped         Operable                 DDR4         16384         2666
  14 DIMM_G2    Missing          Removed                 Undisc       Unknown       Unknown

  15 DIMM_H1    Equipped         Operable                 DDR4         16384         2666
  16 DIMM_H2    Missing          Removed                 Undisc       Unknown       Unknown

  17 DIMM_J1    Equipped         Operable                 DDR4         16384         2666
  18 DIMM_J2    Missing          Removed                 Undisc       Unknown       Unknown

  19 DIMM_K1    Equipped         Operable                 DDR4         16384         2666
  20 DIMM_K2    Missing          Removed                 Undisc       Unknown       Unknown

  21 DIMM_L1    Equipped         Operable                 DDR4         16384         2666
```

```
  22 DIMM_L2    Missing          Removed                  Undisc       Unknown       Unknown

  23 DIMM_M1    Equipped         Operable                  DDR4         16384         2666
  24 DIMM_M2    Missing          Removed                  Undisc       Unknown       Unknown
firepower /chassis/server #
```

Example

This example shows how to display the detailed information of all the available memory modules on a specific server:

```
firepower# scope chassis 1
KSEC-FPR4115-3 /chassis # scope server 1
KSEC-FPR4115-3 /chassis/server # show memory detail
ID 1:
    Location: DIMM_A1
Presence: Equipped
    Overall Status: Operable
    Visibility: Yes
    Vendor: 0x2C00
    Vendor Part Number: 18ASF2G72PDZ-2G6E1
    Vendor Serial (SN): 43585030
    HW Revision: 0
    Form Factor: DIMM
    Type: DDR4
    Capacity (MB): 16384
    Clock: 2666
    Latency: 0.400000
    Width: 64
ID 2:
    Location: DIMM_A2
    Presence: Missing
    Overall Status: Removed
    Visibility: No
    Vendor:
    Vendor Part Number:
    Vendor Serial (SN):
    HW Revision: 0
    Form Factor: Undisc
    Type: Undisc
    Capacity (MB): Unknown
    Clock: Unknown
    Latency: Unknown
    Width: Unknown
ID 3:
    Location: DIMM_B1
    Presence: Equipped
    Overall Status: Operable
    Visibility: Yes
    Vendor: 0x2C00
    Vendor Part Number: 18ASF2G72PDZ-2G6E1
    Vendor Serial (SN): 4358534D
    HW Revision: 0
    Form Factor: DIMM
    Type: DDR4
    Capacity (MB): 16384
    Clock: 2666
    Latency: 0.400000
    Width: 64
          ……
          ……
```

```
                    .....
firepower /chassis/server #
```

show (management interface)

To view current management-interface information, use the **show** command in fabric interconnect mode.

show

Syntax Description

In fabric interconnect mode, this command has a number of keywords, but entering **show** without any modifiers displays the current fabric management-interface information.

Command Modes

scope fabric-interconnect/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays IPv4 and IPv6 management-interface information. Appending the **detail** keyword displays this interface information, along with some additional fabric-specific information.

Example

This example shows how to display management-interface information:

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # show

Fabric Interconnect:
ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
Prefix Operability
---- --------------- --------------- --------------- ---------------- ----------------
------ -----------
A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::               64
    Operable
firepower /fabric-interconnect #
```

Related Commands

Command	Description
scope fabric-interconnect	Enters fabric interconnect mode.
show ipv6-if	Shows the current device management IPv6 address.

show mgmt-port

To view status information for the device management port, use the **show mgmt-port** command.

```
(local-mgmt)# show mgmt-port
```

Syntax Description

This command has no arguments or keywords.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to view information about configuration and status of the device management interface.

Example

This example shows how to display management port information:

```
firepower # connect local-mgmt
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:174151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15273492 (14.5 MiB)  TX bytes:80246582 (76.5 MiB)

firepower(local-mgmt)#
```

Related Commands

Command	Description
show open-network-ports	Shows all open network ports.

show monitor

To view information and resources per security module, use the **show monitor** command.

show monitor [**detail** | **expand**]

Syntax Description

detail	Shows detailed resource usage for the module.
expand	Shows detailed information about the disk file system.

Command Modes

scope ssa/scope slot/

Command History

Release	Modification
2.4(1)	Additional fields were added to show CPU cores, memory, and disk usage.
1.1(1)	Command added.

Usage Guidelines

You can view information about the security module, including the OS version, memory, and uptime. This command is useful for container instances to track resource availability.

Example

The following is sample output from the **show monitor** command.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # show monitor

Monitor:
    OS Version Memory Total (MB) Memory Free (MB) Memory Used (MB) CPU Cores Available Blade
 Uptime Last Updated Timestamp
    ---------- ----------------- ---------------- ---------------- -------------------
------------ ----------------------
    2.4(1.101)             251844           222089            29755                  22 up
 19 days,  2:06

          2018-11-27T18:11:34.155
```

The following is sample output from the **show monitor detail** command.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # show monitor detail

Monitor:
    OS Version: 2.4(1.101)
    CPU Total Load 1 min Avg: 4.790000
    CPU Total Load 5 min Avg: 4.790000
    CPU Total Load 15 min Avg: 4.780000
    Memory Total (MB): 251844
    Memory Free (MB): 222084
```

```
    Memory Used (MB): 29760
    CPU Cores Total: 48
    CPU Cores Available: 22
    Memory App Total (MB): 226886
    Memory App Available (MB): 108514
    Data Disk Total (MB): 699651
    Data Disk Available (MB): 535811
    Secondary Disk Total (MB): 0
    Secondary Disk Available (MB): 0
    Disk File System Count: 5
    Blade Uptime: up 19 days,  1:55
    Last Updated Timestamp: 2018-11-27T18:00:04.560
```

The following is sample output from the **show monitor expand** command.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # show monitor expand
Monitor:
    OS Version: 2.4(1.101)
    Memory Total (MB): 251844
    Memory Free (MB): 222089
    Memory Used (MB): 29755
    CPU Cores Available: 22
    Blade Uptime: up 19 days,  2:06
    Last Updated Timestamp: 2018-11-27T18:11:34.155

    Disk File System:
        File System Mount Point Disk Total (MB) Disk Free (MB) Disk Used (MB)
        ----------- ----------- --------------- -------------- --------------
        /dev/sda1   /mnt/boot              7614           7451            163
        /dev/sda2   /opt/cisco/config
                                           1846           1707             43
        /dev/sda3   /opt/cisco/platform/logs
                                           4565           4278             49
        /dev/sda5   /var/data/cores
                                          46807          44368             54
        /dev/sda6   /opt/cisco/csp
                                         699651         653295          46356
```

Related Commands

Command	Description
show resource	Shows resource usage.

show nfs-mount-def

To display the information of mount def available on the system, use the **show nfs-mount-def** command.

show [**detail**]

Syntax Description

detail	List detailed information of mount def.

Command Modes

Scope monitoring

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope monitoring:

Example

This example shows information for all available mount def:

```
firepower # scope monitoring
firepower /monitoring # show nfs-mount-def
Mount Def:
    Name: external Backup Repository
    Admin State: Disabled
    Local dir: /boot flash/externalcfg
    policy owner: Local
    Purpose: Backup
    Remote dir:
    server:

    Name: external Image Repository
    Admin State: Disabled
    Local dir: /boot flash/external
    policy owner: Local
    Purpose: Image
    Remote dir:
    server:
```

This example shows detailed information of mount def:

```
firepower /monitoring # show nfs-mount-def detail
Mount Def:
    Admin State: Disabled
    Name: external Backup Repository
    Local dir: /boot flash/externalcfg
    policy owner: Local
    Purpose: Backup
    Remote dir:
    server:
    Current Task:

    Admin State: Disabled
    Name: external Image Repository
    Local dir: /boot flash/externalrep
    policy owner: Local
```

```
    Purpose: Image
    Remote dir:
    server:
    Current Task:
```

This example shows expand detailed information of mount def status:

```
firepower /monitoring # show nfs-mount-def fsm status

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:


    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:
```

show nm-fpga-version

To display a fpga version of network adapter, use the **show nm-fpga-version** command.

show nm-fpga-version [**detail**]

Syntax Description

detail	Detailed version information.

Command Modes

scope chassis 1

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

Subcommand of the **show** command in scope chassis 1.

Example

This example shows version information of the network module fpga version:

```
firepower/fabric-interconnect # scope chassis 1
firepower /chassis # show nm-fpga-version

Network Module Version:
    Network Module Slot: 2
    Running-Vers: 0.6.0
    Package-Vers: 0.0
    Activate-Status: Ready
firepower/chassis #
```

show ntp-overall-status

To display overall Network Time Protocol synchronization status for the system, use the **show ntp-overall-status** command.

show ntp-overall-status

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display current clock-synchronization status for chassis and any logical devices installed on the chassis:

```
FP9300-A# show ntp-overall-status

    NTP Overall Time-Sync Status: Time Synchronized
FP9300-A#
```

Related Commands

Command	Description
show clock	Displays the system clock.

show ntp server

To display the NTP server, use the **show ntp-server** command.

show ntp-server

Syntax Description

show ntp-server	This command displays the NTP server in FXOS.

Command Modes

scope system/scope services/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays the NTP server.

Example

This example shows how to display the NTP server:

```
firepower# scope system;scope services

firepower /system/services # show ntp-server

NTP server hostname:
    Name                                                                Time Sync Status
    ------------------------------------------------------------------- ----------------
    192.0.2.1                                                           Time Synchronized

firepower /system/services # show ntp-server expand detail

NTP server hostname:
    Name: 192.0.2.1
    Time Sync Status: Time Synchronized
    NTP SHA-1 key id: 0
    Error Msg:
```

show org

To display current organization information, use the **show org** command.

show org [**detail** | *name*]

Syntax Description

detail	(Optional) Displays details for all currently defined organizations.
name	(Optional) Displays information for the specified organization; maximum of 16 characters for this identifier.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display current organization information:

```
FP9300-A# show org

Organizations:
    Name: / (root)
FP9300-A#
```

Related Commands

Command	Description
scope org	Enters organization (/org) mode.

show package

To display downloaded package information, use the **show package** command.

show package [**detail** | **expand** | **type** *endpoint_type* | *name*]

Syntax Description

detail	(Optional) Displays detailed package information, including version number and time and date stamps.
expand	(Optional) Lists the images bundled in each package. The **detail** keyword is also available.
type *endpoint_type*	(Optional) Displays information for the specified package end-point type: • **b-series-bundle**—Lists information for any available B Series Bundles. • **c-series-bundle**—Lists information for any available C Series Bundles. • **catalog**—Lists information for the FXOS image catalog which is a list of images and packages. • **firmware-fpr4k-bundle**—Lists information for any available FP4100-series firmware bundles. • **firmware-fpr9k-bundle**—Lists information for any available FP9300 firmware bundles. • **image**—Lists available firmware images. • **full-bundle**—Lists information for any downloaded full bundles. • **infrastructure-bundle**—Lists information for any downloaded infrastructure bundles. • **platform-bundle**—Lists information for any downloaded platform bundles. • **unknown**—Lists information for any downloaded bundles of unknown type. The **detail** and **expand** keywords are also available with this option.
name	(Optional) Displays information for the specified package. The **detail**, **expand** and **type** keywords are also available with this option.

Command Modes

Firmware mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you do not include a *name*, the **show package** command lists information for every firmware package on the appliance.

Example

This example shows how to list detailed and expanded information for a specific firmware package:

```
FP9300-A# scope firmware
FP9300-A /firmware # show package fxos-k9.2.3.1.51.SPA detail
Firmware Package fxos-k9.2.3.1.51.SPA:
    Version: 2.3(1.51)
    Type: Platform Bundle
    State: Active
Time Stamp: 2017-10-25T16:53:30.000
Build Date: 2017-10-21 09:10:36 UTC
FP9300-A /firmware # show package fxos-k9.2.3.1.51.SPA expand
Package fxos-k9.2.3.1.51.SPA:
    Images:
        fxos-k9-bundle-infra.2.3.1.51.SPA
        fxos-k9-bundle-server.2.3.1.51.SPA
FP9300-A /firmware #
```

Related Commands

Command	Description
show server firmware	Shows server firmware versions and status information.
verify platform-pack	Verifies a specified FXOS platform image.

show password-profile

To display password profile information, use the **show password-profile** command.

show password-profile [**detail**]

Syntax Description

detail	(Optional) Displays detailed password profile information.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists information for the current security password profile.

Example

This example shows how to display detailed password profile information:

```
FP9300-A# scope security
FP9300-A /security # show password-profile detail

Password profile:
    Password history count: 5
    No password changes allowed (in Hours): 24
    Password change during interval: Enable
    Password change interval (in Hours): 48
    Password change count: 2
FP9300-A#
```

Related Commands

Command	Description
scope password-profile	Enters password profile mode.

show pki fsm status

To display the FSM information, use the **show pki fsm status** command.

show pki fsm status [**expand** | **detail**]

Syntax Description

expand	Displays the FSM status.
Detail	Displays detailed content of FSM status.

Command Modes

scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

By default, this is a subcommand of the **show** command in scope security.

Example

This example shows how to display the FSM status:

```
Firepower# scope security
Firepower # show pki fsm status expand detail
    FSM Status:
        Affected Object: sys/pki-ext/fsm
        Current FSM: updateEp
        Status: Success
        Completion Time: 2022-08-23T05:14:02.628
        Progress (%): 100
        Description:
        Remote Result: Not Applicable
        Error Code: None
        Error Description:

        FSM Stage:

            Order: 1
            Stage Name: updateEpSetKeyRingLocal
            Status: Success
            Try: 1
            Last Update Time: 2022-08-23T05:14:02.626
            Stage Description: keyring configuration on
primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal)

            Order: 2
            Stage Name: updateEpSetKeyRingPeer
            Status: Skip
            Try: 0
            Last Update Time: 2022-08-23T05:14:02.626
            Stage Description: keyring configuration on
secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingPeer)

            Order: 3
            Stage Name: updateEpPostSetKeyRingLocal
```

```
            Status: Skip
            Try: 0
            Last Update Time: 2022-08-23T05:14:02.627
            Stage Description: post processing after keyring configration on
primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingLocal)

            Order: 4
            Stage Name: updateEpPostSetKeyRingPeer
            Status: Skip
            Try: 0
            Last Update Time: 2022-08-23T05:14:02.628
condary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingPeer)g configuration on se--More—
```

show pmon state

To view the status of the processes in local mangement mode, use **show pmon state** command.

show pmon state

Syntax Description

show pmon state	Displays the status of the processes in local management mode.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists the status of processes in local management mode.

Example

This example shows how to display the status of processes information in local management mode:

```
firepower#
firepower# connect local-mgmt
...
firepower(local-mgmt)#(local-mgmt)# show pmon state

SERVICE NAME             STATE     RETRY(MAX)    EXITCODE    SIGNAL    CORE
------------             -----     ----------    --------    ------    ----
svc_sam_controller     running           0(4)           0         0      no
smConLogger            running           0(4)           0         0      no
svc_sam_dme            running           0(4)           0         0      no
svc_sam_dcosAG         running           0(4)           0         0      no
svc_sam_bladeAG        running           0(4)           0         0      no
svc_sam_portAG         running           0(4)           0         0      no
svc_sam_statsAG        running           0(4)           0         0      no
svc_sam_hostagentAG    running           0(4)           0         0      no
svc_sam_nicAG          running           0(4)           0         0      no
svc_sam_licenseAG      running           0(4)           0         0      no
svc_sam_extvmmAG       running           0(4)           0         0      no
httpd.sh               running           0(4)           0         0      no
...
```

show post

To display any errors that occurred during the most-recent BIOS power-on self-test (POST), use the **show post** command.

show post [*id* | **detail** | **expand** | **no-errors**]

Syntax Description

id	(Optional) Show POST information for a specific server; valid values are 0 to 42949667295.
detail	(Optional) Show additional POST details.
expand	(Optional) Show all POST information.
no-errors	(Optional) Show POST information without errors.

Command Modes

Any command mode; most relevant in server (/chassis/server) mode.

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command in server mode.

Example

This example shows how to display POST information:

```
FP9300-A# scope server 1/1
FP9300-A /chassis/server # show post

POST:
    Global ID Code     Severity  Affected Object        Description
    --------- -------- --------- ---------------------- ------------
    608       Post 608 Info      sys/chassis-1/blade-1  Invalid DIMM Configuration
```

Related Commands

Command	Description
show server bios	Shows server BIOS firmware information.

show pre-login-banner

To display the pre-login banner, use the **show pre-login-banner** command.

show pre-login-banner

Command Modes

scope security

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays the pre-login banner information.

Example

This example displays the pre-login banner information:

```
firepower# scope security
firepower /security # scope banner
firepower /security/banner # show pre-login-banner

Pre login banner:
    Message
    -------
    TEST
```

show provider-load-stats

To display the information of provider capabilities available on the system, use the **show provider-load-stats** command.

show provider-load-stats

Command Modes

scope system, scope capability

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope capability.

Example

This example shows how to display the provider capabilities information:

```
Firepower # scope system
Firepower/system # scope capability
Firepower /system/capability # show provider-load-stats

Provider: capabilities/bundle-type-cap
    Vendor:
    Model:
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 8
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-CHORLEYWOOD-revision
-0
    Vendor: Cisco Systems Inc
    Model: CHORLEYWOOD
    Load Errors: 0
    Load Warnings: 1
    Elements Loaded: 5
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-F9K-C9300-revision-0
    Vendor: Cisco Systems Inc
    Model: F9K-C9300
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 5
    Element Load Failures: 0

    TEST
```

This example shows how to display the detailed information of provider capabilities:

```
Firepower /system/capability # show provider-load-stats detail

Provider: capabilities/bundle-type-cap
    Vendor:
    Model:
    Load Errors: 0
```

```
    Load Warnings: 0
    Elements Loaded: 8
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-CHORLEYWOOD-revision
-0
    Vendor: Cisco Systems Inc
    Model: CHORLEYWOOD
    Load Errors: 0
    Load Warnings: 1
    Elements Loaded: 5
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-F9K-C9300-revision-0
    Vendor: Cisco Systems Inc
    Model: F9K-C9300
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 5
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-FPR-4110-K9-revision
-0
    Vendor: Cisco Systems Inc
    Model: FPR-4110-K9
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 5
    Element Load Failures: 0
```

show port-channel (connect fxos)

To display information about configured port channels, use the **show port-channel** command.

show port-channel { **capacity** | **compatibility-parameters** | **database** | **internal** | **load-balance** | **summary** | **traffic** | **usage** }

Syntax Description

capacity	Shows device port-channel capacity information, including total available and total in use.
compatibility-parameters	Lists port-channel interface compatibility requirements and status.
database [**interface port-channel** *number*]	Lists port-channel configuration and status information, including first operational port and age of the port-channel. (Optional) You can specify a particular port-channel to view the information for only that port-channel; valid port-channel numbers are 1 to 4096. You can specify a subinterface by appending a dot and the subinterface number (**.** *subinterface_num*) after the port-channel number. You also can specify a range of port-channels or multiple ranges to view: • To specify a single range, enter *start_num* **-** *end_num* • To specify a multiple ranges, enter *start_num* **-** *end_num* **,** *start_num* **-** *end_num* **,** and so on
internal { **event-history** | **info** | **max-channels** | **mem-stat** | **sdb** }	Show port-channel information for various internal statistics, using one of the following keywords: • **event-history** – You can display logs for a variety of port-channel event types. • **info** – You can display all global internal port-channel information, or interface-specific port-channel information. • **max-channels** – Displays the maximum number of port-channels allowed on this device. • **mem-stats** – Show private memory allocation statistics. The optional keyword **detail** is available to display detailed statistics. • **sdb** – Dumps port-channel internal status information. Most options have additional options and keywords; use the **show port-channel internal** *keyword* **?** command to view the options.
load-balance	Configure port-channel load balance.

summary [**interface port-channel** *number*]	Show port-channel summary. (Optional) You can specify a particular port-channel to view the information for only that port-channel; valid port-channel numbers are 1 to 4096. You can specify a subinterface by appending a dot and the subinterface number (**.** *subinterface_num*) after the port-channel number.
traffic [**interface port-channel** *number*]	Show port-channel traffic statistics. (Optional) You can specify a particular port-channel to view the information for only that port-channel; valid port-channel numbers are 1 to 4096. You can specify a subinterface by appending a dot and the subinterface number (**.** *subinterface_num*) after the port-channel number.
usage	Lists current used and unused port-channel ID numbers.

Command Modes

connect fxos/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

This command is a subcommand of the **show** command in the **connect fxos** shell.

Note When you connect to the FXOS command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to the default prompt with (fxos) appended; see the following examples.

Examples

This example shows port-channel summary information:

```
firepower # connect fxos
firepower(fxos)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth1/3(P)
2     Po2(SU)     Eth      LACP      Eth1/6(P)
48    Po48(SU)    Eth      LACP      Eth1/1(P)
firepower(fxos)#
```

This example shows port-channel traffic information:

```
firepower # connect fxos
firepower(fxos)# show port-channel traffic
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
     1    Eth1/3    0.0%    0.0% 100.00% 100.00%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
     2    Eth1/6    0.0%    0.0% 100.00% 100.00%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
    48    Eth1/1    0.0%    0.0% 100.00% 100.00%    0.0% 100.00%
firepower(fxos)#
```

Related Commands

Command	Description
enter member-port	Enters an existing member port, or creates it if it doens't exist.
enter port-channel	Enters an existing port-channel, or creates it if it doens't exist.

show port-channel (scope fabric)

To display a list of current port-channels with status information, use the **show port-channel** command.

show port-channel [**detail** | **expand** | *port_channel_num*]

Syntax Description

detail	List detailed port-channel information. The **expand** keyword is available with this option.
expand	List expanded port-channel information. The **detail** keyword is available with this option.
port_channel_num	Show status information for only the specified port-channel. The **detail** and **expand** keywords are available with this option.

Command Modes

scope eth-uplink/scope fabric/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope eth-uplink/scope fabric mode.

If you do not specify a port-channel number, information for all port-channels is listed.

Example

This example shows detailed information for a specific port-channel:

```
firepower /eth-uplink/fabric # show port-channel 48 detail

Port Channel:
    Port Channel Id: 48
    Name: Port-channel48
    Port Type: Cluster
    Description:
    Admin State: Enabled
    Oper State: Up
    Port Channel Mode: Active
    Port Channel Mode State: Enabled
    Auto negotiation: No
    Speed: 1 Gbps
    Duplex: Full Duplex
    Oper Speed: 1 Gbps
    Band Width (Gbps): 1
    State Reason:
    flow control policy: default
    LACP policy name: default
    Oper Lacp Policy Name: org-root/lacp-default
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
firepower /eth-uplink/fabric #
```

Related Commands

Command	Description
create port-channel	Creates a new port-channel.
scope port-channel	Scopes into an existing port-channel where you can configure and manage the port-channel.

show power-control-policy

To display the list of power policies available on the system, use the **show power-control-policy** command.

show power-control-policy [**detail** | **expand**]

Syntax Description

detail	Lists detailed power control policies information.
expand	(Optional) Displays expanded information for the current application instance.

Command Modes

scope org

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope org.

Example

This example shows information of all the system power policies:

```
QP1 # scope org
QPD /org # show power-control-policy

Power Policy:
    Name
    ----
    default
    ssp-default

QP1 /org # show power-control-policy detail

Power Policy:
    Name: default
    Admin Priority: 5
    Oper Priority: 5
    Description:
    Policy Owner: Local

    Name: ssp-default
    Admin Priority: No Cap
    Oper Priority: No Cap
    Description: ssp default power policy
    Policy Owner: Local

QP1 /org # show power-control-policy detail expand

Power Policy:
    Name: default
    Admin Priority: 5
    Oper Priority: 5
    Description:
    Policy Owner: Local
```

```
Name: ssp-default
Admin Priority: No Cap
Oper Priority: No Cap
Description: ssp default power policy
Policy Owner: Local
```

show psu

To view information about the installed power supply units, use the **show psu** command in chassis mode.

show psu [*unit_id* | **detail** | **expand**]

Syntax Description

unit_id	(Optional) Enter a power-supply unit number to list information for that unit.
detail	(Optional) Use this keyword to list detailed information about each installed power supply unit.
expand	(Optional) Use this keyword to display expanded power-supply information.

Command Modes

scope chassis/

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

You can use this command without any arguments or keywords to display basic power-supply unit information.

Example

This example shows how to view detailed power-supply unit information:

```
firepower# scope chassis
firepower /chassis # show psu detail

PSU:
    PSU: 1
    Overall Status: N/A
    Operability: N/A
    Threshold Status: N/A
    Power State: Off
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: N/A
    Product Name: Cisco Firepower 9000 Series  AC Power Supply
    PID: FPR9K-PS-AC
    VID: V00
    Part Number: 341-0723-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190705G3
    HW Revision: 0
    Firmware Version: N/A
    Type: DV
    Wattage (W): 0
    Input Source: Unknown

    PSU: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
```

```
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Cisco Firepower 9000 Series  AC Power Supply
    PID: FPR9K-PS-AC
    VID: V00
    Part Number: 341-0723-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190705J8
    HW Revision: 0
    Firmware Version: N/A
    Type: DV
    Wattage (W): 2500
    Input Source: 210AC 50 380DC

firepower /chassis #
```

Related Commands

Command	Description
show inventory	Shows information about the chassis and its installed modules.

show psu-policy

To display the contents of psu policies available on the system, use the **show psu-policy** command.

show psu-policy [**detail**]

Syntax Description

detail	Lists detailed psu policies information.

Command Modes

scope org

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope org.

Example

This example shows how to view psu policies unit information:

```
firepower# scope org
firepower /chassis # show psu-policy

PSU Policy:
    Redundancy Description
    ---------- -----------
    NonRedund



QP1 /org # show psu-policy detail

PSU Policy:
    Redundancy: NonRedund
    Description:
```

show registry-repository

To display service registry information, use the **show registry-repository** command.

show registry-repository

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to view service registry information:

```
FP9300-A# show registry-repository

Service Registry:

    Name:
    ID: 1000
    IP: 0.0.0.0
    Type: Service Reg
    Version:
    Capability: Unspecified
FP9300-A#
```

Related Commands

Command	Description
show service-profile	Shows service profile information.

show remote-user

To display the remote user details, use the **show remote-user** command.

show remote-user

Command Modes

scope security

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays the remote user information.

Example

This example displays the remote user information:

```
firepower# scope security
firepower /ssa # show remote-user
User Name
---------
test1

firepower /security # show remote-user test1 detail
Remote User test1:
    Description:
    User Roles:
        Name: read-only
firepower /security # show remote-user detail
Remote User test1:
    Description:
    User Roles:
        Name: read-only
```

show resource

To view resource allocation for the application instance, use the **show resource** command.

show resource [**detail**]

Syntax Description

detail	Shows resource allocation in a text format instead of a table format.

Command Modes

scope ssa/scope slot/create app-instance/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

To view available resources, enter **show monitor detail**.

Example

The following is sample output from the **show resource** command.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # scope app-instance ftd LD1
firepower /ssa/slot/app-instance # show resource

Resource:
    Allocated Core NR Allocated RAM (MB) Allocated Data Disk (MB) Allocated Binary Disk
(MB)
    ----------------- ------------------ ------------------------ --------------------------

                    6              29593                    40960
3907
```

The following is sample output from the **show resource detail** command.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # scope app-instance ftd LD1
firepower /ssa/slot/app-instance # show resource detail

Resource:
    Allocated Core NR: 6
    Allocated RAM (MB): 29593
    Allocated Data Disk (MB): 40960
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0
```

Related Commands

Command	Description
show monitor detail	Shows resource usage.

Command	Description
show resource-profile	Shows resource profile information.
show resource-profile user-defined	Views resource profile assignments.

show resource-profile

To show vDP resource profiles and resource profiles for use with container instances, use the **show resource-profile** command.

show resource-profile [**system** [*name*] | **user-defined** [*name*] | **vdp** [*version* [*name*]]] [**detail**]

Syntax Description

name	Specifies the name of the profile.
system	Shows only system-defined resource profiles.
user-defined	Shows user-defined container instance profiles profiles, including the default resource profile.
vdp	Shows system-defined vDP profiles.
version	Shows vDP for a particular version.
detail	Shows details about the resource profiles.

Command Modes

scope ssa/

Command History

Release	Modification
2.4(1)	Added the **user-defined** keyword.
1.1(3)	Command added.

Usage Guidelines

Specify the resource profile to use with an application instance using the **set resource-profile-name** command. You can add resource profiles for container instances using the **create resource-profile** command. vDP resource profiles are created automatically by the system. The chassis includes a default container instance resource profile called "Default-Small," which includes the minimum number of cores. You can change the definition of this profile, and even delete it if it is not in use. Note that this profile is created when the chassis reloads and no other profile exists on the system.

Example

The following is sample output from the **show resource-profile** command:

```
firepower# scope ssa
firepower /ssa # show resource-profile
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
bronze              N/A        N/A          No         all
 6              0 No              User Defined low end device
DEFAULT-4110-RESOURCE
                    vdp         8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes              System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
```

```
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
gold               N/A        N/A          No         all
14               0 No              User Defined  highest
silver             N/A        N/A          No         all
 8               0 No              User Defined  mid-level
Default-Small      N/A        N/A          Yes        all
 6             N/A No              User Defined
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
 2           8192 No              System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
 4          16384 No              System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
                                                    8          32768 No              System
firepower /ssa #
```

The following is sample output from the **show resource-profile user-defined** command:

```
firepower# scope ssa
firepower /ssa # show resource-profile user-defined
Profile Name       Is In Use  CPU Logical Core Count Description
------------------ ---------- ---------------------- -----------
bronze               No               6              low end device
gold                 No               14             highest
silver               No               10             mid-level
firepower /ssa #
```

Related Commands

Command	Description
create resource-profile	Adds a container instance resource profile.
set cpu-count	Sets the number of CPUs for the resource profile.
set resource-profile-name	Assigned the resource profile to the application instance.
show monitor detail	Shows resource usage for the security module/engine slot.
show resource detail	Shows resource allocation for the application instance.

show role

To display the list of the roles and its privileges, use the **show role** command.

show role [**detail** | **name**]

Syntax Description

detail	Display the list of the roles.
name	(Optional) Displays content for the specified role.

Command Modes

scope security

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

By default, this is a subcommand of the **show** command in scope security.

Example

This example shows how to display imported certificates and how to verify the certificate status value:

```
firepower# scope security
firepower /ssa # show roleRole:
    Role Name  Priv
    ---------- ----
    aaa        aaa
    admin      admin
    operations fault, operations
    read-only read-only
```

This example shows how to display the contents of the roles in a system:

```
firepower /security # show role detail
Role:
    Role Name: aaa
    Priv: aaa

    Role Name: admin
    Priv: admin

    Role Name: operations
    Priv: fault, operations

    Role Name: read-only
    Priv: read-only
```

This example shows how to display the contents of the selected role:

```
firepower /security # show role aaa

Role:
    Role Name Priv
    ---------- ----
    aaa        aaa
```

show (scope fabric)

To view information on a port channel, use the **show** command.

show

Command Modes

scope eth-uplink/scope fabric a/

Command History

Release	Modification
2.0.1	Command added.

Usage Guidelines

You must create port channels before you use this command.

Example

This example shows how to view detailed information on all port channels:

```
firepower-9300# scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel 3
firepower-9300 /eth-uplink/fabric/port-channel* # show
  Port Channel:
Port Channel Id Name Port Type Admin
State Oper State State Reason
--------------- ---------------- ------------------ -----
------ ---------------- ------------
10 Port-channel10 Data Enabled Failed No operational members


firepower-9300 /eth-uplink/fabric/port-channel #
```

Related Commands

Command	Description
create port-channel	Creates the port-channel.
scope port-channel	Displays individual port-channel and port information.

show schedule infra-fw

To view a list of schedule infrastructure firmware, use the **show schedule infra-fw** command.

show schedule infra-fw [**detail**]

Syntax Description

detail	Displays detailed schedule infrastructure firmware information.

Command Modes

scope system

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system.

Example

This example shows how to display all the system show schedule infrastructure firmware information:

```
Firepower /fabric-interconnect # scope system
Firepower /system # show schedule infra-fw
Schedule:
    Name
    ----
    infra-fw
```

Example

This example shows how to display detailed information of all the available system show schedule infrastructure firmware:

```
Firepower # show schedule infra-fw detail
Schedule:
    Name: infra-fw
    Description: Auto created by the system for Infrastructure upgrade
```

Example

This example shows how to display detailed information of all the scheduled infrastructure firmware:

```
Firepower /system # show schedule infra-fw expand detail
Schedule:
    Name: infra-fw
    Description: Auto created by the system for Infrastructure upgrade

    One-Time Occurrence:
        Name: infra-fw
        Start Date: 2012-07-05T23:27:33.148
        Max Duration (dd hh mm ss): None
        Max Concur Tasks: Unlimited
        Max Tasks: Unlimited
```

```
Min Interval (dd hh mm ss): None
Executed Tasks: 19
```

show security

To display password-related and FSM status-related security information, use the**show security** command.

show security [**detail** | **fsm**]

Syntax Description

detail	(Optional) Displays detailed password-related security information.
fsm status	(Optional) Displays finite state machine status information. The **status** keyword is required.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display expanded information for security mode:

```
FP9300-A# show security detail

security mode:
    Password Strength Check: No
    Minimum Password Length: 8
    Current Task:
FP9300-A#
```

Related Commands

Command	Description
scope security	Enters security mode.

show sel

To display the contents of the system event log (SEL) for a server, use the **show sel** command.

show sel *server_id*

Syntax Description

server_id	The server identifier, expressed as chassis-number/server-number (rack ID is not a valid option).

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display the contents of the SEL for server 1 in chassis 1:

```
FP9300-A# show sel 1/1
 show sel 1/1
1 | 12/16/2015 23:09:55 | CIMC | Event Logging Disabled DDR4_
P2_H2_ECC #0x99 | Log Area Reset/Cleared |  | Asserted
2 | 12/16/2015 23:09:56 | CIMC | Processor P2_THERMTRIP_N #0x
7a | Limit Not Exceeded | Asserted
3 | 12/16/2015 23:09:57 | CIMC | Processor P1_THERMTRIP_N #0x
79 | Limit Not Exceeded | Asserted
4 | 12/16/2015 23:10:00 | CIMC | Platform alert LED_SYS_ACT #
0xa4 | LED is on | Asserted
5 | 12/16/2015 23:10:00 | CIMC | Platform alert LED_SYS_ACT #
0xa4 | LED color is green | Asserted
6 | 12/16/2015 23:10:01 | CIMC | Processor DDR4_P2_H3_TMP #0x
73 | Limit Not Exceeded | Asserted
7 | 12/16/2015 23:10:01 | CIMC | Platform alert LED_LOM_FAULT
 #0xa3 | LED is off | Asserted
8 | 12/16/2015 23:10:01 | CIMC | Platform alert LED_LOM_FAULT
 #0xa3 | LED color is blue | Asserted
9 | 12/16/2015 23:10:03 | CIMC | Processor DDR4_P2_H2_TMP #0x
72 | Limit Not Exceeded | Asserted
--More--

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
scope server	Enters server mode.

show server actual-boot-order

To display the server boot order actually used by the BIOS when the server last booted, use the **show server actual-boot-order** command.

show server actual-boot-order [*server_id* | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays the actual boot order for a specific server, expressed as chassis-number/server-number (rack ID is not a valid option).
uuid *dynamic_uuid*	(Optional) Displays the actual boot order for a server specified using its dynamic universally unique identifier (UUID); specifed in the form NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays actual boot order information for all servers.

Example

This example shows how to display the actual boot order of all servers:

```
firepower# show server actual-boot-order
Server 1/1:
    Last Update: 2017-07-19T17:43:14.982
    LocalStorageAny
        (1) Not found. Please verify presence of device and p
resence of UEFI loader on device

Server 1/2:
    Last Update: 2017-07-19T17:43:14.980
    LocalStorageAny
        (1) Not found. Please verify presence of device and p
resence of UEFI loader on device

firepower#
```

Related Commands

Command	Description
show server boot-order	Shows server boot order.

show server adapter

To display information about network adapters in a server, use the **show server adapter** command.

show server adapter [*server_id* | **detail** | **identity** | **inventory** | **status** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays information about network adapters in a specific server, expressed as chassis-number/server-number (rack ID is not a valid option). The keyword **detail** is available with this option.
detail	(Optional) Displays detailed information in list form.
identity	(Optional) Displays complete identity information for each available adapter. The keywords **uuid** and *server_id* are available with this option.
inventory	(Optional) Lists installed network adapters. The keywords **detail** , **uuid** and *server_id* are available with this option.
status	(Optional) Displays overall status of installed network adapters. The keywords **detail** , **uuid** and *server_id* are available with this option.
uuid *dynamic_uuid*	(Optional) Displays information about network adapters in a particular server, specified using its dynamic universally unique identifier (UUID); entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`. The keyword **detail** is available with this option.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this commands lists the adapters available on each server. This is the same information displayed with the **inventory** keyword.

Example

This example shows how to display identity information about the installed network adapters:

```
firepower# show server adapter identity
Server 1/1:
    Burned-In UUID: 84928111-2710-4e7c-b664-91bce5b5dfbd
    Dynamic UUID: 84928111-2710-4e7c-b664-91bce5b5dfbd
    Adapter 1:
        Product Name: Cisco Firepower 9000 series MLOM Adapter
        PID: FPR-C9300-MP
        VID: V01
        Vendor: Cisco Systems Inc
        Serial: JAD190702J1
        Revision: 0

        Eth Interface:
```

```
        Adapter Interface Dynamic MAC Address
        ------- --------- ------------------
              1         1 00:15:A5:01:01:00
              1         2 00:15:A5:00:00:8E
              1         3 B0:AA:77:2F:5A:4C
              1         4 B0:AA:77:2F:5A:7C
              1         5 B0:AA:77:2F:5A:6C
              1         6 00:15:A5:00:00:CF
              1         7 00:15:A5:00:00:DF
              1         8 00:15:A5:00:01:0F
              1         9 00:15:A5:00:00:BF
              1        10 00:15:A5:00:00:6E
              1        11 00:15:A5:00:01:0C
              1        12 00:15:A5:00:00:EF
              1        13 00:15:A5:00:01:1F
              1        14 00:15:A5:00:00:1F
              1        15 00:15:A5:00:00:3F

        Ext Interface:

        Adapter Interface Mac
        ------- --------- ---
              1         1 BA:DB:AD:BA:D6:08
              1         5 BA:DB:AD:BA:D6:09

    Adapter 2:
        Product Name: Cisco Firepower 9000 series MEZZ Adapter

    <--- remaining lines removed for brevity --->

firepower#
```

Related Commands

Command	Description
scope adapter	Enters adapter mode.

show server assoc

To view the service profile associated with each server, use the **show server assoc** command.

show server assoc [*server_id* | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays information for a particular server, specified by chassis-number/server-number (rack ID is not a valid option).
uuid *dynamic_uuid*	(Optional) Displays information for a particular server, specified using its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this commands lists the service profile associations on each server.

Example

This example shows how to display service profiles associated with the system servers:

```
FP9300-A# show server assoc
Server  Association  Service Profile
------- ------------ ---------------
1/1     Associated   ssp-sprof-1
1/2     Associated   ssp-sprof-2

FP9300-A#
```

Related Commands

Command	Description
show service-profile	Shows service profile information.

show server bios

To view server BIOS firmware information, use the **show server bios** command.

show server bios [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays information for a particular server, specified using chassis-number/server-number (rack ID is not a valid option). The keyword **detail** is available with this option.
detail	(Optional) Displays detailed BIOS information.
uuid *dynamic_uuid*	(Optional) Displays information for a particular server, specified with its dynamic universally unique identifier (UUID), entered in the form NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN. The keyword **detail** is available with this option.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this commands lists the BIOS information for each server.

Example

This example shows how to display detailed BIOS firmware information for all servers:

```
FP9300-A# show server bios detail
Server 1/1:
    Model: FPR9K-SM-24
    Revision: 0
    Serial:
    Vendor: Cisco Systems, Inc.
    Running-Vers: FXOSSM1.1.2.1.3.031420161207
    Package-Vers: 2.0(1.135)
    Init Sequence: 0x0a:0x0a:0x0d:0x0d:0x0b:0x0b:0x01:0x01:0x
00:0x00:0x03:0x03:0x00:0x00:0x02:0x02:0x83:0x83:0xae:0xad
    Init Time: 2015-11-23T19:24:13.159

Server 1/2:
    Model: FPR9K-SM-24
    Revision: 0
    Serial:
    Vendor: Cisco Systems, Inc.
    Running-Vers: FXOSSM1.1.2.1.3.031420161207
    Package-Vers: 2.0(1.135)
    Init Sequence: 0x0a:0x0a:0x0d:0x0d:0x0b:0x0b:0x01:0x01:0x
00:0x00:0x03:0x03:0x00:0x00:0x02:0x02:0x83:0x83:0xae:0xad
    Init Time: 2015-11-23T18:56:23.148
FP9300-A#
```

Related Commands

Command	Description
show server version	Shows current server software versions and status information.

show server boot-order

To display the boot order of a server, use the **show server boot-order** command.

show server boot-order [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays the boot order for a specific server, expressed as chassis-number/server-number (rack ID is not a valid option). The keyword **detail** is available with this option.
detail	(Optional) Displays detailed boot order information.
uuid *dynamic_uuid*	(Optional) Displays the boot order for a particular server, specified with its dynamic universally unique identifier (UUID); entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`. The keyword **detail** is available with this option.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays boot order information for all servers.

Example

This example shows how to display the boot order of all servers:

```
FP9300-A# show server boot-order
Boot Definition:
    Full Name: sys/chassis-1/blade-1/boot-policy
    Reboot on Update: No
    Boot Mode: Uefi

    Boot Storage:
        Order: 1

        Local Storage:
            Name: local-storage

            Boot Any Local Device:
                Order: 1
                Type: Local Any

    Full Name: sys/chassis-1/blade-2/boot-policy
    Reboot on Update: No
    Boot Mode: Uefi

    Boot Storage:
        Order: 1

        Local Storage:
            Name: local-storage
```

```
            Boot Any Local Device:
                Order: 1
                Type: Local Any

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
show server actual-boot-order	Shows actual server boot order.

show server cpu

To display information about the server CPUs, use the **show server cpu** command.

show server cpu [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays the CPU information for a specific server, expressed as chassis-number/server-number (rack ID is not a valid option). The keyword **detail** is available with this option.
detail	(Optional) Displays detailed CPU information in list form.
uuid *dynamic_uuid*	(Optional) Displays the CPU information for a particular server, specified with its dynamic universally unique identifier (UUID); entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`. The keyword **detail** is available with this option.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays CPU information for all servers.

Example

This example shows how to display information about the CPUs in server 1 in chassis 1:

```
FP9300-A# show server cpu 1/1
Server 1/1:
    ID  Presence             Architecture      Socket Cores
     Speed (GHz)
    --- -------------------- ----------------- ------ -------
---- -----------
      1 Equipped             Xeon              CPU1   12
     2.200000
      2 Equipped             Xeon              CPU2   12
     2.200000

FP9300-A#
```

Related Commands

Command	Description
show server inventory	Displays information about the servers installed in this device.

show server decommissioned

To display a list of decommissioned servers, use the **show server decommissioned** command.

show server decommissioned

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display a list of decommissioned servers:

```
FP9300-A# show server decommissioned
Vendor            Model         Serial (SN) Server
----------------- ----------    ----------- ------
Cisco Systems Inc R210-2121605W QCI1442AHFX 2

FP9300-A #
```

Related Commands

Command	Description
show server inventory	Displays information about the servers installed in this device.

show server environment

To display current server status information, use the **show server environment** command.

show server environment [*server_id* | **adapter** | **board** | **cpu** | **detail** | **expand** | **memory** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays status information for a particular server, specified by chassis-number/server-number (rack ID is not a valid option).
adapter	(Optional) Displays server status and status information for each adapter. The keywords **board**, **cpu**, **detail**, and **memory** are also available.
board	(Optional) Displays server status and status information for each motherboard. The keywords **adapter**, **cpu**, **detail**, and **memory** are also available.
cpu	(Optional) Displays server status, motherboard information, and status information for each CPU. The keywords **adapter**, **board**, **detail**, and **memory** are also available.
detail	(Optional) Displays detailed status information in list form.
expand	(Optional) Displays expanded status information, including adapter, motherboard, memory array, DIMM, and CPU information. The **detail** keyword is also available.
memory	(Optional) Lists status information for servers, motherboards, memory arrays, and DIMMs. The keywords **adapter**, **board**, **cpu**, and **detail** are also available.
uuid *dynamic_uuid*	(Optional) Displays status information for a particular server, specified with its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists basic environment information for each server.

Example

This example shows how to display detailed status information for installed network adapters on all servers:

```
FP9300-A# show server environment adapter detail

Server 1/1:
    Overall Status: Ok
    Operability: Operable
    Oper Power: On
```

```
    Adapter 1:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: N/A
        Voltage Status: N/A

    Adapter 2:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: N/A
        Voltage Status: N/A

Server 1/2:
    Overall Status: Ok
    Operability: Operable
    Oper Power: On

    Adapter 1:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
show system	Shows information about the systems configured on this device.

show server firmware

To display server firmware versions and status information, use the **show server firmware** command.

show server firmware [*server_id* | **adapter** | **bios** | **boardcontroller** | **cimc** | **detail** | **fxos** | **storage** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays firmware and status information for a particular server, specified by chassis-number/server-number (rack ID is not a valid option).
adapter	(Optional) Displays firmware version and status information for each adapter. The keyword **detail** is also available.
bios	(Optional) Displays server BIOS firmware versions and status. The keyword **detail** is also available.
boardcontroller	(Optional) Displays management-controller versions and status. The keyword **detail** is also available.
cimc	(Optional) Displays Cisco Integrated Management Controller versions and status. The keyword **detail** is also available.
detail	(Optional) Displays detailed firmware and status information in list form.
fxos	(Optional) Displays version and status information for installed Security Services Processors (SSPs) operating systems. The keyword **detail** is also available.
storage	(Optional) Lists version and status information for local-disk and RAID controllers. The keyword **detail** is also available.
uuid *dynamic_uuid*	(Optional) Displays firmware and status information for a particular server, specified using its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists basic firmware information for each server.

Example

This example shows how to display firmware and status information for local-disk and RAID controllers on all servers:

```
FP9300-A# show server firmware storage
Server 1/1:
    RAID Controller 1:
```

```
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

Server 1/2:
    RAID Controller 1:
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready


    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

FP9300-A#
```

Related Commands

Command	Description
scope firmware	Enters firmware mode.

show server identity

To display identity information for a servers, adapters and interfaces, use the **show server identity** command.

show server identity [*server_id* | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays identifying information for a particular server, specified as chassis-number/server-number (rack ID is not a valid option).
uuid *dynamic_uuid*	(Optional) Displays identifying information for a particular server, specified with its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists identifying information for each server.

Example

This example shows how to display identity information about server 2 in chassis 1:

```
FP9300-A# show server identity 1/2
Server 1/2:
    Burned-In UUID: b3fd461c-b1c7-437b-ab08-c5cb28a84132
    Dynamic UUID: b3fd461c-b1c7-437b-ab08-c5cb28a84132

    Eth Interface:

    Adapter Interface Dynamic MAC Address
    ------- --------- ------------------
          1         1 00:15:A5:01:02:00
          1         2 00:15:A5:00:00:7D
          1         3 B0:AA:77:2F:F0:CD
          1         4 B0:AA:77:2F:F0:ED
          1         5 B0:AA:77:2F:F0:DD
          1         6 00:15:A5:00:00:9D
          1         7 00:15:A5:00:00:BE
          1         8 00:15:A5:00:00:FE
          1         9 00:15:A5:00:00:8D
          1        10 00:15:A5:00:00:5D
          1        11 00:15:A5:00:00:6D
          1        12 00:15:A5:00:00:CE
          1        13 00:15:A5:00:00:DE
          1        14 00:15:A5:00:01:1E
          1        15 00:15:A5:00:00:1E
          2         1 B0:AA:77:2F:F0:FD
          2         2 B0:AA:77:2F:F0:CE
          2         3 B0:AA:77:2F:F0:EE
          2         4 00:15:A5:00:01:0E
          2         5 00:15:A5:00:00:0E
          2         6 00:15:A5:00:00:3E
```

```
          2         7 00:15:A5:00:00:EE
          2         8 00:15:A5:00:00:4D
          2         9 00:15:A5:00:00:AE
          2        10 00:15:A5:00:00:2E
          2        11 00:15:A5:00:00:5E
          2        12 00:15:A5:00:00:4E
          2        13 00:15:A5:00:00:7E

    Ext Interface:

    Adapter Interface Mac
    ------- --------- ---
          1         1 B0:AA:77:21:19:1E
          1         5 B0:AA:77:21:19:1F
          2         1 B0:AA:77:21:19:42
          2         5 B0:AA:77:21:19:43

FP9300-A#
```

Related Commands

Command	Description
scope server	Enters server mode.

show server inventory

To display information about the servers installed in this device, use the **show server inventory** command.

show server inventory
[*id* | *server_id* | **adapter** | **bios** | **board** | **cpu** | **detail** | **expand** | **memory** | **mgmt** | **storage** | **uuid** *dynamic_uuid*]

Syntax Description

id	(Optional) Displays information for the specified server. The ID must be a number between 1 and 255.
server_id	(Optional) Displays inventory information for a particular server, specified using chassis-number/server-number.
adapter	(Optional) Displays server information along with information for each adapter. The keywords **bios**, **board**, **cpu**, **detail**, **memory**, **mgmt**, and **storage** are also available with this keyword.
bios	(Optional) Displays server information along with BIOS information. The keywords **adapter**, **board**, **cpu**, **detail**, **memory**, **mgmt**, and **storage** are also available with this keyword.
board	(Optional) Displays server information along with motherboard information. The keywords **adapter**, **bios**, **cpu**, **detail**, **memory**, **mgmt**, and **storage** are also available with this keyword.
cpu	(Optional) Displays server information along with CPU information. The keywords **adapter**, **bios**, **board**, **detail**, **memory**, **mgmt**, and **storage** are also available with this keyword.
detail	(Optional) Displays detailed inventory information for each server.
expand	(Optional) Displays expanded system information for each server. The keyword **detail** is also available.
memory	(Optional) Displays server information along with DIMM information. The keywords **adapter**, **bios**, **board**, **cpu**, **detail**, **mgmt**, and **storage** are also available with this keyword.
mgmt	(Optional) Displays server-management information. The keywords **adapter**, **bios**, **board**, **cpu**, **detail**, **memory**, and **storage** are also available with this keyword.
storage	(Optional) Displays server information along with disk and RAID information. The keywords **adapter**, **bios**, **board**, **cpu**, **detail**, **memory**, and **mgmt** are also available with this keyword.
uuid *dynamic_uuid*	(Optional) Displays firmware and status information for a particular server, specified with its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists inventory information for each server.

Example

This example shows how to display basic inventory information:

```
FP9300-A# show server inventory
Server  Equipped PID Equipped VID Equipped Serial (SN) Slot S
tatus      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ------
---------- ---------------- ----------
1/1     FPR9K-SM-24  V01          FLM1949C6J5          Equipp
ed                   262144         24
1/2     FPR9K-SM-24  V01          FLM1949C6J1          Equipp
ed                   262144         24
1/3                                                     Empty

FP9300-A#
```

Related Commands

Command	Description
show server environment	Shows current server status information.

show server memory

To display information about the server dual in-line memory modules (DIMMs) installed in this device, use the **show server memory** command.

show server memory [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays memory information for a specific server, specified by chassis-number/server-number (rack ID is not a valid option).
detail	(Optional) Displays detailed memory information for each server.
uuid *dynamic_uuid*	(Optional) Displays memory information for a particular server, specified using its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists memory information for each server.

Example

This example shows how to display detailed memory information:

```
FP9300-A# show server memory detail
Server 1/1:
    Array 1:
        CPU ID: 1
        Current Capacity (MB): 262144
        Error Correction: Undisc
        Max Capacity (MB): 1572864
        Max Devices: 24
        Populated: 16

        DIMMS:

        ID 1:
            Location: A1
            Presence: Equipped
            Overall Status: Operable
            Visibility: Yes
            Vendor: 0xAD00
            Vendor Part Number: HMA42GR7MFR4N-TF
            Vendor Serial (SN): 244BC0A6
            HW Revision: 0
            Form Factor: DIMM
            Type: Undisc
            Capacity (MB): 16384
            Clock: 2133
            Latency: 0.500000
```

```
            Width: 64

        ID 2:
            Location: A2
            Presence: Equipped
            Overall Status: Operable
            Visibility: Yes
            Vendor: 0xAD00
            Vendor Part Number: HMA42GR7MFR4N-TF
            Vendor Serial (SN): 245C4A07
            HW Revision: 0
            Form Factor: DIMM
            Type: Undisc
            Capacity (MB): 16384
            Clock: 2133
            Latency: 0.500000
            Width: 64

        ID 3:
            Location: A3
            Presence: Missing
            Overall Status: Removed
            Visibility: No
            Vendor:
            Vendor Part Number:
            Vendor Serial (SN):
            HW Revision: 0
            Form Factor: Undisc
            Type: Undisc
            Capacity (MB): Unknown
            Clock: Unknown
            Latency: Unknown
            Width: Unknown

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
show server identity	Shows identity information for a servers, adapters and interfaces.

show server status

To display information on the status of a server, use the **show server status** command.

show server status [*id* | *server_id* | **detail** | **uuid** *dynamic_uuid*]

Syntax Description

id	(Optional) Displays information for the specified server. The ID must be a number between 1 and 255.
server_id	(Optional) Displays status information for a particular server, specified as chassis-number/server-number.
detail	(Optional) Displays detailed status information for each server.
uuid *dynamic_uuid*	(Optional) Displays status information for a particular server, specified with its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, the command lists status information for all servers.

Example

This example shows how to display status information for a specific server using the chassis and blade IDs:

```
FP9300-A# show server status 1/1
Server    Slot Status      Overall Status      Discovery
------    -----------      --------------      ---------
1/1        Equipped        Ok                  Complete
1/2        Equipped        Ok                  Complete
1/3        Empty

FP9300-A#
```

Related Commands

Command	Description
show server inventory	Shows information about the servers installed in this device.

show server storage

To display server disk and RAID information, use the **show server storage** command.

show server storage [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays storage information for a particular server, specified as chassis-number/server-number (rack ID is not a valid option).
detail	(Optional) Displays detailed storage information for each server.
uuid *dynamic_uuid*	(Optional) Displays storage information for a particular server, specified using its dynamic universally unique identifier (UUID), entered in the form NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists storage information for each server.

Example

This example shows how to display basic storage information:

```
firepower# show server storage
Server 1/1:
    RAID Controller 1:
        Type: SAS
        Vendor: Cisco Systems Inc
        Model: UCSB-MRAID12G
        Serial: LSV194501YW
        HW Revision: C0
        PCI Addr: 01:00.0
        Raid Support: RAID0, RAID1
        OOB Interface Supported: Yes
        Rebuild Rate: 30
        Controller Status: Optimal

        Local Disk 1:
            Vendor: SAMSUNG
            Model: MZIES800HMHP/003
            Serial: S1N2NYAG800062
            HW Rev: 0
            Operability: Operable
            Presence: Equipped
            Size (MB): 761985
            Drive State: Online
            Power State: Active
            Link Speed: 12 Gbps
            Device Type: SSD
```

```
        Local Disk 2:
            Vendor: SAMSUNG
            Model: MZIES800HMHP/003
            Serial: S1N2NYAG800100
            HW Rev: 0

    <--- remaining lines removed for brevity --->

firepower#
```

Related Commands

Command	Description
show server inventory	Shows information about the servers installed in this device.

show server version

To display current server software versions and status information, use the **show server version** command.

show server version [*server_id* | **adapter** | **bios** | **boardcontroller** | **cimc** | **detail** | **fxos** | **storage** | **uuid** *dynamic_uuid*]

Syntax Description

server_id	(Optional) Displays firmware and status information for a particular server, specified as chassis-number/server-number or rack ID.
adapter	(Optional) Displays firmware version and status information for each adapter. The keyword **detail** is also available.
bios	(Optional) Displays server BIOS firmware versions and status. The keyword **detail** is also available.
boardcontroller	(Optional) Displays management-controller versions and status. The keyword **detail** is also available.
cimc	(Optional) Displays Cisco Integrated Management Controller versions and status. The keyword **detail** is also available.
detail	(Optional) Displays detailed firmware and status information in list form.
fxos	(Optional) Displays version and status information for installed Security Services Processors (SSPs) operating systems. The keyword **detail** is also available.
storage	(Optional) Lists version and status information for local-disk and RAID controllers. The keyword **detail** is also available.
uuid *dynamic_uuid*	(Optional) Displays firmware and status information for a particular server, specified with its dynamic universally unique identifier (UUID), entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists basic software information for each server.

Example

This example shows how to display software versions and status information for local-disk and RAID controllers on all servers:

```
FP9300-A# show server version storage
Server 1/1:
    RAID Controller 1:
```

```
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

Server 1/2:
    RAID Controller 1:
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready


    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

FP9300-A#
```

Related Commands

Command	Description
show server firmware	Shows server firmware versions and status.

show service-profile

To display service profile information, use the **show service-profile** command.

show service-profile { **assoc** | **circuit** | **connectivity** | **identity** | **inventory** | **path** | **status** }

Syntax Description

assoc	Displays server and association information for each service profile. The following optional keywords are available: • **detail**—Displays detailed association information for the service profiles. • **org** *name*—Displays service-profile association information for the specified organization. • **server** { *id* | *server_id* }—Displays service-profile association information for the specified server. • **uuid** { **derived** | *dynamic_uuid* }—Displays service-profile association information for the specified UUID.
circuit	Displays network circuit information for the service profiles. The following optional keywords are available: • **detail**—Displays detailed network-circuit information for the service profiles. • **name** *name*—Displays network-circuit information for the specified service profile. • **org** *org_name*—Displays service-profile circuit information for the specified organization. • **server** { *id* | *server_id* }—Displays service-profile circuit information for the specified server; *id* is a value between 1 and 255; *server_id* is specified as chassis-number/blade-number. • **uuid** { **derived** | *dynamic_uuid* }—Displays service-profile circuit information for the specified UUID, entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

identity	Displays service-profile identity (UUID pool) information. These optional keywords are available: • **name** *name*—Displays identity information for the specified service profile. • **org** *org_name*—Displays service-profile identity information for the specified organization. • **server** {*id* | *server_id*}—Displays service-profile identity information for the specified server; *id* is a value between 1 and 255; *server_id* is specified as chassis-number/blade-number. • **uuid** {**derived** | *dynamic_uuid*}—Displays service-profile identity information for the specified UUID, entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

inventory	Lists the current service-profile inventory, with type, assigned-server and association-status information. The following optional keywords are available: • **adapter**—Displays information about the adapters associated with the service profiles. • **bios**—Displays server and BIOS information associated with the service profiles. • **board**—Displays server and motherboard information associated with the service profiles. • **cpu**—Displays information about servers and CPUs associated with the service profiles. • **detail**—Displays detailed inventory information for the service profiles. • **expand**—Displays expanded inventory information for the service profiles. • **memory**—Displays server and DIMM information associated with the service profiles. • **mgmt**—Displays server configuration information associated with the service profiles. • **name** *name*—Displays inventory information for the specified service profile. • **org** *org_name*—Displays service-profile inventory information for the specified organization. • **server** {*id* | *server_id*}—Displays service-profile inventory information for the specified server; *id* is a value between 1 and 255; *server_id* is specified as chassis-number/blade-number. • **storage**—Displays server, local disk and RAID information associated with the service profiles. • **uuid** {**derived** | *dynamic_uuid*}—Displays service-profile inventory information for the specified UUID, entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

path	Displays service profile network-path information, including connection type and port information. The following optional keywords are available: • **detail**—Displays detailed network-path information for the service profiles. • **name** *name*—Displays path information for the specified service profile. • **org** *org_name*—Displays network-path information for the specified organization. • **server** {*id* | *server_id*}—Displays service-profile network-path information for the specified server; *id* is a value between 1 and 255; *server_id* is specified as chassis-number/blade-number. • **uuid** {**derived** | *dynamic_uuid*}—Displays network-path information for the service profile specified by the given UUID, entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.
status	Displays service-profile status, with operational status, assigned server and association status information. The following optional keywords are available: • **detail**—Displays detailed status information for the service profiles. • **expand**—Displays expanded status information for the service profiles. • **name** *name*—Displays status information for the specified service profile. • **org** *org_name*—Displays service-profile status information for the specified organization. • **power**—Displays server power and status information for the service profiles. • **server** {*id* | *server_id*}—Displays service-profile status information for the specified server; *id* is a value between 1 and 255; *server_id* is specified as chassis-number/blade-number. • **thermal**—Displays server status, temperature and thermal information for the service profiles. • **uuid** {**derived** | *dynamic_uuid*}—Displays status information for the service profile specified by the given UUID, entered in the form `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`. • **voltage** —Displays server status, power and voltage information for the service profiles.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command lists information for each service profile.

Examples

This example shows how to display inventory information for a specific service profile:

```
FP9300-A# show service-profile inventory name ssp-sprof-1

Service Profile Name Type              Server  Assignment Association
-------------------- ----------------- ------- ---------- -----------
ssp-sprof-1          Instance          1/1     Assigned   Associated

FP9300-A#
```

This example shows how to display power status information for the service profiles:

```
FP9300-A# show service-profile status power
Service Profile Name: ssp-sprof-1
Type: Instance
Server: 1/1
Description: ssp service profile
Assignment: Assigned
Association: Associated
Power State: On
Op State: Ok
Oper Qualifier: N/A
Conf State: Applied
Config Qual (Deprecated): N/A
Server Config Issues: N/A
Network Config Issues: N/A
Storage Config Issues: N/A
vNIC Config Issues: N/A
iSCSI Config Issues: N/A
Current Task:
    Server 1/1:
        Overall Status: Ok
        Operability: Operable
        Oper Power: On

        Motherboard:
            Threshold Status: OK
            Overall Status: N/A
            Operability: N/A
            Oper Power: On
            Power State: Ok
            Thermal Status: OK
            Voltage Status: OK
            CMOS Battery Voltage Status: Ok
            Mother Board Power Usage Status: Ok

            Motherboard Temperature Statistics:
                Motherboard Front Temperature (C): 42.000000
                Motherboard Rear Temperature (C): 57.000000

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
scope service-profile	Enters service profile mode.

show shell-session-limits

To display the list of shell sessions available on the system, use the **show shell-session-limits** command.

show shell-session-limits [**detail**]

Syntax Description

detail	Displays detailed information on shell sessions limits.

Command Modes

scope system/scope services

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope services.

Examples

This example shows how to display information on system shell session limits:

```
Firepower /fabric-interconnect # scope system
Firepower /system #scope services
Firepower /system/services # show shell-session-limits
Shell Sessions:
    Maximum logins for single user Maximum Sessions
    ------------------------------ ----------------
    32                             32
```

Example

This example shows how to display detailed information on all shell sessions:

```
Firepower /system/services # show shell-session-limits detail
Shell Sessions:
    Maximum logins for single user: 32
    Maximum Sessions: 32
```

show (slot)

To view current SSP information, use the **show** command in slot mode.

show [**app-instance** | **detail** | **event** | **expand** | **fault** | **fsm** | **heartbeat** | **heartbeat-config** | **monitor**]

Syntax Description

app-instance	(Optional) Displays information about the module application instance. The following options are also available: • *app-name*—Shows information for only the specified instance. • **detail**—Shows detailed application instance information. The **expand** keyword is available with this option. • **expand**—Shows expanded application instance information. The **detail** keyword is available with this option. • **fsm**—Shows finite state machine information for the application instance.
detail	(Optional) Displays detailed information for the module application instance. The **expand** keyword is available with this option.
event	(Optional) Displays event management information for the application. The **detail** and **expand** keywords are available with this option.
expand	(Optional) Displays expanded information for the module application instance. The **detail** keyword is available with this option.
fault	(Optional) Displays information about faults that have occurred on the SSP. The following options are also available with this keyword: • *fault_ID*—Shows information for the specified fault. • **cause**—Shows information for only the specified cause type. • **detail**—Shows detailed fault information. • **severity**—Shows information for only the specified severity level. • **suppressed**—Lists suppressed faults. The **cause**, **detail** and **severity** keywords are available with this option.
fsm task	(Optional) Displays FSM task information for the SSP. The **detail** keyword is available with this option.
heartbeat	(Optional) Displays information about the last-received heartbeat. The **detail** and **expand** keywords are available with this option.
heartbeat-config	(Optional) Displays information about the current heartbeat configuration for the SSP. The **detail** and **expand** keywords are available with this option.
monitor	(Optional) Displays monitoring information for the SSP. The **detail** and **expand** keywords are available with this option.

Command Modes scope ssa/scope slot

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines By default, this command displays general module configuration information.

Example

This example shows how to display general slot information:

```
firepower# scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # show
Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    2          Info      Ok           Online
firepower /ssa/slot #
```

Related Commands

Command	Description
scope slot	Enters module configuration mode for a specific slot.

show slot

To view the list of slots like admin state and operstate available on the system, use the **show slot** command.

show [**detail** | **expand**]

Syntax Description

detail	Displays detailed slots information.
expand	(Optional) Displays expanded information for slots.

Command Modes

scope ssa

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope ssa mode

Example

This example shows how to display information of all slots in the system:

```
Firepower / fabric-interconnect # scope ssa
Firepower /ssa # show slot

Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online

This example shows detailed information for all available slots.

Firepower /ssa # show slot detail
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
    Clear Log Data: Available
    Error Msg:
#
```

Example

This example shows how to display detailed information of all available slots detail expand:

```
Firepower /ssa #show slot detail expand
  Slot:
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
```

```
Clear Log Data: Available
Error Msg:

Heartbeat:
    Last Received Time: 2012-07-04T22:43:13.030
    Heartbeat Interval: 5
    Max Number of Missed heartbeats Permitted: 3

Monitor:
    OS Version: 82.14(0.48i)
    CPU Total Load 1 min Avg: 0.360000
    CPU Total Load 5 min Avg: 0.360000
    CPU Total Load 15 min Avg: 0.360000
    Memory Total (MB): 64221
    Memory Free (MB): 54576
    Memory Used (MB): 8584
    CPU Cores Total: 24
    CPU Cores Available: 22
    Memory App Total (MB): 52957
    Memory App Available (MB): 52957
    Data Disk Total (MB): 128727
    Data Disk Available (MB): 128727
    Secondary Disk Total (MB): 0
    Secondary Disk Available (MB): 0
    Disk File System Count: 5
    Blade Uptime: up 6 days, 12:04
    Last Updated Timestamp: 2012-07-04T22:42:52.566

    Disk File System:
        File System: /dev/sda1
        Mount Point: /mnt/boot
        Disk Total (MB): 7614
        Disk Free (MB): 7447
        Disk Used (MB): 167

        File System: /dev/sda2
        Mount Point: /opt/cisco/config
        Disk Total (MB): 1846
        Disk Free (MB): 1736
        Disk Used (MB): 15

        File System: /dev/sda3
        Mount Point: /opt/cisco/platform/logs
        Disk Total (MB): 4629
        Disk Free (MB): 4329
        Disk Used (MB): 62

        File System: /dev/sda5
        Mount Point: /var/data/cores
        Disk Total (MB): 46679
        Disk Free (MB): 28868
        Disk Used (MB): 15427

        File System: /dev/sda6
        Mount Point: /opt/cisco/csp
        Disk Total (MB): 128727
        Disk Free (MB): 128566
        Disk Used (MB): 161
```

show snmp (connect fxos)

To display extensive information about the current Simple Network Management Protocol (SNMP) configuration, use the **show snmp** command when connected to the FXOS command shell.

show snmp [**community** | **context** | **engineID** | **group** | **host** | **internal** | **mib** | **sessions** | **source-interface** | **trap** | **user**]

Syntax Description

community	(Optional) Display the current SNMP community string and groups assigned access.
context	(Optional) List the SNMP context mapping entries.
engineID	(Optional) Display the local SNMP engine ID.
group	(Optional) List the SNMP roles and their access permissions.
host	(Optional) Display the currently defined SNMP destinations.
internal	(Optional) Display a variety of SNMP internal information. Use the **?** keyword to view additional options.
mib	(Optional) Display the SNMP MIB cache or interface tables. Use the **?** keyword to view additional options.
sessions	(Optional) Display the current SNMP sessions.
source-interface	(Optional) Display the SNMP source interface for both notification types.
trap	(Optional) List all enabled SNMP trap types.
user	(Optional) List all currently defined SNMPv3 users and their parameters. Use the *name* option to view information for a specific user.

Command Modes

connect fxos/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

By default, this command displays current SNMP configuration information, including community string, system contact and system location, as well as listing SNMP input and output packet types.

Example

The following example shows you how to connect to the FXOS shell and use the **show snmp** command to view current SNMP information:

```
firepower # connect fxos
firepower(fxos) # show snmp
Community            Group / Access      context    acl_filter
```

```
---------            --------------      -------    ----------
SNMPcommunity         network-operator
sys contact: R_Admin
sys location:

0 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
398 SNMP packets output
        0 Too big errors
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 In No such name PDU
        0 In Bad vlaue PDU
        0 In Read only PDU
        0 In General errors
        0 In Get Responses
        0 Unknown Context name
        398 Out Traps PDU
        0 Out Get Requests
        0 Out Get Next Requests
        0 Out Set Requests
        0 Out Get Responses
        0 Silent Drops



_____________________________________________________________
                  SNMP USERS
_____________________________________________________________

User                          Auth  Priv(enforce) Groups
____                          ____  _____________ ______
test1                         sha   no            network-operator

snmp-user1                    sha   no            network-operator

snmp-user2                    sha   no            network-operator

_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________

User                          Auth  Priv
____                          ____  ____


SNMP Tcp Authentication Flag : Enabled.

-----------------------------------------------------------------------------------------------
Port Monitor : unset
-----------------------------------------------------------------------------------------------


Policy Name : default
```

```
Admin Status: Not Active
Oper Status: Not Active
Port type   : All Ports
-------------------------------------------------------------------------------------------
Counter                 Threshold  Interval Rising Threshold event Falling Threshold  event
 In Use
-------                 ---------  -------- ---------------- ----- ------------------ -----
 ------
Link Loss                Delta      60       5                4     1                  4
   Yes
Sync Loss                Delta      60       5                4     1                  4
   Yes
Invalid Words            Delta      60       5                4     1                  4
   Yes
Invalid CRC's            Delta      60       1                4     0                  4
   Yes
RX Performance           Delta      60       5                4     1                  4
   Yes
LR RX                    Delta      60       200              4     10                 4
   Yes
LR TX                    Delta      60       5                4     1                  4
   Yes
Timeout Discards         Delta      60       5                4     1                  4
   Yes
Credit Loss Reco         Delta      60       200              4     10                 4
   Yes
TX Credit Not Available  Delta      1        1                4     0                  4
   Yes
RX Datarate              Delta      1        10               4     0                  4
   Yes
TX Datarate              Delta      60       80               4     20                 4
   Yes
ASIC Error Pkt from Port Delta      60       80               4     20                 4
   Yes
-------------------------------------------------------------------------------------------


SNMP protocol : Enabled


--------------------------------------------------------------------
Context                          [Protocol instance, VRF, Topology]
                                 [vlan, MST]
--------------------------------------------------------------------
1                               ,
                                ,
                                ,
                                1,

--------------------------------------------------------------------
101                             ,
                                ,
                                ,
                                101,

--------------------------------------------------------------------
102                             ,
                                ,
                                ,
                                102,

--------------------------------------------------------------------

    <--- remaining lines removed for brevity --->
```

```
firepower(fxos) #
```

Related Commands

Command	Description
enable snmp	Enables SNMP.
set snmp	Sets SNMP configuration parameters.
show snmp (monitoring)	Shows basic information about the current SNMP configuration.

show snmp (monitoring)

To display basic information about the current Simple Network Management Protocol (SNMP) configuration, use the **show snmp** command.

show snmp [**community**]

Syntax Description

community	(Optional) Displays the current SNMP community name. **Note** This keyword has been deprecated, since for security, only an empty field is displayed.

Command Modes

scope monitoring/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

By default, this command displays current SNMP configuration information, including admin state, system contact and system location.

Example

The following example shows you how to scope into monitoring mode and use the **show snmp** command to view current SNMP configuration:

```
firepower# scope monitoring
firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Related Commands

Command	Description
enable snmp	Enables SNMP.
set snmp	Sets SNMP configuration parameters.
show snmp (connect fxos)	Shows extensive information about the current SNMP configuration.

show snmp-trap

To display information about currently defined SNMP traps, enter the **show snmp-trap** command.

show snmp-trap [**detail** | *trap_ID*]

Syntax Description

detail	(Optional) Use this keyword to view detailed information about the SNMP trap(s).
trap_ID	(Optional) Specify the host name or IP address of a particular SNMP trap destination to view information about that trap. (This option is available only in scope monitoring/ mode.) The **detail** keyword is available with this option.

Command Modes

scope monitoring/

scope monitoring/snmp-trap/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

In scope monitoring/ mode, by default, this command displays a current list of SNMP traps.

In scope monitoring/snmp-trap/ mode, this command displays information about the current trap.

Example

The following example shows you how to scope into monitoring mode and use the **show snmp-trap** command to view a list of current SNMP traps:

```
firepower# scope monitoring
firepower /monitoring # show snmp-trap

SNMP Trap:
    SNMP Trap                Port     Community  Version V3 Privilege Notification Type
    ------------------------ -------- ---------- ------- ------------ -----------------
    trap1_informs            162      ****       V2c     Noauth       Informs
    192.168.10.100           162      ****       V3      Noauth       Traps
firepower /monitoring #
```

Related Commands

Command	Description
create snmp-trap	Creates a new SNMP trap.
enable snmp	Enables SNMP.
set (snmp-trap)	Specifies parameters for an existing SNMP trap.
show snmp (monitoring)	Shows basic information about the current SNMP configuration.

Command	Description
show snmp (connect fxos)	Shows extensive information about the current SNMP configuration.

show snmp-user

To display information about currently defined SNMPv3 users, enter the **show snmp** command.

show snmp-user [**detail** | **fault** | *user_name*]

Syntax Description

detail	(Optional) Use this keyword to view detailed information about the SNMPv3 user(s).
fault	(Optional) Use this keyword to view fault information for this user. The following optional keywords are available with this option: • **cause** – Use this keyword to filter fault information by cause. • **detail** – Use this keyword to view detailed fault information. • **severity** – Use this keyword to filter fault information by severity. • **suppressed** – Use this keyword to view only suppressed faults. • *fault_ID* – You can specify a particular fault by entering its ID number; valid values are 0 to 18446744073709551615. **Note** This option is available only in scope monitoring/snmp-user/ mode.
user_name	(Optional) Specify the name of a particular SNMP user to view information about that user. (This option is available only in scope monitoring/ mode.) The **detail** keyword is available with this option.

Command Modes

scope monitoring/

scope monitoring/snmp-user/

Command History

Release	Modification
1.1.1	Command added.

Usage Guidelines

In scope monitoring/ mode, by default, this command displays a current list of SNMPv3 users with authentication type for each.

In scope monitoring/snmp-trap/ mode, this command displays information about the current SNMPv3 user.

Example

The following example shows you how to scope into monitoring mode and use the **show snmp-user** command to view a list of current SNMPv3 users, as well as detailed configuration information for a specific user:

```
firepower# scope monitoring
firepower /monitoring # show snmp-user

SNMPv3 User:
```

```
    Name                    Authentication type
    ----------------------- -------------------
    snmp-user1              Sha
    testuser                Sha
    snmp-user2              Sha
firepower /monitoring # show snmp-user snmp-user1 detail

SNMPv3 User:
    Name: snmp-user1
    Authentication type: Sha
    Password: ****
    Privacy password: ****
    Use AES-128: Yes
firepower /monitoring #
```

Related Commands

Command	Description
create snmp-user	Creates a new SNMPv3 user.
enable snmp	Enables SNMP.
set (snmp-user)	Specifies parameters for an existing SNMPv3 user.
show snmp (monitoring)	Shows basic information about the current SNMP configuration.
show snmp (connect fxos)	Shows extensive information about the current SNMP configuration.

show ssh-server

To display information about the SSH server, use the **show ssh-server** command.

show server [**host-key**]

Syntax Description

host-key	(Optional) Displays SSH server host key size, and whether the key has been deleted.

Command Modes

Services mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to view SSH connection and authentication information.

Example

This example shows how to display SSH server information:

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # show ssh-server
Name: ssh
    Admin State: Enabled
    Port: 22
    Kex algorithm: diffie-hellman-group14-sha1
    Mac algorithm: hmac-sha1,hmac-sha2-256,hmac-sha2-512
    Encrypt algorithm:
aes128-ctr,aes192-ctr,aes256-ctr,3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
    Authentication algorithm: Rsa
    Host Key Size: 2048
    Rekey Limit Volume: None Time: None
FP9300-A /system/services #
```

Command	Description
create ssh-server	Creates a new SSH server host key.
delete ssh-server	Deletes the existing SSH server host key.
set ssh-server	Sets the SSH host key size.

show stats

To display IPSec statistics, use the **show stats** command.

show stats [**detail** | **listauthor** | **listcert** | **listconn** | **listsa** | **status**]

Syntax Description

detail	(Optional) Shows additional IPSec statistics.
listauthor	(Optional) Shows all available trustpoints. The **detail** keyword is available with this option.
listcert	(Optional) Shows all available certifications. The **detail** keyword is available with this option.
listconn	(Optional) Shows the operational state of all connections. The **detail** keyword is available with this option.
listsa	(Optional) Shows the operational state of all IPSec security associations (SAs). The **detail** keyword is available with this option.
status	(Optional) Shows overall IPsec status. The **detail** keyword is available with this option.

Command Modes

IPSec mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to display IPSec statistics.

Example

This example shows how to display IPSec connection information for a specified connection:

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # show stats

Ipsec Stats:
    Stats Type: Status
    Stats Data: Status of IKE charon daemon (strongSwan 5.3.5, Linux 3.14.39ltsi, i686):
  uptime: 11 days, since Jun 29 17:36:39 2018
  malloc: sbrk 2289664, mmap 0, used 199808, free 2089856
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints
 pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf xcbc cmac hmac files
 attr kernel-netlink resolve socket-default stroke vici updown xauth-generic
Listening IP addresses:
  10.122.150.220
  192.15.1.250
  192.15.1.251
  192.3.0.254
```

```
  192.5.254.1
  192.5.1.254
  192.7.254.1
  192.9.0.1
  192.128.254.1
  203.0.113.126
  192.16.254.1
Connections:
Security Associations (0 up, 0 connecting):
  none

    Time Stamp: 2018-07-11T17:20:17.542
FP9300-A /security/ipsec #
```

Related Commands

Command	Description
show connection	Shows configuration information for the current IPSec connections.
show ipsec-log	Shows IPSec connection logs.

show storage

To display all the partitions and their current disk usage in a disk, use the **show storage** command.

show storage

Command Modes

scope fabric-interconnect

Command History

Release	Modification
2.11.1	Command added.

Usage Guidelines

Use this command to display the disk usage.

Example

Following example displays the storage on a local flash drive of fabric interconnect:

```
firepower /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        106540           43
    callhome         128              Empty
    dev-shm          512              59
    isan             4000             36
    mnt-cfg-0        73               3
    mnt-cfg-1        73               3
    mnt-plog         47               3
    mnt-pss          73               41
```

show subinterface

To show information about the subinterface, use the **show subinterface** command.

show subinterface [**detail**]

Syntax Description

detail	Shows information for each subinterface in a non-table format.

Command Modes

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/create port-channel/

Command History

Release	Modification
2.4(1)	Command added.

Usage Guidelines

Subinterfaces are supported for container instances only.

Example

The following is sample output from the **show subinterface** command.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface ethernet1/8
firepower /eth-uplink/fabric/interface # show subinterface

Sub Interface:
    Sub-If Id  Sub-Interface Name VLAN        Port Type
    ---------- ------------------ ----------- ---------
           100 Ethernet1/5.100    100         Data
```

The following is sample output from the **show subinterface detail** command.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface ethernet1/8
firepower /eth-uplink/fabric/interface # show subinterface detail

Sub Interface:
    Sub-If Id: 100
    Sub-Interface Name: Ethernet1/5.100
    VLAN: 100
    Port Type: Data
```

Related Commands

Command	Description
create port-channel	Creates an EtherChannel (port channel).
create subinterface	Adds a subinterface.

Command	Description
scope interface	Enters the physical interface object.
set port-type	Sets the interface type.

show sup

To view chassis supervisor version information, use the **show sup version** command.

show sup version [**detail**]

Syntax Description		
	detail	(Optional) Displays detailed supervisor version information.

Command Modes

Chassis mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this commands lists the supervisor ROMMON and FPGA version information.

Example

This example shows how to display detailed supervisor firmware information for all servers:

```
FP9300-A /chassis # show sup version detail
SUP FIRMWARE:
    ROMMON:
        Running-Vers: 1.0.11
        Package-Vers: 1.0.11
        Activate-Status: Ready
        Upgrade Status: SUCCESS
    FPGA:
        Running-Vers: 1.05
        Package-Vers: 1.0.11
        Activate-Status: Ready

FP9300-A /chassis #
```

Related Commands

Command	Description
show version	Shows current software versions and status information for each server on the chassis.

show system

To display information about the systems configured on this device, use the **show system** command.

show system [**detail** | **firmware** | **version**]

Syntax Description

detail	(Optional) Displays detailed system information.
firmware	(Optional) Displays system firmware-version and status information. The optional keywords **detail** and **expand** are also available.
version	(Optional) Displays system version and status information. The optional keywords **detail** and **expand** are also available.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays name, mode and IP addresses for each configured system.

Example

This example shows how to display expanded system version information:

```
FP9300-A# show system version expand
FPRM:
    Running-Vers: 4.2(1.62)
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready

Catalog:
    Running-Vers: 4.2(1.62)T
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready

Management Extension:
    Running-Vers: 2.2(1.8)
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready

Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.21.62)
    Running-Sys-Vers: 5.0(3)N2(4.21.62)
    Package-Vers: 2.2(1.63)
    Startup-Kern-Vers: 5.0(3)N2(4.21.62)
    Startup-Sys-Vers: 5.0(3)N2(4.21.62)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:

Chassis 1:
```

```
    Server 1:
        CIMC:
            Running-Vers: 3.1(20a)
            Package-Vers: 2.2(1.63)
            Update-Status: Ready
            Activate-Status: Ready

        Adapter 1:
            Running-Vers: 4.0(1.57)
            Package-Vers: 2.2(1.63)
            Update-Status: Ready
            Activate-Status: Ready
        Adapter 2:
            Running-Vers: 4.0(1.57)

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Related Commands

Command	Description
scope system	Enters system mode.

show system reset-reason

To display information about the system reset reason, use the **show system reset-reason** command.

show system reset-reason

Syntax Description

reset-reason	(Optional) Displays detailed reset reason information.

Command Modes

connect fxos

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays the reset reason information.

Example

This example shows how to display reset reason information for a module:

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 826701 usecs after Sun Jul 11 09:14:12 2021
    Reason: Reset Requested by CLI command reload <=========Manual reboot requested from
CLI.
    Service:
    Version: 5.0(3)N2(4.81)

2) At 865598 usecs after Wed Apr 21 17:10:58 2021
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 5.0(3)N2(4.61)
```

show stats system-stats

To display the information of system stats available on the system, use the **show stats system-stats** command.

show stats system-stats detail

Syntax Description

detail	(Optional) Shows additional IPSec statistics.

Command Modes

scope fabric-interconnect a

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope fabric-interconnect a.

Example

This example shows how to display system stats information:

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect  # show stats system-stats
 System Stats:
    Time Collected: 2012-07-15T06:55:00.187
    Monitored Object: sys/switch-A
    Suspect: No
    Load: 3.800000
    Mem Available (MB): 11762
    Mem Cached (MB): 2008
    Thresholded: 0

This example shows detailed information of stats history system stats:
QP1 /fabric-interconnect # show stats history system-status
System Stats:
    Time Collected: 2012-07-15T06:54:00.249
    Monitored Object: sys/switch A/sysstats
    Suspect: No
    Load: 3.930000
    Mem Available (MB): 11814
    Mem Cached (MB): 2008
    Thresholder: 0

    Time Collected: 2012-07-15T06:46:30.804
    Monitored Object: sys/switch A/sysstats
    Suspect: No
    Load: 3.480000
    Mem Available (MB): 11814
    Mem Cached (MB): 2009
    Thresholded: 0

    Time Collected: 2012-07-15T06:39:00.173
    Monitored Object: sys/switch-A/sysstats
    Suspect: No
    Load: 3.780000
    Mem Available (MB): 11758
    Mem Cached (MB): 2009
```

This example shows how to display detailed information of stats history system stats detail:

```
FP9300-A /fabric-interconnect # show stats history system-status detail

System Stats:
    Time Collected: 2012-07-15T06:54:00.249
    Monitored Object: sys/switch-A/sysstats
    Suspect: No
    Load: 3.930000
    Load Min: 3.380000
    Load Max: 5.300000
    Load Avg: 4.320666
    Mem Available (MB): 11814
    Mem Available Min (MB): 11796
    Mem Available Max (MB): 11815
    Mem Available Avg (MB): 11804
    Mem Cached (MB): 2008
    Mem Cached Min (MB): 2008
    Mem Cached Max (MB): 2010
    Mem Cached Avg (MB): 2008
    Thresholded: 0

    Time Collected: 2012-07-15T06:46:30.804
    Monitored Object: sys/switch-A/sysstats
    Suspect: No
    Load: 3.480000
    Load Min: 3.480000
```

show system uptime (connect fxos)

To display information about the system uptime for each configured system, use the **show system uptime** command.

show system uptime

Syntax Description

system uptime	Displays system uptime information.

Command Modes

connect fxos

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays system uptime for the configured system.

Example

This example shows how to display system uptime information:

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show system uptime
System start time:          Sun Jul 11 09:19:55 2021
System uptime:              89 days, 23 hours, 20 minutes, 21 seconds
Kernel uptime:              89 days, 23 hours, 22 minutes, 59 seconds
Active supervisor uptime:   89 days, 23 hours, 20 minutes, 21 seconds
```

show tech-support

To view or save troubleshooting information about the device hardware and software, use the **show tech-support** command.

`(module)#` **show tech-support**

`(local-mgmt)#` **show tech-support** { **chassis** *chassis_ID* | **fprm** | **module** *module_ID* [**app-instance** *application_name application_ID* | **brief** | **detail**] }

Syntax Description

	In module mode, this command has no arguments or keywords.
chassis *chassis_ID* [**brief** | **detail**]	Collects chassis-related troubleshooting data; the *chassis_ID* is always 1. The following options are available: • **brief** – Use this keyword to list a condensed set of troubleshooting information on your terminal. You can use the > and >> operators to save this information to a file; see Save Show Command Output, on page 17 for more information. • **detail** – Use this keyword to save detailed troubleshooting information to a file in the `techsupport` directory on the device. If you do not enter either keyword, the **brief** output is displayed on your terminal screen.
fprm [**brief** | **detail**]	The **fprm** option was deprecated in version 2.8(1) and can no longer be used.
module *module_ID* [**app-instance** *application_name application_ID* | **brief** | **detail**]	Collects troubleshooting data for the module specified by *module_ID*. The following options are available: • **app-instance** – In a multiple-instance environment, you can use this keyword to list information for the application instance specified by *application_name* and *application_ID*. • **brief** – Use this keyword to list a condensed set of troubleshooting information on your terminal. • **detail** – Use this keyword to list detailed troubleshooting information on your terminal. You can use the > and >> operators to save this information to a file; see Save Show Command Output, on page 17 for more information. If you do not enter a keyword, the **brief** output is displayed on your terminal screen.

Command Modes

connect local-mgmt

connect module

Command History

Release	Modification
1.1(1)	Command added.
2.4(1)	The **app-instance** keyword was added to the **module** option.
2.8(1)	The **fprm** option was deprecated in version 2.8(1) and can no longer be used. Use **show tech-support {chassis}** command instead.

Usage Guidelines

Use this command to view or save a collection of log messages, configuration information, and command output for transmission to Cisco Technical Assistance; this data is used to determine the status of the device hardware and software.

Use the **copy** command in local management mode to transfer a troubleshooting file to another device or location.

Note In module mode, this command simply lists the collected troubleshooting information for the specified module on your terminal

Examples

This example shows how to generate a file of detailed chassis-related troubleshooting information:

```
firepower # connect local-mgmt
Firepower(local-mgmt)# show tech-support chassis 1 detail

The show tech support file will be located at
/workspace/techsupport/20191105041703_firepower-9300_BC1_all.tar

Initiating tech-support information task on FABRIC A ...

Initiating tech-support information task on Chassis 1 Fabric Extender 1 ...
Initiating tech-support information task on Chassis 1 CIMC 1 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/1 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/1 ...
Initiating tech-support information task on Chassis 1 CIMC 2 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/2 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/2 ...
Completed initiating tech-support subsystem tasks (Total: 8)
Waiting (Timeout: 900 Elapsed: 30) for completion of subsystem tasks (1/8).
Waiting (Timeout: 900 Elapsed: 50) for completion of subsystem tasks (2/8).
Waiting (Timeout: 900 Elapsed: 70) for completion of subsystem tasks (5/8).
Waiting (Timeout: 900 Elapsed: 90) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 110) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 130) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 150) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 170) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 190) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 210) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 230) for completion of subsystem tasks (7/8).
--More--
The detailed tech-support information is located at workspace:///techsupport/201--More--
91105041703_firepower-9300_BC1_all.tar
```

This example shows how to save a file of troubleshooting information for the Security Module, and confirm its location on the device:

```
firepower # connect local-mgmt
firepower(local-mgmt)# show tech-support module 1 detail
The show tech support file will be located at
/workspace/techsupport/20191107082242_firepower-9300_BC_CIMC1.tar

Try connecting to Firepower-module 1...
Last login: Wed Oct 23 09:03:56 CDT 2019 from 127.128.254.1 on pts/0
Cisco Firepower Extensible Operating System (FX-OS) Software. TAC support:
http://www.cisco.com/tac Copyright (c) 2009-2016, Cisco Systems, Inc. All rights reserved.
 The copyrights to certain works contained in this software are owned by other third parties
 and used and distributed under license. Certain components of this software are licensed
under the 'GNU General Public License, version 3' provided with ABSOLUTELY NO WARRANTY under
 the terms of 'GNU General Public License, Version 3', available here:
http://www.gnu.org/licenses/gpl.html. See User Manual (''Licensing'') for details. Certain
 components of this software are licensed under the 'GNU General Public License, version
2' provided with ABSOLUTELY NO WARRANTY under the terms of 'GNU General Public License,
version 2', available here: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html. See User
 Manual (''Licensing'') for details. Certain components of this software are licensed under
 the 'GNU LESSER GENERAL PUBLIC LICENSE, version 3' provided with ABSOLUTELY NO WARRANTY
under the terms of 'GNU LESSER GENERAL PUBLIC LICENSE' Version 3, available here:
http://www.gnu.org/licenses/lgpl.html. See User Manual (''Licensing'') for details. Certain
 components of this software are licensed under the 'GNU Lesser General Public License,
version 2.1' provided with ABSOLUTELY NO WARRANTY under the terms of 'GNU Lesser General
Public License, version 2', available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html. See User Manual (''Licensing'') for
 details. Certain components of this software are licensed under the 'GNU Library General
Public License, version 2' provided with ABSOLUTELY NO WARRANTY under the terms of 'GNU
Library General Public License, version 2', available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html. See User Manual (''Licensing'') for
 details.


            Cisco Security Services Platform
                 Type ? for list of commands
Firepower-module1>support  send_diag_archive
Creating default Archive...
Archive created in 11 secs.
Starting to transfer Firepower-Module1_11_07_2019_08_22_44.tar of 5109760 bytes.
Transferred Firepower-Module1_11_07_2019_08_22_44.tar successfully to MIO at
/bladelog/blade-1/ in 1 sec(s).
Firepower-module1>support send_allcontainerlogs size 3063
Upload container logs triggered from Supervisor Module, Starting upload ....
No container instances running, skipping container logs

The detailed tech-support information is located at
workspace:/techsupport/Firepower-Module1_11_07_2019_08_22_44.tar
```

Running **show tech-support module 1|2|3 [detail]** may timeout when the blade is in offline or other error states. In such scenarios, please follow the below steps to collect the module tech-support (detail):

1. Connect to the intended blade by connect module 1|2|3 console|telnet

```
FPR4110# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit
```

2. Generate the Diag Bundle

```
Firepower-module1>support diagnostic

======= Diagnostic =======

 1. Create default diagnostic archive
 2. Manually create diagnostic archive
 3. Exit

Please enter your choice: 1

Creating Default archive

ASA running ...

Done with extracting tech support information from ASA. Log file saved as
asa_tech_support.log

1. Added file: cspCfg_cisco-asa.9.16.1__asa_001_JMX2309L046K6AY356.xml
2. Added file: tech_support_report.txt
3. Added file: ssp-cardmgmt.log
4. Added file: ssp_ntp.log.2
5. Added file: ssp_tz.log
6. Added file: ssp_ntp.log.1
7. Added file: ssp-pm.log
```

3. Copy the diag bundle to Supervisor(MIO)

```
Firepower-module1>support fileupload
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:1
-----------files------------
2021-09-29 17:24:36.571927 | 4065280    | Firepower-Module1_09_29_2021_17_23_17.tar
2021-09-29 17:27:34.094890 | 4065280    | Firepower-Module1_09_29_2021_17_26_15.tar
2021-09-29 17:24:38.211954 | 10240      |
Firepower-module1_09_29_2021_17_24_38_container.tar

([s] to select files or [x] to Exit):s

Type the partial name of the file to add, [<] to cancel
> Firepower-Module1_09_29_2021_17_26_15.tar
Firepower-Module1_09_29_2021_17_26_15.tar
Are you sure you want to add these files? (y/n) y
=== Package Contents ===
[Added] Firepower-Module1_09_29_2021_17_26_15.tar
========================

Type the partial name of the file to add, [<] to cancel
> <
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:3
Transfer of Firepower-Module1_09_29_2021_17_26_15.tar started.
Firepower-module1>support fileupload
Please choose from following:
```

```
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:4
File Transfer Status:
--------------------------------------------
Firepower-Module1_09_29_2021_17_26_15.tar       Status: Completed.
```

4. Exit out of Module console with ~ and exit, locate the file in MIO

```
Firepower-module1>
telnet> quit
Connection closed.
FPR4110# connect local-mgmt
FPR4110(local-mgmt)# dir workspace:/bladelog/blade-1/
<>
1 4065280 Sep 29 17:30:04 2021 Firepower-Module1_09_29_2021_17_26_15.tar <---
<>
```

Related Commands

Command	Description
copy	In local management mode, makes a copy of the specified file.
dir	In local management mode, lists the contents of the current directory.

show timezone

To display the currently configured time zone, use the **show timezone** command.

show timezone

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to display the current time zone:

```
FP9300-A# show timezone
Timezone: America/Chicago
FP9300-A#
```

Related Commands

Command	Description
set timezone	Sets the time zone for the device.

show trustpoint

To show the list (or chain) of certificates for all trustpoints, or for a specific trustpoint, use the **show trustpoint** command.

show trustpoint [**detail** | *trustpoint_name*]

Syntax Description

detail	Shows detailed certificate information.
trustpoint_name	Shows certificate information for the specifed trustpoint. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Command Modes

Security mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to display trusted point certificate information.

You can also use the **show** command in trustpoint (/security/trustpoint) mode to view certificate information for the connected trustpoint.

Example

This example shows how to display certificate information for a specific trustpoint:

```
FP9300-A# scope security
FP9300-A /security # show trustpoint CHdefault

Trustpoint CA:
    Trustpoint Name Trustpoint certificate chain Cert Status
    --------------- ---------------------------- -----------
    CHdefault       -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
MAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2ln
biwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJp
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
aXR5IC0gRzUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1
nmAMqudLO07cfLw8RRy7K+D+KQL5VwijZIUVJ/Xxrcgxi V0i6CqqpkKzj/i5Vbex
t0uz/o9+B1fs70PbZmIVYc9gDaTY3vjgw2IIPVQT60nKWVSFJuUrjxuf6/WhkcIz
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
```

```
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
MzEzMA0GCSqGSIb3DQEBBQUAA4IBAQCTJEowX2LP2BqYLz3q3JktvXf2pXkiOOzE
p6B4Eq1iDkVwZMXnl2YtmAl+X6/WzChl8gGqCBpH3vn5fJJaCGkgDdk+bW48DW7Y
5gaRQBi5+MHt39tBquCWIMnNZBU4gcmU7qKEKQsTb47bDN0lAtukixlE0kF6BWlK
WE9gyn6CagsCqiUXObXbf+eEZSqVir2G3l6BFoMtEMze/aiCKm0oHw0LxOXnGiYZ
4fQRbxC1lfznQgUy286dUV4otp6F01vvpX1FQHKOtw5rDgb7MzVIcbidJ4vEZV8N
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
 Valid

FP9300-A /security #
```

Command	Description
set certchain	Enters a list (or chain) of certificates for a trustpoint.
set trustpoint	Sets the certificate trustpoint for a keyring.

show user-sessions

To display information about the local and the remote user sessions, use the **show user-sessions** command.

show user-sessions

Command Modes

scope security

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

By default, this command displays user sessions information.

Example

This example shows how to display the local and remote user sessions information:

```
firepower# scope security
firepower /security # show user-sessions local
Session Id      User            Host                Login Time
--------------- --------------- ------------------- ----------
pts_0_1_24360*  admin           192.0.2.1           2021-10-11T20:46:16.000


firepower# show user-sessions local detail
Session Id pts_0_1_24360*:
    Fabric ID: A
    Term: pts/0
    User: admin
    Host: 192.0.2.1
    Pid: 24360
    Login Time: 2021-10-11T20:46:16.000
    Refresh Period (in secs): 0
    Session Timeout (in secs) for web, ssh, telnet sessions: 0
    Absolute Session Timeout (in secs) for web, ssh, telnet sessions: 0


firepower /security # show user-sessions remote

Session Id      User            Host                Login Time
--------------- --------------- ------------------- ----------
pts_1_1_9578    test1           192.0.2.2           2021-10-11T21:39:52.000


firepower /security # show user-sessions remote detail
Session Id pts_1_1_9578:
    Fabric ID: A
    Term: pts/1
    User: test1
    Host: 192.0.2.2
    Pid: 9578
    Login Time: 2021-10-11T21:39:52.000
    Refresh Period (in secs): 0
    Session Timeout (in secs) for web, ssh, telnet sessions: 0
    Absolute Session Timeout (in secs) for web, ssh, telnet sessions: 0
```

show validate-task

To check the status of a manually initiated image verification, use the **show validate-task** command.

show validate-task [**detail** | **fsm** | *pack_version*]

Syntax Description

detail	(Optional) Displays detailed package status information for all available platform packages.
fsm status	(Optional) Lists the finite state machine validation status. The **expand** keyword and the *pack_version* variable are also available.
pack_version	(Optional) Displays validation information for the specified package. The **detail** keyword is also available with this option.

Command Modes

Firmware mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

If you do not include a *pack_version*, the **show validate-task** command lists information for every firmware image on the appliance.

You can use this command or the **show validation package** command to determine the desired package version number.

Example

This example shows how to show validation history for a specific firmware package:

```
FP9300-A# scope firmware
FP9300-A /firmware # show validate-task 2.3(1.51)

Validate task:
    Pack Name: fxos-k9-bundle-infra.2.3.1.51.SPA
    Pack Version: 2.3(1.51)
    Validation Time Stamp: Never
    Validation State: None
    Overall Status String:

    Pack Name: fxos-k9-bundle-server.2.3.1.51.SPA
    Pack Version: 2.3(1.51)
    Validation Time Stamp: Never
    Validation State: None
    Overall Status String:

    Pack Name: fxos-k9.2.3.1.51.SPA
    Pack Version: 2.3(1.51)
    Validation Time Stamp: 2017-10-25T16:53:30.914
    Validation State: None
    Overall Status String: Ok
```

```
FP9300-A /firmware #
```

Related Commands

Command	Description
download image	Downloads an FXOS software image to the Firepower 4100/9300 chassis.
verify platform-pack	Verifies the integrity of a downloaded FXOS platform bundle.

show version

To display the current system software-version information, use the **show version** command.

show version [**detail**]

To display software-version and status information for all the chassis components, use the **show version** command in chassis mode.

show version [**detail** | **package-version**]

To display software-version and status information for a server's components, use the **show version** command in server mode. In server mode, you also can show version information for individual components.

show version [**adapter** | **bios** | **boardcontroller** | **cimc** | **detail** | **fxos** | **package-version** | **storage** |]

Syntax Description

adapter	(Optional) Show version information for adapters installed in the connected server. This keyword is available only in server mode.
bios	(Optional) Show BIOS version information for the connected server. This keyword is available only in server mode.
boardcontroller	(Optional) Show Management Controller version information for the connected server. This keyword is available only in server mode.
cimc	(Optional) Show CIMC version and status information for the connected server. This keyword is available only in server mode.
detail	(Optional) Show additional verison information.
fxos	(Optional) Show SSP operating system version information for the connected server. This keyword is available only in server mode.
package-version	(Optional) Show only package-verison information. This keyword is available only in adapter, chassis, fabric-interconnect, server, and system modes.
storage	(Optional) Show version information for RAID and local disk controllers for the connected server. This keyword is available only in server mode.

Command Modes

Any command mode – shows system software-version information

Chassis mode – shows software-version and status information for all chassis components

Server mode – shows software-version and status information for the connected server's components

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The **package-version** keyword is available only in adapter, chassis, fabric-interconnect, server, and system modes.

In fabric-interconnect mode, this command displays additional version information; see the following example.

Examples

This example shows how to display detailed management-system version information:

```
FP9300-A# show version detail
FPRM:
    Running-Vers: 4.2(1.62)
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready
    Startup-Vers: 4.2(1.62)

FP9300-A#
```

This example shows how to display version information in fabric-interconnect mode:

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect #show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.31.60)
    Running-Sys-Vers: 5.0(3)N2(4.31.60)
    Package-Vers: 2.3(1.51)
    Startup-Kern-Vers: 5.0(3)N2(4.31.60)
    Startup-Sys-Vers: 5.0(3)N2(4.31.60)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:

FP9300-A /fabric-interconnect #
```

This example shows how to display chassis-component version information:

```
FP9300-A# scope chassis 1
FP9300-A /chassis # show version detail
Chassis 1:
    Server 1:
        CIMC:
            Running-Vers: 3.1(23a)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready

        Adapter 1:
            Running-Vers: 4.0(1.67)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready
            Bootloader-Update-Status: Ready
        Adapter 2:
            Running-Vers: 4.0(1.67)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready
            Bootloader-Update-Status: Ready
        BIOS:
            Running-Vers: FXOSSM1.1.2.1.6.072020171212
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready

        SSP OS:
```

```
            Running-Vers: 2.3(1.50)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status:

        RAID Controller 1:
            Running-Vers: 24.12.1-0203|6.30.03.0|NA
            Package-Vers: 2.3(1.51)
            Activate-Status: Ready

        BoardController:
            Running-Vers: 14.0
            Package-Vers: 2.3(1.51)
            Activate-Status: Ready

        Local Disk 1:
            Running-Vers: EM14
            Package-Vers:
            Activate-Status: Ready

        Local Disk 2:
            Running-Vers: EM14
            Package-Vers:
            Activate-Status: Ready

    Server 2:
        CIMC:
            Running-Vers: 3.1(23a)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready

    <--- remaining lines removed for brevity --->

FP9300-A /chassis #
```

Related Commands

Command	Description
show server version	Shows current server software versions and status information.

shutdown

To shutdown the device, use the **shutdown** command.

shutdown [**no-prompt** | *reason*]

Syntax Description

no-prompt	(Optional) Use this keyword to initiate shutdown immediately. Otherwise, a **commit-buffer** is required to initiate shutdown.
reason	(Optional) A text string to be appended to the shutdown log; can be up to 510 characters.

Command Modes

Chassis mode

Local management mode: obsolete

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

We recommend backing up the system configuration before shutting down.

This command is obsolete in local management mode; use **shutdown** in chassis mode.

Example

This example shows how to enter chassis mode and shut the system down:

```
Firepower # scope chassis 1
Firepower /chassis # shutdown no-prompt
Starting chassis shutdown. Monitor progress with the command "show fsm status".
Please set the power switch to the off position after "INIT: no more processes left in this
 runlevel" message is seen.
Firepower /chassis #
Broadcast message from root@Firepower (Tue Jul 14 11:40:47 2020):

All shells being terminated due to system /sbin/shutdown

Cisco FPR Series Security Appliance
INIT: Sending processes the TERM signal
Jul 14 11:40:53 %TTYD-2-TTYD_ERROR TTYD Error ttyd bad select

INIT: no more processes left in this runlevel
```

Related Commands

Command	Description
reboot	Restarts the chassis or fabric-interconnect.

show web-session-limits

To display a list of web sessions available on the system, use the **show web-session-limits** command.

show validate-task [**detail**]

Syntax Description

Detail	Displays list of detailed web session limits.

Command Modes

scope system/scope services

Command History

Release	Modification
2.3.1	Command added.

Usage Guidelines

This is a subcommand of the **show** command in scope system, scope services

Example

This example shows how to display information of system web session limits:

```
Firepower /fabric-interconnect # scope system
Firepower /system # scope services
Firepower /system/services # show web-session-limits

Web Sessions:
    Maximum logins for single user Maximum Sessions
    ------------------------------ ----------------
    32                             256
```

Example

This example shows how to display detailed information of the available web sessions detail:

```
Firepower /system/services # show web-session-limits detail

Web Sessions:
    Maximum logins for single user: 32
    Maximum Sessions: 256
```

PART III

T – W Commands

T – W Commands

terminal

To set the number of lines, and the width of the lines, displayed in the terminal window, use the **terminal** command.

terminal {**length** *lines* | **width** *characters*}

Syntax Description

length *lines*	The number of lines displayed in the terminal window. Valid values range from 0 to 511 lines. Enter 0 to eliminate pausing.
width *characters*	The number of characters per line displayed in the terminal window. Valid values range from 24 to 511 characters.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to set the number of lines, and the number of characters per line, to be displayed in the terminal window.

Example

This example shows how to set the number of lines displayed in the terminal window to 12:

```
FP9300-A# terminal length 12
FP9300-A *# commit-buffer
FP9300-A#
```

Related Commands

Command	Description
set cli	Specifies whether command output lines wrap or truncate, whether table headers are displayed, and whether commas or spaces are used to separate fields in command output tables.

top

To enter root (EXEC) from any mode, use the **top** command.

top

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to enter root from any mode:

```
FP9300-A /system/services # top

FP9300-A#
```

Related Commands

Command	Description
up	Moves up one mode.

traceroute (connect local-mgmt)

To trace the route to another device on the network using its host name or IPv4 address, use the **traceroute** command.

traceroute {*hostname* | *IPv4_address*} [**source** *header_IP*]

Syntax Description

hostname | *IPv4_address*	The host name or IP address of the network device to be contacted. The maximum number of characters allowed for the host name is 510.
source *header_IP*	(Optional) Use this keyword to specify the device IP address to be included in the packet headers.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to trace the route of IP packets to a network host.

If you do not specify the **source** IP address to be included in the packet headers, the management port address is used.

Example

This example shows how to connect to the local management CLI and then trace the route to another device on the network:

```
firepower# connect local-mgmt
firepower(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1  198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

firepower(local-mgmt)#
```

Related Commands

Command	Description
ping	Pings the device at a specified destination (IPv4 address).

traceroute6 (connect local-mgmt)

To trace the route to another device on the network using its host name or IPv6 address, use the **traceroute6** command.

traceroute6 {*hostname* | *ipv6_address*} [**source** *header_ip*]

Syntax Description

hostname | *ipv6_address*	The host name or IPv6 address of the network device to be contacted. The maximum number of characters allowed for the host name is 510.
source *header_ip*	(Optional) Use this keyword to specify the device IP address to be included in the packet headers.

Command Modes

connect local-mgmt

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

Use this command to trace the route of IP packets to a network host.

If you do not specify the **source** IP address to be included in the packet headers, the management port address is used.

Example

This example shows how to connect to the local management CLI and then trace the route to another device on the network:

```
firepower# connect local-mgmt
firepower(local-mgmt)# traceroute 2001:DB8:1::1
traceroute to 2001:DB8:1::1 (2001:DB8:1::1), 30 hops max, 40 byte packets
 1  2001:DB8:1::4 (2001:DB8:1::4)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (2001:DB8:1::6)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (2001:DB8:1::8)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (2001:DB8:1::7)  0.336 ms  0.267 ms  0.289 ms

firepower(local-mgmt)#
```

Related Commands

Command	Description
ping6	Pings the device at a specified destination (IPv6 address).

up

To move up one level in the command-mode hierarchy, use the **up** command.

up

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to move up one mode:

```
FP9300-A /org/service-profile # up
FP9300-A /org #
```

Related Commands

Command	Description
exit	Exits the current CLI session and disconnects from the device, or exits from a connected object mode and returns to the root (EXEC) level.
top	Enters root (EXEC) from any mode.

verify platform-pack

To manually verify the integrity of a downloaded FXOS platform bundle, use the **verify platform-pack** command.

verify platform-pack **version** *version_number*

Syntax Description

version *version_number*	Specifies the version number of the platform package to verify.

Command Modes

Firmware mode

Command History

Release	Modification
1.1(1)	Command added.

Usage Guidelines

The integrity of the image is automatically verified when a new image is downloaded to the Firepower 4100/9300 chassis; use this command to later manually verify the integrity of a downloaded image.

You can use the **show validate-task** or the **show validation package** command to determine the desired package version number.

You also can use the **show validate-task** command to monitor the verification process. The output display does not refresh automatically, so you may have to enter the command multiple times.

Example

This example shows how to verify a specific platform package:

```
FP9300-A# scope firmware
FP9300-A /firmware # show validation package
Firmware Package 2.2(2.19):
    Validation Time Stamp: 2017-10-26T14:34:24.925
    Pack Name: fxos-k9.2.2.2.19.SPA
    Validation State: None
    Overall Status Code: Ok

Firmware Package 2.3(1.51):
    Validation Time Stamp: 2017-10-25T16:53:30.914
    Pack Name: fxos-k9.2.3.1.51.SPA
    Validation State: None
    Overall Status Code: Ok
FP9300-A /firmware # verify platform-pack version 2.3(1.51)
The currently installed FXOS platform software package is 2.3(1.51)
All the Security Modules will be installed with these software components:
    Security Module Adapter  4.0(1.67)
    Security Module BIOS     FXOSSM2.1.3.1.13.0927171811
    Security Module FXOS     2.3(1.50)

INFO: There is no service impact to install this FXOS platform software 2.3(1.51)


Verifying FXOS platform software package 2.3(1.51). Verification could take several minutes.
Do you want to proceed? (yes/no) [yes]:
```

Related Commands

Command	Description
download image	Downloads an FXOS software image to the Firepower 4100/9300 chassis.
show validate-task	Displays the status of the image verification process.

where

To determine where you are in the CLI command hierarchy, use the **where** command.

where

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
1.1(1)	Command added.

Example

This example shows how to determine where you are in the CLI:

```
FP9300-A /org/service-profile # where
Mode: /org/service-profile
Mode Data:
       scope org
       enter org org10
       enter service-profile sp10 instance
FP9300-A /org/service-profile #
```

Related Commands

Command	Description
top	Moves to top (EXEC) level from any mode.
up	Moves up one mode.

where

PART IV

connect *shell* Commands

connect *shell* Commands

connect adapter: Command List

After you have used the Supervisor **connect adapter** command to connect to the command shell for a specific adapter, the following commands are available in that shell. See connect adapter, on page 40 for information about the **connect adapter** command.

Attention These commands should be used only when troubleshooting virtualized network adapters with Cisco TAC supervision.

Note that when you connect to an adapter command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to `adapter n/n/n`, where `n/n/n` is the adapter's chassis/server/ID combination you entered to connect.

To exit adapter mode, type **exit**.

Example

The following example shows how to connect to the adapter command shell, and view available commands:

```
firepower# connect adapter 1/2/1
adapter 1/2/1 # help
Available commands:
  connect             - Connect to remote debug shell
  exit                - Exit from subshell
  help                - List available commands
  history             - Show command history
  show-fwlist         - Show firmware versions on the adapter
  show-identity       - Show adapter identity
  show-phyinfo        - Show adapter phy info
  show-systemstatus   - Show adapter status
adapter 1/2/1 # exit
firepower#
```

Table 6: Commands Available in the Adapter's Primary Command Shell

Command	Additional Information
connect	Connects to the debug shell; provides access to the commands listed in the following table.
exit	Exits from the adapter command shell.
help	Lists the commands available in this shell.
history	Shows a list of commands issued since entering this shell.
show-fwlist	Shows firmware versions on the adapter.

Command	Additional Information
show-identity	Show adapter identity
show-phyinfo	Show adapter phy info
show-systemstatus	Show adapter status

The following commands are available in the debug subshell; accessed by entering the **connect** command in the adapter's primary command shell.

Note When you connect to an adapter shell's debug subshell, the command-line prompt changes from the `adapter n/n/n` prompt, to `adapter n/n/n (top):n`, where `(top):` indicates you are in the top subshell of the adapter command shell, and `n` represents the number of command lines presented thus far in this debug session.

To exit the debug subshell, type **exit**.

Example

The following example shows how to connect to the adapter's debug subshell, and view available commands:

```
adapter 1/2/1 # connect
No entry for terminal type "dumb";
using dumb terminal settings.
adapter 1/2/1 (top):1# help
Available commands:
  attach-fls      - Attach to fls
  attach-mcp      - Attach to mcp
  estat           - Run fc performance monitor
  exit            - Exit from subshell
  help            - List available commands
  history         - Show command history
  phy-read        - Read PHY register
  show-acltab     - Show ACL table
  show-fru        - Show FRU contents
  show-fwdtab     - Show forwarding table
  show-log        - Show system log
  show-macstats   - Show MAC statistics
  show-pcisw      - Show PCIE switch status
adapter 1/2/1 (top):2# exit
adapter 1/2/1 #
```

Table 7: Commands Available in the Adapter Debug Subshell

Command	Additional Information
attach-fls	Attaches to the adapter's fabric login service; provides access to the commands listed in a following table.
attach-mcp	Attaches to the Master Control Program. A large number of debug-information commands are available; use the **help** command to view a list. Again, these commands are for use only with Cisco TAC guidance.
estat	Launches a Fibre Channel performance monitor.
exit	Exits from this subshell.
help	Lists the commands available in this subshell.
history	Shows a list of commands issued since entering this subshell.
phy-read	Read PHY register
show-acltab	Show ACL table
show-fru	Show FRU contents
show-fwdtab	Show forwarding table
show-log	Show system log
show-macstats	Show MAC statistics
show-pcisw	Show PCIE switch status

The following commands are available in the Fabric Login Service (FLS) subshell; accessed by entering the **attach-fls** command in the adapter's debug shell.

Note When you connect to the FLS subshell of an adapter's debug subshell, the command-line prompt changes from `adapter n/n/n (top):n`, to `adapter n/n/n (fls):n` where `(fls):` indicates you are in the FLS subshell of the debug subshell, and *n* represents the number of command lines presented thus far in this FLS session.

To exit the FLS subshell, type **exit**; you are returned to the debug subshell.

Example

The following example shows how to attach to the FLS subshell from the debug subshell, and view available commands:

```
adapter 1/2/1 # connect
No entry for terminal type "dumb";
```

```
using dumb terminal settings.
adapter 1/2/1 (top):1#  attach-fls
No entry for terminal type "dumb";
using dumb terminal settings.
adapter 1/2/1 (fls):1# help
Available commands:
         d - dumps the contents of the last fw request
      exit - Exit from subshell
  fwactive - retrieve active fcpu exchanges
     fwcqs - retrieves fcpu cq information
    fwexch - retrieves fcpu exchange data
     fwlif - retrieves fcpu lif data
    fwvnic - retrieves fcpu vnic data
      help - List available commands
   history - Show command history
       lif - Show lif information
     login - Show login information pertaining to vnic
   lunlist - Show Nameserver and Report LUN's response information for vnic
    lunmap - Show lunmap information pertaining to vnic
      vnic - Show vnic information

adapter 1/2/1 (fls):2# exit
adapter 1/2/1 (top):2#
```

Table 8: Commands Available in the FLS Subshell

Command	Additional Information
d	Dumps the contents of the last firmware request.
exit	Exits from the FLS subshell.
fwactive	Retrieves active fcpu exchanges
fwcqs	Retrieves fcpu cq information
fwexch	Retrieves fcpu exchange data
fwlif	Retrieves fcpu lif data
fwvnic	Retrieves fcpu vnic data
help	Lists available commands
history	Shows command history
lif	Shows lif information
login	Shows login information pertaining to vnic
lunlist	Shows Nameserver and Report LUN's response information for vnic
lunmap	Shows lunmap information pertaining to vnic
vnic	Shows vnic information

connect cimc: Command List

After you have used the Supervisor **connect cimc** command to connect to the CIMC firmware debug utility for a specific module, the following commands are available in that shell. See connect cimc, on page 44 for information about the **connect cimc** command.

This utility provides access to a read-only shell with commands that let you view real-time CIMC debug information. These commands are used mainly for troubleshooting CIMC issues: viewing alarms, system event logs, on-board failures, and power controls.

Note When you connect to the CIMC command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to `[ xxx ]`, where *xxx* is the last command you entered; see the following example.

To exit the CIMC shell, type **exit**.

Example

The following example shows how to connect to CIMC mode and then list the available commands:

```
firepower# connect cimc 1/1
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.

CIMC Debug Firmware Utility Shell [ support ]
[ help ]# help
_____________________________________________
          Debug Firmware Utility
_____________________________________________
Command List
_____________________________________________
alarms
cores
dimmbl
exit
i2cstats
images
mctools
memory
messages
mrcout
network
obfl
post
power
programmables
sensors
sel
fru
tasks
top
update
users
version
```

```
cert
sldp
help
help [COMMAND]

_____________________________________
 Notes:
"enter Key" will execute last command
"COMMAND ?" will execute help for that command
_____________________________________
[ help ]# power
OP:[ status ]
Power-State:                 [ on ]
Master-State:                [ Master ]
VDD-Power-Good:              [ active ]
Power-On-Fail:               [ inactive ]
Power-Ctrl-Lock:             [ unlocked ]
Power-System-Status:         [ Good ]
Front-Panel Power Button:    [ Disabled ]
Front-Panel Reset Button:    [ Disabled ]
Source of Last Power Change: [ Software - "mcserver" ]
OP-CCODE:[ Success ]
[ power ]# exit
Connection closed by foreign host.
firepower#
```

Table 9: Commands Available in the CIMC Debug Shell

Command	Additional Information
alarms	Displays the current StatusLED state, and which sensors are in alarm, if any. Alarm Levels: 1 - OK (GREEN ON) 2 - Mem Init (GREEN BLINK) 3 - Mild Fault (AMBER ON) 4 - Severe Fault (AMBER BLINK)
cores	Lists the Core Dump Directory.
exit	Exits from the CIMC subshell.
fru	Lists all field-replaceable unit (FRU) device information.
help [COMMAND]	Entering just the command **help** lists all available commands. Entering **help** *cmd_name*, or *cmd_name* **?**, shows help information for the specfied command.
i2cstats	Displays I^2C controller register information, driver counters, and multi-primary debug trace data.
images	Displays software image version and status information.
mctools	Displays current MCtools state information: socket and share-file cache size information.

Command	Additional Information
memory	Lists memory and load statistics.
messages	messages [dump|follow|tail] dump - Dump the /var/log/messages file follow - Tail and Follow /var/log/messages file tail - Dump the last 100 messages
mezz1fru	Show the mezz card 1 FRU information
mezz2fru	Show the mezz card 2 FRU information
mrcout	Dump MrcOut*.txt
network	view network status in realtime ; Dump Network information
obfl	Dump the OBFL - on-board fault log dump - Dump OBFL follow - Tail and Follow OBFL tail - Dump the last 100 messages
post	Dump BIOS Post Information
power	view power status in realtime Dump Blade Power Status
programmables	Dump Board Programmable Versions
sensors	view all sensors in realtime sensors [all|power|temp|fault|pres|led] all - Dump all Sensors (default) power - Dump only Power Sensors temp - Dump only Temprature Sensors fault - Dump only Fault Sensors pres - Dump only Presence Sensors led - Dump only LED Sensors
sel	Show the Blade SEL Information - system event log
sldp	Cisco CIMC Interactive Debug This command performs interactive debug authentication with the aid of the user and Cisco support personnel.
tasks	Dump Running Task Information

Command	Additional Information
top	Run TOP Process Monitoring
update	Current Firmware Update Status
users	Dump IPMI Users
version	Get the Version Information

connect fxos: Command List

After you have used the Supervisor **connect fxos** command to connect to the FXOS CLI shell for the switching fabric, the following commands are available in that shell. See connect adapter, on page 40 for information about the **connect fxos** command.

Note When you connect to the FXOS command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to the default prompt with `(fxos)` appended; see the following example.

To exit the FXOS shell, type **exit**.

Example

The following example shows how to connect to the FXOS command shell, and view available commands:

```
firepower# connect fxos
firepower(fxos)# ?
  clear         Reset functions
  cli           CLI commands
  debug         Debugging functions
  debug-filter  Enable filtering for debugging functions
  ethanalyzer   Configure cisco packet analyzer
  no            Negate a command or set its defaults
  ntp           NTP configuration
  show          Show running system information
  system        System management commands
  terminal      Set terminal line parameters
  test          Test command
  undebug       Disable Debugging functions (See also debug)
  end           Go to exec mode
  exit          Exit from command interpreter
  pop           Pop mode from stack or restore from name
  push          Push current mode to stack or save it under name
  where         Shows the cli context you are in

firepower(fxos)# exit
firepower#
```

Table 10: Commands Available in the FXOS Shell for the Switching Fabric

Command	Additional Information
clear	Reset functions counters - Clear counters logging - Clear logging information mac - MAC

Command	Additional Information
cli	CLI commands var - Define a variable
debug	Debugging functions; see following table
debug-filter	Enable filtering for debugging functions ip - IP events ipv6 - IPv6 events pktmgr - Pm debug-filter routing - Routing events
ethanalyzer	Configure Cisco packet analyzer local - Start local capture of frames to Sup
no	Negate a command or set its defaults debug - Debugging functions debug-filter - Enable filtering for debugging functions ethanalyzer - Configure cisco packet analyzer terminal - Set terminal line parameters test - Test command
ntp	NTP configuration sync-retry - Retry synchronization with configured servers
show	Show running system information; see following table
system	System management commands hap-reset - Enables resetting of local or remote sup on ha failures heartbeat - Enables heartbeat no - Negate a command or set its defaults
terminal	Set terminal line parameters; see the following table
test	Test command aaa - Aaa authentication eltm - Display eltm information forwarding - Fib information hardware - Test hardware parameters otv

Command	Additional Information
undebug	Disable Debugging functions (See also debug) all - Disable all debugging icmpv6 - ICMPv6 debug commands ip - IP events ipv6 - IPv6 events l2 - Layer2 l3vm - Debug L3VM information pktmgr - Packet manager debug/tunnel information rpm - Route Policy Manager (RPM) sockets - Sockets system - Enable debugging of system components
end	Go to exec mode
exit	Exit from command interpreter
pop	Pop mode from stack or restore from name *name* – Name (optional)
push	Push current mode to stack or save it under name *name* – Name (optional)
where	Shows the cli context you are in detail – Shows each entry on separate line (optional)

Table 11: Debug, Show and Terminal Commands Available in the FXOS Command Shell

Command	Additional Information
debug	

Command	Additional Information
	Debugging functions aaa – Enable debugging for aaa aclcomp – Configure aclcomp debug acllog – Configure acllog debug aclmgr – Configure aclmgr debug afm – Configure afm debug assoc – Original ID to Translated ID Association bcm-usd – BCM USD bootvar – Enable bootvar debugging callhome – Enable debugging for Callhome cdp – Configure CDP debugging cert-enroll – Configure debugging for cert enroll daemon cfs – Enable debugging for CFS cli – Debug cli clis – Debug cli server clk_mgr – Configure clk_mgr debug copp – Configure copp debug core – Configure core daemon debugging csm – Enable csm debugs device-alias – Configure debugs for Device Alias Distribution Service dstats – Configure delta statistics debugging eltm – Configure eltm debug ethpc – Configure ethpc debug ethpm – Configure ethpm debug evmc – Event manager client debugs fc-mac – Debug fcp information fc2 – Configure FC2 debugging fc2d – Configure fc2d debug fcdomain – Enable fcdomain debugging fcfwd – Enable fcfwd debugging fcns – Debug name server fcoe_klm – Configure FCOE_KLM debugging fcpc – Configure fcpc debug

Command	Additional Information
	fcs – Configure Fabric Configuration Server Debugging fdmi – Configure fdmi debugging fex – Debug cli for FEX process fex – Configure fex debug flogi – Configure flogi debug fm – Configure feature manager debugging fspf – Configure FSPF debugging hardware – Debug hardware,kernel loadable module parameters icmpv6 – ICMPv6 debug commands idehsd – Configure Idehsd handler debugging im – Configure im debug ip – IP events ipconf – Configure ipconf debug ipfib – Configure ipfib debug ipqos – Configure IP QoS Manager debug ipv6 – IPv6 events klm – Debug kernel loadable module parameters l2 – Layer2 l3vm – Debug L3VM information lacp – Configure lacp debug ldap – Configure debugging for ldap ledmgr – Configure LED manager debugging license – Enable debugging for Licensing lldp – Configure lldp debug logfile – Direct debug output to logfile logging – Configure logging or syslogd debug m2rib – Configure m2rib debug mcec – Configure MCEC debugging mcm – Configure mcm debug mfdm – Configure mfdm debug monitor – Configure Ethernet SPAN sessions msp – Configure msp debug mvsh – MVSH server debugs

Command	Additional Information
	nf – Configure nf debug nohms – Configure nohms debug npacl – Configure NPACL feature nsmgr – Configure nsmgr debug ntp – Debug NTP module obfl – Configure obfl debugging pfm – Configure pfm debug pfstat – Configure pfstat debug pktmgr – Packet manager debug/tunnel information platform – Configure platform debugging platform – Platform internal information platform – Platform plog – Configure plog debugging pltfm_config – Configure pltfm_config debug plugin – Configure plugin debug port – Configure port debugging port-channel – Configure port-channel debug port-profile – Enable port-profile manager debugs port-resources – Configure prm debug port-security – Port security related command private-vlan – Configure debug flags for private VLAN process-sap – SAP of the process to be debugged provision – Configure provision debug psshelper – Psshelper debug psshelper_gsvc – Psshelper debug ptplc – Configure ptplc debug qd – Show information about qd radius – Configure debugging for radius daemon res_mgr – Configure res_mgr debug rib – Configure rib debugging rlir – Configure RLIR debugging rpm – Route Policy Manager (RPM) rscn – Configure RSCN debugging

Command	Additional Information
	sal – Configure sal debug san-port-channel – Configure san-port-channel debug scsi-target – Configure scsi target daemon debugging security – Configure debugging for security session-mgr – Enable session manager debugs snm – Configure snm debug snmp – Configure snmp-server Debugging sockets – Sockets spm – Configure spm debug statsclient – Stats system – Enable debugging of system components system – Debug system tacacs+ – Configure debugging for TACACS+ track – Configure track debug transceiver – FC transceiver debug commands tunnel – Configure tunnel debug udld – Configure udld debug **Note** Unidirectional link detection (UDLD) is not supported by FXOS; ignore any references to UDLD. ufdm – Configure ufdm debug vim – Configure vim debug vlan – Configure debug flags for vlan manager vmm – Configure vmm debug vms – Configure vms debug vsan – Enable VSAN manager debugging willesden – Configure willesden debugging wwn – Configure WWN Manager Debugging xml – XML agent zone – Zone server debug commands zschk – Configure zschk debug

Command	Additional Information
show	

Command	Additional Information
	Show running system information aaa – Show aaa information access-lists – List access lists accounting – Show accounting configuration banner – Show current motd banner message boot – Show Bootvar Variables callhome – Show callhome information cdp – Show Cisco Discovery Protocol information cfs – CFS Show Command handler class-map – Show class maps cli – Show CLI information clock – Display current Date cluster-state – View cluster state configuration – Show information about configuration sessions copyright – Copyright information debug – Show debug flags device-alias – Show information about Device Alias Distribution Service diagnostic – Diagnostic commands ecmp-groups – Display all ECMP groups environment – System environment information fc2 – Show fc2 tables and statistics fc2d – Show information about fc2d fcalias – Fcalias show commands fcdomain – Show fcdomain information fcdroplatency – Show switch or network latency fcflow – Show fcflow information fcid-allocation – Show information about fcid-allocation list fcns – Show name server tables fcroute – Show FC routes fcs – Show Fabric Configuration Server Information fctimer – Show Fibre Channel timers fdmi – Show fdmi information flogi – Show information about FLOGI

Command	Additional Information
	fp – Fp fspf – Show information about FSPF hardware – Show hardware information hostname – Show the system's hostname hosts – Show information about DNS in-order-guarantee – Show in-order delivery guarantee configuration incompatibility – Show incompatible configurations install – Show the software install impact between two images interface – Show interface status and information inventory – Show physical inventory ip – Display IP information ip – IP information ipmc-groups – Display all IPMC groups ipv6 – Display IPv6 information klm – Show kernel module information l2-class-id – L2 class ID allocation l2-table – Display all L2 entries lacp – Show LACP information ldap-server – Show LDAP configuration information line – Show the line configuration lldp – Show information about lldp loadbalancing – Show unicast loadbalancing of a certain flow or exchange locator-led – Display locator led status on the device logging – Show logging configuration and contents of logfile mac – MAC module – Show module information monitor – Show Ethernet SPAN information msp – Msp commands nsm – Show Network Segment Manager information ntp – Show NTP information phy-bypass – Hardware Bypass platform – Shows list of events received by Platform Manager policy-map – Show policy maps

Command	Additional Information
	port – Show port information port-channel – Show port-channel information port-profile – Show port-profile port-security – Port security related command queuing – Show interface queuing information radius-server – Show RADIUS configuration information redundancy – Show system redundancy status resource – Show resource configuration for VDC rlir – Show RLIR information rmon – Display RMON statistics role – Show role configuration routing – Display routing information routing-context – Display the current routing context rscn – Show RSCN information running-config – Current running configuration san-port-channel – Show port-channel information scsi-target – Show discovered scsi target information snmp – Show snmp information sprom – SPROM contents ssh – Show SSH information startup-config – Current startup configuration svs – Show svs information switchname – Show the system's hostname system – System-related show commands tacacs-server – Show TACACS+ configuration information tech-support – Gather information for troubleshooting telnet – Show telnet server configuration terminal – Display terminal configuration parameters topology – Show information of connected switches track – Tracking information trunk – Show trunk information udld – UDLD protocol

Command	Additional Information
	Note Unidirectional link detection (UDLD) is not supported by FXOS; ignore any references to UDLD. user-account – Show user information users – Show the current users logged in the system vdc – Show Virtual Device Contexts version – Show the software version vifs – Virtual interfaces vlan – Vlan commands vms – Vms commands vmware – Vmware related vrf – Display VRF information vsan – Show vsan information wwn – Show wwn information xml – XML agent zone – Zone show commands zoneset – Zoneset show commands

Command	Additional Information
terminal	Set terminal line parameters alias – Show aliases (if no arugments); create 'exec' aliases (not persistent). Persistent aliases are in config mode, see 'cli alias' color – Enable colorization of prompt(green if last command ok, red if error), command line (blue), output (default color) dont-ask – Don't ask 'are you sure' questions, take default answer instead edit-mode – Set command line edition keys (vi or emacs; emacs is default) event-manager – Event manager cli event history – Configure terminal history properties length – Set number of lines on a screen monitor – Copy Syslog output to the current terminal line no – Negate a command or set its defaults output – How output of show commands should be formated prompt – Configure how the prompt should look like redirection-mode – Set the redirection mode session-timeout – Set session timeout sticky-mode – Search for the command match in current mode only terminal-type – Set the terminal type time – Save the current time under a variable tree-update – Updates the main parse tree verify-only – Verify command and do not execute width – Set width of the display terminal

connect local-mgmt: Command List

After you have used the Supervisor **connect local-mgmt** command to connect to the local management shell, the following commands are available in that shell. See connect adapter, on page 40 for information about the **connect local-mgmt** command.

In this shell, you can perform operations on the fabric interconnect, including copying files, rebooting the fabric interconnect, running ping and traceroute commands, and perhaps most importantly, generating troubleshooting files.

Note When you connect to the local-management command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to the default prompt with `(local-mgmt)` appended; see the following example.

To exit the local-management mode, type **exit**.

Example

The following example shows how to connect to the local-management command shell, and view available commands:

```
firepower# connect local-mgmt
firepower(local-mgmt)#  ?
  cd                Change current directory
  clear             Clear managed objects
  cluster           Cluster mode
  connect           Connect to Another CLI
  copy              Copy a file
  cp                Copy a file
  delete            Delete managed objects
  dir               Show content of dir
  enable            Enable
  end               Go to exec mode
  erase             Erase
  erase-log-config  Erase the mgmt logging config file
  exit              Exit from command interpreter
  fips              FIPS compliance
  ls                Show content of dir
  mgmt-port         Management Port
  mkdir             Create a directory
  move              Move a file
  mv                Move a file
  ping              Test network reachability
  ping6             Test IPv6 network reachability
  pwd               Print current directory
  reboot            Reboots Fabric Interconnect
  restore-check     Check if in restore mode
  rm                Remove a file
  rmdir             Remove a directory
  run-script        Run a script
  show              Show system information
  shutdown          Shutdown
  ssh               SSH to another system
  tail-mgmt-log     tail mgmt log file
```

```
  telnet            Telnet to another system
  terminal          Terminal
  top               Go to the top mode
  traceroute        Traceroute to destination
  traceroute6       Traceroute to IPv6 destination
  verify            Verify Application Image

firepower(local-mgmt)# exit
firepower#
```

Table 12: Commands Available in the Local Management Shell

Command	Additional Information
cd	Change current directory usbdrive: - File URI volatile: - File URI workspace: - File URI clear - Clear managed objects sshkey - Host public SSH key
cluster	Cluster mode force - Force local fabric interconnect to become primary lead - Make subordinate fabric interconnect primary
connect	Connect to Another CLI adapter - Mezzanine Adapter cimc - Cisco Integrated Management Controller fxos - Connect to FXOS CLI local-mgmt - Connect to Local Management CLI module - Security Module Console
copy	Copy a file ftp: - Source File URI scp: - Source File URI sftp: - Source File URI tftp: - Source File URI usbdrive: - Source File URI volatile: - Source File URI workspace: - Source File URI

Command	Additional Information
cp	Copy a file ftp: - Source File URI scp: - Source File URI sftp: - Source File URI tftp: - Source File URI usbdrive: - Source File URI volatile: - Source File URI workspace: - Source File URI
delete file	Delete managed objects usbdrive: - Source File URI volatile: - Source File URI workspace: - Source File URI
dir	Show content of dir order (Optional) - Order files by time usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI
enable cluster	Enable cluster mode a.b.c.d - Cluster IpV4 address ipv6 - IPv6 Cluster mode
end	Go to exec mode
erase	Erase configuration - System configuration
erase-log-config	Erase the mgmt logging config file
exit	Exit from command interpreter
fips	FIPS compliance fault-test - Execute FIPS fault tests self-test - Execute FIPS self-test on demand

Command	Additional Information
ls	Show content of dir order (Optional) - Order files by time usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI
mgmt-port	Management Port no-shut (Optional) - Management port up shut (Optional) - Management port down
mkdir	Create a directory usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI
move	Move a file usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI
mv	Move a file usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI
ping	remote_host - Hostname or IP addr (Min size 0, Max size 510)
ping6	Test network reachability Test IPv6 network reachability remote_host - Hostname or IP addr (Min size 0, Max size 510)
pwd	Print current directory
reboot	Reboots Fabric Interconnect
	Check if in restore mode
rm	Remove a file usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI

Command	Additional Information
rmdir	Remove a directory usbdrive: (Optional) - File URI volatile: (Optional) - File URI workspace: (Optional) - File URI
run-script	Run a script workspace: - Name of a script to run
show	Show system information cli - CLI Information clock - Clock file - File Commands license - Show license information mgmt-ip-debug - IP Debug Info mgmt-port - Management Port open-network-ports - Show open network ports pmon - Pmon processes - Processes sel - System Event Log software - Software sshkey - Sshkey tech-support - Tech Support
shutdown	Shutdown
ssh	SSH to another system remote_system - Enter hostname or user@hostname (Min size 0, Max size 510)
tail-mgmt-log	tail mgmt log file module - Module Name (Min size 0, Max size 510)
telnet	Telnet to another system remote_host - Hostname or IP addr (Min size 0, Max size 510)
terminal	Set terminal line parameters length - Set number of lines on a screen width - Set width of the display terminal
top	Go to the top mode

Command	Additional Information
traceroute	Traceroute to destination remote_host - Hostname or IP addr (Min size 0, Max size 510)
traceroute6	Traceroute to IPv6destination remote_host - Hostname or IP addr (Min size 0, Max size 510)
verify signature	Verify Application Image bootflash: - Image File Name usbdrive: - Image File Name volatile: - Image File Name workspace: - Image File Name

Note You will find differences in CPU usage values when you use **show processes** and **show system resources** CLIs simultaneously. The CPU usage values differ because of the number of iterations and intervals that each CLI uses by default to summarize the output after sampling through the iterations.

connect module: Command List

After you have used the Supervisor **connect module** command to connect to a specific module console, the following commands are available on that console. See connect module, on page 52 for information about the **connect module** command.

In this shell, you can perform operations on the fabric interconnect, including copying files, rebooting the fabric interconnect, and running ping and traceroute commands.

Note When you connect to a module command shell, the command-line prompt changes from your default prompt, which is the name you assigned to the appliance, to `Firepower-module`*n*, where *n* is the number of the module to which you connected; see the following example.

Examples

The following example shows how to connect to the module 1 using Telnet, and view available commands:

```
firepower# connect module 1 telnet
Type exit or Ctrl-] followed by . to quit.
Firepower-module1>?
    secure-login     => Enable blade secure login
    show             => Display system information. Enter show ? for options
    config           => Configure the system. Enter config ? for options
    terminalLength   => Terminal settings. Enter terminal ? for options
    ping             => Ping a host to check reachability
    nslookup         => Look up an IP address or host name with the DNS servers
    traceroute       => Trace the route to a remote host
    connect          => Connect to specific csp console (asa, etc)
    support          => System file operations
    testcrashinfo    => Test crashinfo support
    exit             => Exit the session
    help             => Get help on command syntax
Firepower-module1> <Ctrl-], .>
firepower#
```

Table 13: Commands Available on a Module Console

Command	Additional Information
secure-login	Enable blade secure log in

Command	Additional Information
show	Display system information. Enter show ? for options diskusage – Display current disk space usage time – Display current system date and time faults – Display the security module faults if any memoryusage – Display the system Memory usage cpuinfo – Display the system CPU Information users – Display who is logged on and user operations uptime – Display system up time slot – Display the slot number of SSP to which this blade is connected processes – Display all system processes hosts – Show hosts route – Show configured routes interfaces – Show currently configured interfaces version – Display product version netstat – Show network connections vnicmap – Display VNICs with Ethernet interfaces platform – None memory – Display the memory monitor configuration disk – Display the disk monitor configuration cpu – Display the CPU monitor configuration ntp – Show NTP time sync information coredump – Show coredump configuration maxRestart – Show maxRestart turboBoost – Show turboBoost configuration services – Display status of the services process – Show process details cgroups – Display the cgroups tech-support – Generate system information report for troubleshooting purposes

Command	Additional Information
config	Configure the system. Enter config ? for options vnic – Configure specified VNIC memory – Configure memory monitor disk – Configure disk monitor process – Configure process cpu monitor maxRestart – Configure maximum restarts CSP. 0 shall Disable feature. Default 8 restartTimeInter – Configure time in seconds to block all CSPs from starting if server restarts maxRestart in this interval. Default 1200 restartCounters – To reset the restart_count coredump – config coredump {...} turboBoost – config turboBoost {...}
terminalLength	Terminal settings. Enter terminal ? for options enable – terminal length enable disable – terminal length disable
ping	Ping a host to check reachability *host*
nslookup	Look up an IP address or host name with the DNS servers *host*
traceroute	Trace the route to a remote host *host*
connect	Connect to specific csp console (asa, etc) *appname apphost*

Command	Additional Information
support	System file operations platform – Platform operations fileupload – Copy Archive files to MIO diagnostic – Create diagnostic Archive file filelist – List existing files in system directories fileview – View files in the system filetail – Tail files in the system deleteBootImage – Delete boot image certdownload – Download certificate from remote syslog server verify – verify image generate – support generate {command..} tunnel – support tunnel {command..} dplug-access – Enable dplug access send_diag_archiv – Uploads a Default Archive to MIO send_logs – Uploads select files to MIO
testcrashinfo	Test crashinfo support singleprocess – Test crashinfo support with single process multiprocess – Test crashinfo support with multiple processes multithread – Test crashinfo support with multiple threads
help	Get help on command syntax