ID	Type	Message	Description	Action
700101	Debug	[msg:%s]		
702001	Debug	[msg:%s]		
703001	Debug	[msg:%s]		
703100	Debug	Client Match: LoadBal Band mismatch Skipping match for Client [mac:%m] Dest AP [name:%s] [bss:%m]		
703101	Debug	Client Match: LoadBal unsupport channel Skipping match for Client [mac:%m] Dest AP [name:%s] [bss:%m] [ch:%d]		
703102	Debug	Client Match: LoadBal Not found match for Client [mac:%m] Dest AP [name:%s] [bss:%m] signal -[signal:%d] snr thresh [thresh:%d]		
703103	Debug	Client Match: LoadBal Found match for Client [mac:%m] Dest AP [name:%s] [bss:%m] Eff_Signal -[e_sig:%d] dBm (Signal -[signal:%d] dBm EIRP [pwr:%s] dBm) snr delta thresh [thresh:%d]		
703104	Debug	Client Match: LoadBal no match for Client [mac:%m] with Dest AP [name:%s] [bss:%m] assoc:(Signal -[assoc_sig:%d], EIRP [assoc_pwr:%s] Eff_Signal -[assoc_e_sig:%d]), dst:(Signal -[dst_sig:%d], EIRP [dst_pwr:%s] Eff_Signal -[dst_e_sig:%d]), snr delta thresh [thresh:%d]		
703105	Debug	Client Match: LoadBal Adding pot sta [mac:%m] for move from AP [name:%s] [bss:%m] Current SNR [snr:%d]		
703106	Debug	Client Match: MUBal Skip monitor/spectrum mode radio [mac:%m] AP [name:%s]		
703107	Debug	Client Match: MUBal Skip radio [mac:%m] AP [name:%s] num_cl [cl:%d] num_mu_cl [mucl: %d]		
703108	Debug	Client Match: MUBal Checking AP [name:%s] radio [mac:%m] num_mu_clients [mu:%d]		
703109	Debug	Client Match: MUBal Skip visited radio [mac:%m] AP [name:%s]		
703110	Debug	Client Match: MUBal Check VBR nbr AP [name:%s] radio [mac:%m]		
703111	Debug	Client Match: MUBal PBSS skip AP [name:%s] radio [mac:%m] num_cl [numcl:%d] num_mu_cl [mucl:%d]		
703112	Debug	Client Match: MUBal Adding Client [mac:%m] for MU steer		
703113	Debug	Client Match: MUBal Incompatible AP [name:%s] radio [rad:%m] for Client [mac:%m] SNR [sig:%d] required SNR [rsig:%d]		
703114	Debug	Client Match: MUBal Found compatible AP [name:%s] radio [rad:%m] for Client [mac:%m] SNR [sig:%d] required SNR [rsig:%d]		
703115	Debug	Client Match: MUBal Steering Client [mac:%m] from AP [src:%s] radio [srcrad:%m] to AP [name:%s] radio [rad:%m]		
703116	Debug	Client Match: MUBal Signal delta exceeded for Client [mac:%m] with Dest AP [name:%s] [bss:%m] effective diff [eff_diff:%d], assoc:(Signal -[assoc_sig:%d], EIRP [assoc_pwr:%s] Eff_Signal -[assoc_e_sig:%d]), dst:(Signal -[dst_sig:%d], EIRP [dst_pwr:%s] Eff_Signal -[dst_e_sig:%d]), snr delta thresh [thresh:%d]		
703117	Debug	Client Match: MUBal Signal delta within bounds for Client [mac:%m] with Dest AP [name:%s] [bss:%m] effective diff [eff_diff:%d], assoc:(Signal -[assoc_sig:%d], EIRP [assoc_pwr:%s] Eff_Signal -[assoc_e_sig:%d]), dst:(Signal -[dst_sig:%d], EIRP [dst_pwr:%s] Eff_Signal -[dst_e_sig:%d]), snr delta thresh [thresh:%d]		
700102	Error	[msg:%s]		
702002	Error	[msg:%s]	This log indicates that we encountered an internal system error	Contact your support provider
703002	Error	[msg:%s]		
703003	Info	[msg:%s]		
703005	Info	[msg:%s]	System related info messages logged in the arm process	
700100	Warning	[msg:%s]		
703000	Warning	[msg:%s]		
703004	Warning	[msg:%s]	System related warning messages logged in the arm process	

ID	Type	Message	Description	Action
200101	Alert	FIPS Alert: [msg:%s]	This is a FIPS alert log in network module.	
202080	Alert	Vlan [vlanid:%u] couldn't be added to database		
200102	Critical	FIPS Critical: [msg:%s]	This is a FIPS critical log in network module.	
200001	Debug	Received frame src mac [smac:%s] type [etype:%x] from datapath/auth: opcode [op:%s], ingress port [ing:%s] egress port [ep:%s], incoming vlan [vl:%d], v6-vlan [v6_vlan:%d], length [len:%d] flags [fl:%x]	NA	
200004	Debug	Sending frame src mac [smac:%s] back to datapath: opcode [op:%s], ingress port [ing:%s] egress port [ep:%s], packet vlan(home) [vl:%d], v6-vlan [v6_vlan:%d], length [len:%d], packet flags [pfl:%x]	NA	
200005	Debug	Error creating or obtaining tunnel ID from [lcl:%pI4] to [rmt:%pI4]	NA	
200006	Debug	Added L2-GRE Tunnel for local IP address [lcl:%pI4] to remote IP address [rip:%pI4]	NA	
200008	Debug	L2-GRE Tunnel for local IP address [lcl:%pI4] to remote IP address [rip:%pI4] already exists	NA	
200010	Debug	Received invalid DHCP packet from remote switch	NA	
200011	Debug	L2-GRE Tunnel with start [st:%s] endpoint [ter:%s] is down	NA	
200012	Debug	Received dnat msg from ipsakmpd master switch ip [swip:%pI4] mapped to masterip [mip:%pI4]	NA	
200107	Debug	FIPS Debug: [function:%s], [file:%s]:[line:%d]: [msg:%s]	This is a FIPS debugging log in network module.	
202001	Debug	constructor, ip=0x[ip:%0]8X, lease_min=[lease_min:%d]n	A debug message indicating a DHCP pool has been created.	
202004	Debug	Killing DHCPD daemon	A debug message indicating DHCP wrapper is terminating DHCPD. DHCPD will be restarted if necessary.	
202005	Debug	backupLease stat flash returned [errno:%d]n	A debug message indicating an error occurred while measuring the size of the backup lease file.	
202006	Debug	backuplease memsize=[mem_st_siz:%d], flashsize=[flash_st_siz:%d]n	A debug message notifying the size of the backup lease file.	
202008	Debug	restoreLease stat flash returned [errno:%d]n	A debug message notifying DHCPD is unable to determine the size of lease file.	
202009	Debug	restoreLease memsize=[msm_st_siz:%d], flashsize=[flash_st_siz:%d]n	A debug message notifying the size of the lease file.	
202011	Debug	Starting DHPCD daemon	A debug message indicating DHCP wrapper is starting DHCPD. At dawn or when configuration changes	
202013	Debug	Child process DONE.	A debug message indicating DHCPD has completed its execution. It will be restarted if necessary.	
202014	Debug	Daemon child id = [g_chil:%d]n	A debug message notifying the process id of DHCPD.	
202015	Debug	Daemon DHCPD [g_child:%d] is being restarted	A debug message notifying that DHCPD was killed and is being restarted	
202018	Debug	Dhcpdwrap got vLan change message	To be filled out	
202019	Debug	Dhcpdwrap got switch ip change message	A debug message indicating switch's IP address has changed.	
202020	Debug	Dhcpdwrap got vrrp ip change message	A debug message indicating a virtual router's IP address has changed.	
202022	Debug	Found relay to delete, [s_size:%d] leftn	A debug message indicating the relay IP address is found in the internal database.	
202025	Debug	Received provap enable packet, ip=[ipaddr:%s]		
202026	Debug	Received provap disable packet		
202027	Debug	Dhcpdwrap got switch add dhcpc options message		
202028	Debug	Dhcpdwrap got switch delete dhcpc options message		
202043	Debug	parseNetwork: range val=[val:%d]		
202048	Debug	Got AMAPI_SET type=[objectType:%d], [key:%s]: [value:%s]		
202050	Debug	...continue async show command		
202052	Debug	Got Show DHCP Database		
202053	Debug	Got Show DHCP bindings		
202054	Debug	Got Show DHCP pool		
202056	Debug	Got AMAPI_DELETE type=[objectType:%d], [key:%s]: [value:%s]		
202057	Debug	Deleting pool [key:%s]: [value:%s]		

202058	Debug	Disabling DHCP service		
202064	Debug	Got [key:%s]: [value:%s]n		
202073	Debug	DNS Server for AP provisioning dropping DNS request		
202079	Debug	debugDHCP packet too small [len:%d]([my_dhcp_packet:%zu]). srcIP: [src_ip: %s] dstIP: [dst_ip: %s] srcPort: [src_port: %d] dstPort: [dst_port: %d]"	Debug message indicating small size DHCP packet (may be DHCP informs) was received,	
202081	Debug	Vlan [vlanid:%u] couldn't be found in database, [line:%u]		
202083	Debug	Vlan [vlanid:%u] has no IP address	Debug message to indicate that action couldn't be performed since Vlan had no IP address	
202085	Debug	[str:%s]	DHCP generic debug message	
202088	Debug	Packet vlan unknown for DHCP packet from host mac [str:%s]	Debug message to report a malformed header	
202501	Debug	...address is [s_addr:%s], vlanid is [vlanid:%d]n		
202503	Debug	...interface [g_ifIPs:%s]		
202505	Debug	Reinitializing DHCP RELAY mappings		
202507	Debug	CLI ip-helper vlan=[vlan:%s], addr=[addr:%s]		
202509	Debug	vlan=[vlan:%s], addr=[addr:%s]		
202511	Debug	Found relay to delete, [sz:%d] leftn		
202513	Debug	Could not find interface and/or vlan for ip=[ip:%s], could be reply to mobility message.		
202514	Debug	done with relayInitn		
202515	Debug	In relayScann		
202516	Debug	readfd=[readfd:%x], inner=[inner:%x], desc=[desc:%d]n		
202517	Debug	relayScan Removing giaddr [s_addr:%s], name=[name:%s]		
202518	Debug	relayScan added descriptor [desc:%d] to Dispatcher, return=[r:%d]n		
202519	Debug	relayScan readfd=[readfd:%p], inner=[inner:%p], desc=[desc:%d]n		
202520	Debug	relayScan Adding giaddr [s_addr:%s], name=[name:%s], vlan=[vlanid:%d]		
202521	Debug	relayScan donen		
202522	Debug	In readEventn		
202523	Debug	[func:%s]: mac=[chaddr:%s] dev=[name:%s], length=[length:%d], from_port=[from_port:%d], op=[op:%d], giaddr=[s_addr:%s], packet_vlan[packet_vlan:%d]		
202524	Debug	Discarding packet with invalid hlen.		
202525	Debug	no relay servers. dropping packet		
202526	Debug	Error while stripping relay agent options from packet with CHADDR=[chaddr:%s] Packet Len=[length:%d], dropping		
202527	Debug	RelayToClient: [str:%s] src=[src_addr:%s] dest=[dest_addr:%s] client yiaddr=[client_addr:%s] giaddr=[s_addr:%s] MAC=[chaddr:%s]		
202528	Debug	Relay got packet from lon		
202529	Debug	Out VLAN ID = 0. dhcprelay dropping		
202530	Debug	dropping packet without our giaddr=[giaddr:%s]		
202531	Debug	Error while adding relay options for packet with CHADDR=[chaddr:%s] Dropping packet		
202532	Debug	got [cnt:%d] relay servers		
202533	Debug	Relayed: [str:%s] server=[server_addr:%s] giaddr=[gi_addr:%s] MAC=[chaddr:%s]		
202534	Debug	[hdr:%s]: DISCOVER [chaddr:%s] Transaction ID:[xid:%x] [tlr:%s]		
202536	Debug	[hdr:%s]: REQUEST [chaddr:%s] Transaction ID:[xid:%x] reqIP=[reqIP:%s] [tlr:%s]		
202538	Debug	[hdr:%s]: RELEASE [chaddr:%s] Transaction ID:[xid:%x] clientIP=[s_addr:%s]		
202540	Debug	[hdr:%s]: DECLINE [chaddr:%s] Transaction ID:[xid:%x] reqIP=[s_addr:%s]		
202541	Debug	Received DHCP packet from Datapath, Flags [msg_flg:%x], Opcode [op:%x], Vlan [vlan:%d], Ingress [ing:%s], Egress [eg:%s], SMAC [smac:%s]		
202542	Debug	[hdr:%s]: INFORM [chaddr:%s] Transaction ID:[xid:%x] clientIP=[s_addr:%s]		
202544	Debug	[hdr:%s]: ACK [chaddr:%s] Transaction ID:[xid:%x] clientIP=[s_addr:%s]		
202546	Debug	[hdr:%s]: OFFER [chaddr:%s] Transaction ID:[xid:%x] clientIP=[s_addr:%s]		
202548	Debug	[hdr:%s]: NAK [chaddr:%s] Transaction ID:[xid:%x] clientIP=[s_addr:%s]		
202550	Debug	Pool info sip[start:%x] eip[end:%x] ptype[pool:%d]	DHCP pool configuration publish	
202554	Debug	DHCP-RELAY: Object for mac addr: [str:%s] found in STA channel.	STA channel object lookup successful for the mac.	
202555	Debug	DHCP-RELAY: Object for mac addr: [str:%s] not found in STA channel.	STA channel object lookup failed for the mac.	
202556	Debug	Discarding packet with invalid hlen while adding L2 option-82		
202557	Debug	Error while stripping L2 relay agent options from packet with CHADDR=[chaddr:%s] Packet Len=[length:%d], dropping		
202559	Debug	SendToClient L2 Option82: [str:%s] dest=[dest_addr:%s] client yiaddr=[client_addr:%s] MAC=[chaddr:%s]		
202561	Debug	Added L2 Option82: [str:%s] server=[server_addr:%s] giaddr=[gi_addr:%s] MAC=[chaddr:%s]		
202562	Debug	[str:%s]	DHCP generic debug message	
202563	Debug	DHCP-RELAY: Object for ap mac addr: [str:%s] found in BSS channel.	BSS channel object lookup successful for the mac.	

202564	Debug	DHCP-RELAY: Object for ap mac addr: [str:%s] not found in BSS channel.	BSS channel object lookup failed for the mac.	
202565	Debug	DHCP-RELAY: Object for ap group: [str:%s] found in BSS channel.	BSS channel object lookup successful for the ap-group.	
202567	Debug	Debug: [func:%s] [line:%d] DHCP-OPTION82 relay agent add, received unsupported combination for client[addr:%s].	DHCP-OPTION82 relay agent add, received unsupported combination for client.	
202568	Debug	Debug: [func:%s] [line:%d] DHCP-OPTION82 relay agent transmit, subtype5 applied for client=[chaddr:%s].	DHCP-OPTION82 relay agent transmit, subtype5 applied.	
202570	Debug	Error: Relay agent receive, bogus giaddr[giaddr:%s].	Relay agent receive, bogus giaddr.	
202572	Debug	Debug: [func:%s] [line:%d] DHCP-OPTION82 relay agent, subtype5 route address retrieval passed for [addr:%s].	DHCP-OPTION82 relay agent, subtype5 route address retrieval passed.	
202573	Debug	Debug: [func:%s] [line:%d] DHCP-OPTION82 relay agent debug l3helper[flag:%d] client[caddr:%s] interface[iaddr:%s].	DHCP-OPTION82 relay agent debug.	
203004	Debug	[ame:%s]	Debug message indicating service name being used to contact the server	
203013	Debug	Begin discovery	Debug message indicating discovery process has begun.	
203015	Debug	Unable to get switch MAC address: [errno:%s]n	PPPoE cannot get switch MAC address. Contact technical support.	
203018	Debug	Sending LCP ECHOREQ	Debug message indicating switch is sending an LCP ECHO request.	
203023	Debug	Ignoring packet with PPPoE Code: 0x[code:%x]	A debug message indicating an unknown PPPoE packet has arrived. If the problem persists contact the service provider.	
203025	Debug	Received IPCP CONFREQ. Sending CONFACK	A debug message indicating an IPCP configuration request has arrived.	
203027	Debug	Received LCP ECHOREQ. Sending ECHOREP	A debug message indicating the server sent an LCP ECHO request.	
203029	Debug	Received LCP ECHOREP	A debug message indicating PPPoE server has sent LCP ECHO reply.	
204201	Debug	Received IGMP [version:%d] QUERY from [ip:%pI4] on VLAN [vlan:%d]	NA	
204202	Debug	Received IGMP [version:%d] REPORT from [ip:%pI4] on VLAN [vlan:%d]	NA	
204204	Debug	Received IGMP LEAVE from [ip:%pI4] on VLAN [vlan:%d]	NA	
204205	Debug	Received unknown IGMP message type [type:%d] from [ip:%pI4] on VLAN [vlan:%d]	NA	
204206	Debug	Sending IGMP QUERY to group [ip:%pI4] out VLAN [vlan:%d] and dest [dest:%x]	NA	
204207	Debug	Received Mobile IP message [msg:%s] from mobile client [ip:%pI4]	NA	
204209	Debug	Received Mobile IP add group [group:%s] for address [ip:%pI4]	NA	
204211	Debug	Received Mobile IP remove group [group:%s] for address [ip:%pI4]	NA	
204212	Debug	Received unknown Mobile IP message [id:%d]	NA	
204213	Debug	Sending Mobile IP message type [type:%d] for client [ip:%pI4]	NA	
204215	Debug	Clearing IP multicast group members in VLAN [vlan:%d] from group [group:%s]	NA	
204227	Debug	Received IP multicast interface message [type:%d]	NA	
204228	Debug	Received IP multicast interface VLAN [type:%s] message for VLAN [id:%d], IGMP [igmp:%d], and PIM [pim:%d]	NA	
204229	Debug	Received IP multicast interface VLAN [type:%s] message for VLAN [id:%d]	NA	
204232	Debug	Received PIM [type:%s] from [ip:%pI4]	NA	
204233	Debug	No PIM RPF[id:%d] path for [ip:%pI4]	NA	
204234	Debug	Received an IP multicast packet that needs an [type:%s] for [source:%s] [str:%s]	NA	
204238	Debug	Adding [type:%s] [ip:%pI4] to PIM prune list	NA	
204239	Debug	Adding [type:%s] [ip:%pI4] to PIM join list	NA	
204240	Debug	Forwarding PIM BOOTSTRAP to new neighbor [ip:%pI4]	NA	
204241	Debug	Received PIM REGISTER STOP for unknown group [group:%s]	NA	
204242	Debug	Delete (S,G)RTP group [group:%s]	NA	
204243	Debug	Received PIM JOIN/PRUNE address to [ip:%pI4]	NA	
204244	Debug	PIM JOIN/PRUNE contains [num:%d] group	NA	
204245	Debug	PIM JOIN/PRUNE group [ip:%pI4] contains [joins:%d] joins and [prunes:%d] prunes	NA	
204247	Debug	PIM JOIN/PRUNE join [ip:%pI4] with flags [flags:%x]	NA	
204248	Debug	PIM JOIN/PRUNE prune [ip:%pI4] with flags [flags:%x]	NA	
204251	Debug	Received PIM BOOTSTRAP from non-RPF path [ip:%pI4]	NA	
204254	Debug	Forwarding PIM BOOTSTRAP message to VLAN [id:%d]	NA	
204255	Debug	Received a data timeout from datapath for PIM group [group:%s]	NA	
204256	Debug	Deleting idle PIM group [group:%s]	NA	

204259	Debug	Sending PIM HELLO to VLAN [id:%d]	NA	
204261	Debug	Sending PIM JOIN/PRUNE for group [group:%s] to [ip:%pI4]	NA	
204262	Debug	Sending PIM periodic JOIN/PRUNE to [ip:%pI4]	NA	
204263	Debug	Sending PIM triggered JOIN/PRUNE for [group:%s]	NA	
204264	Debug	Adding IGMP memory to PIM group [group:%s]	NA	
204265	Debug	Removing IGMP memory from PIM group [group:%s]	NA	
204267	Debug	Sending PIM ICMP ECHO request to [ip:%pI4]	NA	
204268	Debug	Clearing PIM VLAN [id:%d]	NA	
204269	Debug	Deleting PIM neighbor [ip:%pI4]	NA	
204271	Debug	NEW IGMP MEMBER [ip:%pI4] ADDED [GROUP:%s]	NA	
204272	Debug	EXISTING IGMP MEMBER [ip:%pI4] UPDATED [GROUP:%s]	NA	
204273	Debug	RECEIVED QUERY [version:%d] UPSTREAM IP [ip:%pI4] VLAN [vlan:%d]	NA	
204274	Debug	[str:%s]	Generic network debug message	
204275	Debug	RECEIVED LEAVE DELETE MEMBER [ip:%pI4], GROUP [maddr:%pI4]	NA	
204276	Debug	INTERFACE TIMER DELETE TIME OUT MEMBER [ip:%pI4], GROUP [maddr:%pI4]	NA	
204277	Debug	STOPPING REPORT TO UPSTREAM GROUP [ip:%pI4]	NA	
204278	Debug	INTERFACE TIMER DELETE NOT LAST MEMBER [ip:%pI4], GROUP [maddr:%pI4]	NA	
204279	Debug	PROXY SENDING REPORT GROUP [maddr:%pI4] VLAN [vlan:%d] Type [type:%d]	NA	
204280	Debug	UPDATING DATAPATH CONFIG VLAN [vlan:%d], IGMP [igmp:%d], PIM[pim:%d], PROXY[proxy:%d], DEST[dest:%d]	NA	
204281	Debug	PROXY: ADDED NEW GROUP [maddr:%pI4] VLAN [vlan:%d]	NA	
204282	Debug	PROXY: STARTING JOIN TIMER GROUP [maddr:%pI4]	NA	
204283	Debug	PROXY: SENDING LEAVE GROUP [maddr:%pI4] VLAN [vlan:%d]	NA	
204284	Debug	PROXY: FREEING GROUP [maddr:%pI4]	NA	
204285	Debug	RECEIVED REPORT UPSTREAM GROUP [maddr:%pI4]	NA	
204286	Debug	Received CPFW port info proto [proto:%d] sp [sp:%d] lp [lp:%d] action [add:%d]	NA	
204295	Debug	Adding group [maddr:%pI4] to mobileip message for [ip:%pI4]	NA	
204404	Debug	Publishing ESI group [group:%s] with id [id:%d] ([type:%d]		
204407	Debug	Received ping response from ESI server [ip:%pI4]		
204500	Debug	Killing RADVD daemon	A debug message indicating RADV wrapper is terminating RADVD. RADVD will be restarted if necessary.	
204501	Debug	Daemon RADVD [g_child:%d] is being restarted	A debug message notifying that RADVD was killed and is being restarted	
204502	Debug	radvdwrap got vLan change message	A debug message indicating that radvdwrap has got a vlan change message	
204505	Debug	radvd: vlan [vlan:%d] - operational state changed - [old:%s] to [new:%s]	Debug message indicating that the operational state of a vlan changed	Please contact Aruba tech-support if this problem persists
204506	Debug	Starting RADVDD daemon	A debug message indicating RADV wrapper is starting RADVD. At dawn or when configuration changes	
204507	Debug	Disabling RADV service		
204509	Debug	radvd: vlan [vlan:%d] - [msg:%s]	Debug message indicating L2 vlan add delete modify	Please contact Aruba tech-support if this problem persists
204510	Debug	Old RADVD instance [g_child:%d] is being cleaned ip. Spawning again	A debug message notifying that the old instance of RADVD is being cleaned up and the new instance is starting again	
207003	Debug	[str:%s]	NTP generic debug message	
208004	Debug	Dot1q Change Call back is called [intIfNum:%d] event [event:%s] ([eventid:%d])		
208006	Debug	Changing the vlan [vlan:%d] state to [state:%s] from [oldstate:%s]	VLAN state has changed to up or down as indicated	
208009	Debug	Link state of the XSec Vlan Interface [vlan:%d] has changed to [state:%s]		
208012	Debug	DHCPC: Entering released state	To be filled out	
208014	Debug	DHCPC: adding option [code:%2x]		
208019	Debug	DHCPC: payload length is [payload_length:%d] bytes		
208020	Debug	DHCPC: Sending discover over vlan [vlan:%d], mac [mac:%s]		
208021	Debug	DHCPC: Sending request over vlan [vlan:%d], mac [mac:%s] for [requested:%s]...		
208022	Debug	DHCPC: Sending renew over vlan [vlan:%d], mac [mac:%s]		

208023	Debug	DHCPC: Sending release over vlan [vlan:%d], mac [mac:%s]		
208029	Debug	DHCPC: transitioning the client state to [state:%s]:[reason:%s]		
208043	Debug	Nim received event [event:%s] for interface [intIfNum:%d] linkState [linkState:%d]		
208044	Debug	Nim Interface [intIfNum:%d] state change notification, new state [state:%s]		
208045	Debug	Received event [event:%d] for Interface [intfNum:%d]		
208054	Debug	VRID [id:%d] is not configured	System dropped VRRP advertisement due to incorrect configuration	
208058	Debug	Port [type:%s] [port:%s] oldstate [olds:%s] newstate [ns:%s]		
208059	Debug	Port-Channel [pc_id:%d] oldstate [olds:%s] newstate [ns:%s]		
208064	Debug	IPv6 VRID [id:%d] is not configured	System dropped VRRP advertisement due to incorrect configuration	
208067	Debug	VRID [id:%d] has been shutdown	System dropped VRRP advertisement since the VRRP has been shutdown	
208077	Debug	LACP: LACPDU received on port [port:%s]		
208082	Debug	PPPoE: Message received for client SrcPortNum [port:%d]	To be filled out	
208801	Debug	LACP: [str:%s]	This is an generic network debugging log for LACP.	
235002	Debug	LLDP Recv PKT at ingress [ingress_idx:%d]	NA	
235003	Debug	LLDP Sent PKT at egress [egress_idx:%d]	NA	
235007	Debug	Function: [function:%s] [x:%s]	NA	
236200	Debug	ospf_rtChanged [Action:%s] [addr:%s] [mask:%s] [cost:%u] [nexthop:%s]		
236209	Debug	Pkt RX - Intf [intf:%s] src_ip [src_ip:%s] dst_ip [dst_ip:%s] area [area:%s] type [type:%s]		
236210	Debug	Pkt TX - Intf [intf:%s] src_ip [src_ip:%s] dst_ip [dst_ip:%s] area [area:%s] type [type:%s]		
236217	Debug	Dropping DD packet from neighbor [neig:%s]. flags [flag:%s] DD Length [len:%d]		
236218	Debug	Unable to retransmit last DD to neighbor [neig:%s] after receiving duplicate DD in EXCHANGE state		
236219	Debug	Conductor discarding duplicate DD in [st:%s] state		
236220	Debug	Discarding invalid DD		
236222	Debug	[str:%s]		
236223	Debug	[str:%s]		
236404	Debug	[log_msg:%s]	Wrapper for opensource pppd syslogs	
237501	Debug	[msg:%s]		
237502	Debug	[msg:%s]		
238501	Debug	[msg:%s]		
299800	Debug	[function:%s], [file:%s]:[line:%d]: [error:%s]	This is an internal network debugging log.	
299801	Debug	[str:%s]	This is an generic network debugging log.	
200100	Emergency	FIPS Emergency: [msg:%s]	This is a FIPS emergency log in network module.	
200007	Error	Failed to Add L2-GRE Tunnel for local IP address [lcl:%pI4] to remote IP address [rip:%pI4]	Mobility failed to add HA-FA L2-GRE tunnel	Contact technical support
200103	Error	FIPS Error: [msg:%s]	This is a FIPS error log in network module.	
202000	Error	Failed to receive frame on socket [rfdesc:%d], errno [errno:%s], addr [s_addr:%x]hn	Error while receiving DHCP packet from socket.	Please contact support if this problem persists.
202016	Error	Error in sending PAPI message	Error message indicating the internal transport, PAPI, has failed.	Please contact Aruba tech-support if this problem persists
202017	Error	getCommandObjects failed line=[__line: %d]	Error message indicating that an error occured while reading DHCP configuration.	Please Contact Aruba tech-support if this problem persists.
202023	Error	Unable to find relay [addr:%s] for vlan [vlanid:%d] to deleten	An error message indicating the relay IP address is not found in the internal database.	
202046	Error	key size is [key_size: %d] instead of 2	Mismatch in key during configuration	Check DHCP configuration
202047	Error	deleteRelay key size is [key_size: %d] instead of 2	Mismatch in key during configuration	Check DHCP configuration
202049	Error	Could not find pool to turn on authoritative.	Error in DHCP pool configuration	Please contact Aruba tech-support if this problem persists.
202051	Error	DHCPD/CFGM messaging error during show command.	Error message indication that an internal communication error occured during show command	Please contact Aruba tech-support if this problem persists.

202061	Error	Could not find pool to turn off authoritative.	Error in DHCP pool configuration	Please contact Aruba tech-support if this problem persists.
202065	Error	Unable to enable datapath DHCP debug	Error message indicating the internal transport, PAPI, has failed.	
202067	Error	Unable to bind to UDP port 53 for DNS during AP provisioning.	An internal socket error occured when enabling DNS Server	Please contact Aruba tech-support if this problem persists
202071	Error	DNS Server got handleDNS error.	An internal socket error occured while initializing packet handler for DNS	Please contact Aruba tech-support if this problem persists
202075	Error	DNS reply, ioctl SIOCGIFFLAGS failed	Error message indicating that an internal error occured while getting interface information using IOCTL.	Please contact Aruba tech-support if this problem persists.
202076	Error	omapi_init failedn	Error message indicating that an error occured while initialzing OMAPI	
202077	Error	RelayToClient ERROR: [str:%s] src=[src_addr:%s] dest=[dest_addr:%s] client=[client_addr:%s] giaddr=[s_addr:%s] MAC=[chaddr:%s]	Error message indicating that an internal error occured while sending packet from relay to client	
202078	Error	Relay ERROR: [str1:%s] [str2:%s] server=[server_addr:%s] giaddr=[gi_addr:%s] MAC=[chaddr:%s]	Error message indicating that an internal error occured while sending packet from relay	
202087	Error	[str:%s]	DHCP generic debug message	
202545	Error	Could not find pool to turn off upsell.	Error in DHCP pool configuration	Please contact Aruba tech-support if this problem persists.
202549	Error	Could not find pool to turn on upsell.	Error in DHCP pool configuration	Please contact Aruba tech-support if this problem persists.
202551	Error	Failed to add pool [pool_name:%s] which has [num_leases_str:%s] addresses. Maximum addresses configurable is [g_dhcp_max_leases:%d]. Currently configured are [current_total_leases:%d] addresses. You may want to exclude unused address ranges.	DHCP maximum addresses reached.	
202552	Error	More DHCP addresses included and maximum address limit of [g_dhcp_max_leases:%d] exceeded. 1 or more active pools will be disabled. You may want to exclude unused address ranges.	DHCP maximum addresses reached.	
202553	Error	DHCP is oversubscribed. Maximum address limit is [g_dhcp_max_leases:%d]. Currently configured are [current_total_leases:%d] addresses. You may want to exclude unused address ranges.	DHCP maximum addresses reached.	
202558	Error	SendToClient L2 Option82 ERROR: [str:%s] dest=[dest_addr:%s] client=[client_addr:%s] MAC=[chaddr:%s]	Error message indicating that an internal error occured while sending packet from relay to client	
202560	Error	L2 Option82 send error: [str1:%s] [str2:%s] server=[server_addr:%s] giaddr=[gi_addr:%s] MAC=[chaddr:%s]	Error message indicating that an internal error occured while sending packet from relay	
202566	Error	DHCP-RELAY: Object for ap group: [str:%s] not found in BSS channel.	BSS channel object lookup failed for the ap-group.	
202569	Error	Error: [func:%s] [line:%d] DHCP-OPTION82 relay agent, subtype5 route address retrieval failed for [addr:%s].	DHCP-OPTION82 relay agent, subtype5 route address retrieval failed.	
202571	Error	Error: DHCP-OPTION82 relay agent transmit, option82 data exceeded 256 bytes.	DHCP-OPTION82 relay agent transmit, option82 data exceeded 256 bytes.	
202574	Error	Error: [func:%s] [line:%d] DHCP-OPTION82 relay agent vlan info retrieval failed for interface[ipaddr:%s].	DHCP-OPTION82 relay agent vlan info retrieval failed.	
203001	Error	[error_msg:%s]	PPPoE server doesn't understand the configured service name during discovery	Correct the service name using the CLI command "configure terminal ip pppoe-service-name"
203002	Error	[error_msg:%s]	PPPoE server returned a system error during discovery. This may be due to incorrectly configured PPPoE parameters	Verify PPPoE parameters using the CLI command "show ip pppoe-info"
203003	Error	[error_msg:%s]	PPPoE server returned a generic error during discovery. This may be due to incorrectly configured PPPoE parameters	Verify PPPoE parameters using the CLI command "show ip pppoe-info"

203005	Error	[error_msg:%s]	PPPoE server doesn't understand the configured service name during session confirmation.	Correct the service name using the CLI command "configure terminal ip pppoe-service-name"
203006	Error	[error_msg:%s]	PPPoE server returned a system error during session confirmation.	Verify PPPoE parameters using the CLI command "show ip pppoe-info"
203007	Error	[error_msg:%s]	PPPoE server returned a generic error during session confirmation.	Verify PPPoE parameters using the CLI command "show ip pppoe-info"
203009	Error	Bogus PPPoE length field ([length:%u])	Received invalid PADO (PPPoE Active Discovery Offer) packet from server with invalid PPPoE length.	Contact the service provider regarding PPPoE issues
203012	Error	Access concentrator used a session value of [session:%x] -- the AC is violating RFC 2516	PPPoE server is violating RFC 2516 with invalid session values.	Contact the service provider regarding PPPoE issues
203014	Error	Invalid ether type 0x[type:%x] in discovery	Received a non DISCOVERY packet in discovery mode.	Contact service provider.
203016	Error	Max LCP ECHO failures reached. Exiting	PPPoED is exiting because there is no response from server for LCP echo messages.	Verify configured PPPoE parameters.
203022	Error	PADT received from peer. Exiting	Remote PPPoE server has ended the session by sending a terminate request. These are initiated by the ISP and could be caused by poor line signal or suspension of service.	If the disconnects are excessive, please contact the ISP
203026	Error	Received IPCP TERMREQ. Connection Terminated	Remote PPPoE sever sent an IPCP terminate request. This is typically caused by an invalid authentication method or credentials	Contact the service provider if the problem persists.
203028	Error	Received LCP TERMREQ. Connection Terminated	Remote PPPoE sever sent an LCP terminate request. This is typically caused by an invalid authentication method or credentials	Contact the service provider if the problem persists.
203033	Error	Cannot initialize PAPI ([func_name:%s])	An error message indicating the internal transport, PAPI, has failed to initialize	Please contact Aruba Tech Support if the problem persists
203034	Error	Invalid PPPoE version ([ve:%d])	PPPoE server sent a packet with version number other than 1, the only version supported	Contact the service provider if problem persists.
203035	Error	Invalid PPPoE type ([typ:%d])	PPPoE server sent a packet with type other than 1, the only type supported	Contact the service provider if problem persists.
203036	Error	Invalid PPPoE packet length ([len:%u])	PPPoE server sent a packet with invalid length.	Contact the service provider if problem persists.
203037	Error	Invalid PPPoE tag length ([tagLen:%u])	PPPoE server sent a packet with invalid tag length.	Contact the service provider if problem persists.
203042	Error	PPPoE application error [str:%s]	PPPoE generic process error	Contact Aruba Techsupport if the errors are causing service interruptions
203047	Error	Service name mismatch [err_msg:%s]	An error message indicating there is a service name mismatch.	Verify that PPPoE parameters are configured correctly. Contact the ISP if problem persists
203048	Error	[err_msg:%s]	An error message indicating there is a system error	Verify PPPoE parameters.
203049	Error	[err_msg:%s]	An error message indicating there is a generic error.	Verify PPPoE parameters.
203053	Error	Packet too big! Check MTU on PPP interface	PPP packet is too big. Contact service provider if the problem persists.	
204203	Error	Could not add IP multicast group member [ip:%pI4] to group [group:%s]	NA	
204210	Error	Could not add Mobile IP IGMP group member [ip:%pI4]	NA	
204218	Error	Could not allocate IP multicast group [group:%s], out of memory	NA	
204222	Error	Could not allocate IP multicast group member, out of memory	NA	
204235	Error	Could not allocate PIM group [group:%s]	NA	

204236	Error	Could not add PIM neighbor [ip:%pI4]	NA	
204237	Error	Could not add PIM member [ip:%pI4] to group [group:%s]	NA	
204250	Error	Could not copy PIM members to group [group:%s]	NA	
204253	Error	Could not add RP [ip:%pI4] to PIM group	NA	
204260	Error	Not enough space in PIM JOIN/PRUNE for source [ip:%pI4]	NA	
204287	Error	Received CPFW port info: invalid data, protocol/port cannot be zero	NA	
204288	Error	Received CPFW port info: invalid data, start port cannot be greater than end port	NA	
204289	Error	Received CPFW port info: Could not allocate bw contract bw_contract_count [count:%d]	NA	
204290	Error	Received CPFW port info: Could not allocate bw contract [name:%s]	NA	
204291	Error	Received CPFW bwm info: invalid contract [index:%d]	NA	
204292	Error	Received CPFW bwm info: can't remove contract [index:%d], invalid value	NA	
204293	Error	Received CPFW bwm info: invalid contract [index:%d] with usecount 0	NA	
204296	Error	Received CPFW port info: Could not allocate bw contract	NA	
204297	Error	Received CPFW port info: bw contract already present name [contract:%s]	NA	
204299	Error	[str:%s]	Generic network error message	
204504	Error	Error in sending PAPI message	Error message indicating the internal transport, PAPI has failed	Please contact Aruba tech-support if this problem persists
204508	Error	getCommandObjects failed line=[__line: %d]	Error message indicating that an error occured while reading RADV configuration.	Please Contact Aruba tech-support if this problem persists.
207000	Error	[str:%s]	NTP generic error message	
208013	Error	DHCPC: Error adding the option: option: [name:%s] code: [code:%x] reason: [reason:%s]	Error message indicating dhcp option could not be added to the DHCP message due to size constraints	
208016	Error	DHCPC: Switch IP Address is Modified. Switch should be rebooted now	The switch IP address has been changed and switch rebooted to reflect this change	Save the current configuration and restart the controller
208017	Error	DHCPC: IP Address conflicts with another Interface	The DHCP client IP address conflicts with another interface IP on the controller	Check all the VLAN interfaces IPs configured on the controller for duplicates
208018	Error	DHCPC: Cannot Set IP Address: [ipaddr:%s]	An error occured when trying to set the DHCP Client interface IP	If this error persists please contact support
208025	Error	DHCPC: VLAN [dhcp_client_vlan:%d] is invalid	The VLAN on which DHCP client has been configured for is not valid	Check if the DHCP client vlan has been deleted, or if the vlan is not yet configured
208028	Error	DHCPC: Server failed to respond. Retrying	DHCP Server failed to respond to DHCP Client message. The operation will be retried	
208032	Error	DHCPC: couldnt get option from packet -- ignoring	DHCP Client could not parse the one of the options in the packet, and that option would be ignored	
208034	Error	DHCPC: No lease time with ACK, using 1 hour lease	Lease option was missing in the received packet. Client will use a default value	
208046	Error	DHCPC:Server failed to respond. Stopping the wizard		
208050	Error	Out of Packet Memory buffers	This is an internal error indicating system is out of packet memory buffers	
208051	Error	VRID [id:%d] failed to transition to master on [reason:%s]	Backup failed to transition to master for the specified reason	
208052	Error	Invalid VRRP Advertisement length [len:%u] received, expected [elen:%zu]	System received a short VRRP advertisement message. The message was ignored	
208053	Error	VRID [id:%d] failed to transition to backup	Master recieved a failed to transition to backup	
208055	Error	Invalid advertisement received for VRID [id:%d], [str:%s]	System dropped VRRP message due to invalid header content (such as TTL, type length, checksum, interval of authentication type)	
208056	Error	Invalid version received for VRID [id:%d]	System dropped VRRP message due to invalid version in the header	
208061	Error	IPv6 VRID [id:%d] failed to transition to master on [reason:%s]	Backup failed to transition to master for the specified reason	

208062	Error	Invalid VRRP IPv6 Advertisement length [len:%d] received, expected [elen:%d]	System received a short VRRP advertisement message. The message was ignored	
208063	Error	IPv6 VRID [id:%d] failed to transition to backup	Master recieved a failed to transition to backup	
208065	Error	Invalid advertisement received for IPv6 VRID [id:%d], [str:%s]	System dropped VRRP message due to invalid header content (such as TTL, type length, checksum, interval of authentication type)	
208066	Error	Invalid version received for IPv6 VRID [id:%d]	System dropped VRRP message due to invalid version in the header	
208804	Error	LACP: [str:%s]	This is an generic network debugging log for LACP.	
221002	Error	VLAN [vlan:%d] is not configured.	An non-existent VLAN was derived from DHCP option 77 processing.	Create the VLAN.
221003	Error	DHCP packet too small: len=[len1:%d] expected=[len2:%d].	DHCP option 77 processing was aborted because the received packet was too small.	Check the DHCP server, clients, and network for problems.
235004	Error	Function: [function:%s] [x:%s]	NA	
236202	Error	On interface [intf:%s] cannot include all neighbors in Hello		
236205	Error	Virtual link [intf:%s] transit area [area:%s] is an invalid transit area type [areaType:%s]		
236206	Error	Failed to add all link information to area [area:%s] router LSA. Router LSA full		
236207	Error	Failed to add all link information to area [area:%s] network LSA. Network LSA full		
236208	Error	LSA Checksum error detected for LSID [lsid:%s] checksum [chksum:%x]. OSPF Database may be corrupted		
236211	Error	Max allowed OSPF pkt len on Intf [intf:%s] is zero		
236212	Error	OSPFv2 attempted to install a zero length LSA		
236213	Error	[__FUNCTION:%s]: LSA length [len:%d] less than LSA header length [hd_len:%d]		
236214	Error	Max allowed OSPF buf len is zero for LSA type [type:%d]		
236215	Error	Route prefix [r_pre:%s] mask [r_mask:%s] not contained in T7 range addr [ra_addr:%s] mask [ra_mask:%s]		
236216	Error	Dropping OSPFv2 DD packet received on [intf :%s]. DD MTU is [d_mtu:%u]. Local MTU is [l_mtu:%u]		
236221	Error	LSA Checksum error in LsUpdate, dropping LSID [id:%s] checksum [cksum0x:%0x]		
236228	Error	Dropping [pktType:%s] received on intf [intf:%s]. OSPF payload length [len:%d] is big		
236229	Error	Mismatched OSPF Hello interval received on [intf:%s]		
236230	Error	Mismatched OSPF Dead interval received on [intf:%s]		
236400	Error	[log_msg:%s]	Wrapper for opensource pppd syslogs	
237001	Error	Received network error from WEB_CC module,[function:%s], [file:%s]:[line:%d]	WEB_CC module generic Network error	
237503	Error	[msg:%s]	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
237504	Error	[msg:%s]	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
238503	Error	[msg:%s]	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
243000	Error	LACP: LACPDU received on invalid intIfNum [num:%d]	System received a LACPDU frame on an invalid port	
299802	Error	[str:%s]	This is an generic network error log.	
200106	Info	FIPS Info: [msg:%s]	This is a FIPS info log in network module.	
202002	Info	Interface change detected	An informational message indicating DHCP has detected a change in one or more interfaces.	
202007	Info	Backing up lease file to flash.	An informational message indicating backup of lease file is happening.	
202010	Info	Using lease file from flash.	An informational message indicating lease file from flash is currently being used.	
202021	Info	Deleting DHCP relay IP [addr:%s] from vlan [vlanid:%d]n	An informational message indicating DHCP relay IP address is being deleted.	
202024	Info	Adding DHCP relay IP [addr:%s] for vlan [vlanid:%d]n	An informational message indicating DHCP relay is enabled on VLAN.	

202029	Info	set domain to [domain:%s]	An informational message indicating the internal value stored for the domain.	
202030	Info	setting DNS import	An informational message indicating that DNS is being imported.	
202031	Info	set dns to [dns:%s] ...	An informational message indicating the internal value stored for DNS.	
202032	Info	unsetting DNS import	An informational message indicating that import DNS is being unset.	
202033	Info	deleted dns entry [dns_ip:%s]	An informational message indicating that DNS entry is deleted.	
202034	Info	setting netbios import	An informational message indicating that netbios entry is being imported.	
202035	Info	set netbios to [netbios:%s] ...	An informational message indicating the internal value stored for netbios.	
202036	Info	unsetting netbios import	An informational message indicating that import netbios is being unset.	
202037	Info	deleted netbios entry [netbios_ns:%s]	An informational message indicating that the netbios entry is deleted.	
202038	Info	set router to [router:%s] ...	An informational message indicating the internal value stored for default-router.	
202039	Info	deleted router entry [router_ip:%s]	An informational message indicating that the router entry is deleted.	
202040	Info	added new option. code: [code:%d] option: [value:%s]	An informational message indicating the DHCP option being added.	
202041	Info	deleted option. code: [code:%d]	An informational message indicating the DHCP option is deleted	
202042	Info	set lease to [lease_day:%d] [lease_hr:%d] [lease_min:%d] [lease_sec:%d]	An informational message indicating the internal value stored for lease	
202044	Info	ip=[ip:%s], mask=[mask:%s]	An informational message indicating the internal value stored for network	
202045	Info	Cmd exclude [s:%s] [e:%s]	An informational message indicating the network value excluded	
202055	Info	Clearing IP DHCPD Leases and bindings	An informational message indicating that DHCP leases and bindings are cleared	
202062	Info	deleted domain-name	An informational message indicating that domain name entry is deleted	
202063	Info	deleted lease	An informational message indicating that dhcp lease entry is deleted	
202066	Info	Initialized DHCPD PAPI Messaging.	An informational message indicating that PAPI is initialzed	
202068	Info	Enabled DNS Server.		
202069	Info	Enabled DHCP Server for AP provisioning.		
202070	Info	Disabled DHCP Server for AP provisioning.		
202072	Info	DNS Server replied to IP [s_addr:%s] during AP provisioning with answer [g_provip:%s]		
202082	Info	Vlan [vlanid:%u] entry already present		
202086	Info	[str:%s]	DHCP generic informational message	
203000	Info	pppoed started. pid: [pid:%d]	Informational message indicating PPPoE daemon has completed initialization	
203008	Info	Sending PADI	Informational message indicating a PPPoE Active Discovery Initiation (PADI) packet has been sent	
203011	Info	PPPoE session id is [session:%d]	Information indicating the PPPoE session ID	
203017	Info	No response for LCP ECHO Request. Retrying	Informational message indicating an LCP ECHO response has not arrived.	
203019	Info	Sending connection params to FPAPPS	Informational message indicating PPPoE daemon is sending session parameters to enable the connection.	

203020	Info	Terminate request received from FPAPPS. Exiting	An informational message indicating PPPoE daemon has been terminated due to change in PPPoE parameters.	
203024	Info	Invalid Ether Type: 0x[h_proto:%x]	An informational message indicating a packet has arrived that has an ether type of neither DISCOVERY or SESSION. Contact the service provider if the problem persists.	
203030	Info	PPPoED: invalid ppp proto: 0x[payloa:%0]4xn	An informational message indicating a PPP packet that is neither LCP or IPCP has arrived	Contact service provider if problem persists
203046	Info	Sent PADT	An informational message indicating session terminate request has been sent.	
203050	Info	[buf:%s]	An informational message that displays PPPoE packet received.	
203051	Info	end-of-file in syncReadFromPPP	An error occurred while reading PPP packet	Contact support if the problem persists
203052	Info	end-of-file in asyncReadFromPPP	An error occurred while reading PPP packet	Contact support if the problem persists
204216	Info	[str:%s]	NA	
204219	Info	Added IP multicast group [group:%s]	NA	
204220	Info	Deleted IP multicast group [group:%s]	NA	
204223	Info	Added IP multicast [type:%s] member [ip:%pI4] to group [group:%s]	NA	
204224	Info	Removed IP multicast member [ip:%pI4] from group [group:%s]	NA	
204225	Info	Added IP multicast interface with VLAN [id:%d] and address [ip:%pI4]	NA	
204226	Info	Removed IP multicast interface with VLAN [id:%d] and address [ip:%pI4]	NA	
204298	Info	Added IPv6 multicast [type:%s] member [ip:%s] to group [group:%s]	NA	
204402	Info	ESI server [server:%s] added to group [group:%s]	ESI server was added to specified group	
204403	Info	ESI server [server:%s] removed from group [group:%s]	ESI server was removed from specified group	
204405	Info	Ping response timed out for [type:%s] ESI server [ip:%pI4]	ESI server failed to respond to ping request. The request will be retried up to configured limit	
204503	Info	Initialized RADVD PAPI Messaging.	An informational message indicating that PAPI is initialzed	
207002	Info	[str:%s]	NTP generic informational message	
208001	Info	Spanning Tree Topology Changed. Port [type:%s] [port:%s] oldstate [olds:%s] newstate [ns:%s]	Spanning Tree topology has changed for the specified port	
208002	Info	[type:%s] Bad BPDU Packet size [dataLen:%d], Dropping it	A BPDU of invalid size was detected and dropped	
208003	Info	Spanning Tree Topology Change. Switch is the new root of the Spanning tree	System is the new root of the spanning tree	
208007	Info	Vlan interface [vlanId:%d] state is [state:%s]	VLAN interface state is currently up or down as indicated	
208008	Info	No change in the Vlan Interface [vlanId:%d] state [state:%s] [reason:%s]	VLAN interface change request could not be processed due to specified reason	
208010	Info	Switch IP VLAN interface ([vlanId:%d]) state is changed to [state:%s]	Switch IP VLAN interface state changed to up or down as indicated	
208011	Info	DHCPC: Unicasting a release of [ipaddr:%s] to [server_ip:%s]	DHCP client released an IP address to the specified DHCP server	
208024	Info	DHCPC: Removed DHCP client from vlan [vlan:%d]	DHCP client disabled on the specified VLAN	
208026	Info	DHCPC: VLAN [vlan:%d] current vlan state is [state:%s]	This messages indicates current state of VLAN where DHCP client is active	
208027	Info	DHCPC: DHCP client is enabled on vlan [vlan:%d]	DHCP client was enabled on specified VLAN	
208030	Info	DHCPC: Ignoring XID [xi:%x] (our xid is [xid:%x])	DHCP client will ignore received DHCP packet due to mismatch in transaction ID	
208031	Info	DHCPC: DUPLICATE XID 0x[xid:%x] chosen by switch [switch_mac:%s] and mac [mac:%s]	DHCP client will ignore received DHCP packet due to mismatch in MAC address. The DHCP operation will be reset and retried	
208033	Info	DHCPC: No server ID in message		
208035	Info	DHCPC: Lease of [yiaddr:%s] obtained, lease time [lease:%d]	DHCP client is setting lease time to value derived from obtained lease time from the server	

208036	Info	DHCPC: Indefinite lease	DHCP client lease time is set to indefinite period	
208037	Info	DHCPC: Received DHCP NAK for other server, ignoring	DHCP client received DHCP NAK from another server. It will be ignored	
208038	Info	DHCPC: Received DHCP NAK	DHCP client received NAK. Client state will be reset and operation retried	
208039	Info	DHCPC: Received DHCPFORCERENEW	DHCP client received FORCERENEW packet from server. Client state will be reset DHCP operation restarted	
208040	Info	PPPoE: VLAN [vlan:%d] state is [state:%s]	This message shows PPPoE client VLAN state (Up or Down)	
208041	Info	PPPoE: Connection established. IP [ipaddr:%s] netmask [nm:%s] Router [rtr:%s] DNS [dn:%s]	PPPoE connection was established with server successfully	
208048	Info	PPPoE: Setting the TCP MSS to [mss:%d]	PPPoE TCP MSS is set to specified value	
208049	Info	PPPoE: Removed TCP MSS	PPPoE TCP MSS override was cleared	
208057	Info	PPP: Connection established. IP [ipaddr:%s] netmask [netmask:%s] Router [router:%s] DNS [dns:%s] Unit [unit:%d]	A PPP connection has been established with the remote server.	
208060	Info	Spanning Tree Topology Changed. Port-Channel [pc_id:%d] oldstate [olds:%s] newstate [ns:%s]	This information message indicates change in spanning tree topology for the specified port-channel	
208071	Info	LACP: LACP is enabled on port [port:%s]	Link Aggregation Control Protocol is enabled on the specified port	
208072	Info	LACP: LACP is disabled on port [port:%s]	Link Aggregation Control Protocol is disabled on the specified port	
208073	Info	LACP: Port [port:%s] is attached to LAG [pc_id:%d]	Specifed port was attached to LAG aggregator	
208074	Info	LACP: Port [port:%s] is detached from LAG [pc_id:%d]	Specified port was detached from LAG aggregator	
208075	Info	LACP: Collection and distribution is enabled on port [port:%s]	Specified port was enabled to receive and transmit frames	
208076	Info	LACP: Collection and distribution is disabled on port [port:%s]	Specified port was disabled to receive and transmit frames	
208078	Info	LACP: LACPDU received on invalid port [port:%s] intIfNum [num:%d]	System received a LACPDU frame on an invalid port	
208079	Info	LACP: Illegal LACPDU received on port [port:%s]	System received an LACPDU frame of illegal type	
208080	Info	LACP: Unknown LACPDU received on port [port:%s]	System received an LACPDU frame of unknown type	
208081	Info	PPPoE: Client doesn't exist for vlan [vlan:%d]	To be filled out	
208802	Info	LACP: [str:%s]	This is an generic network debugging log for LACP.	
208805	Info	SDWAN: [action:%s] ([proto:%s]) [net:%s]/[prefix:%d] cost [cost:%d]	FPAPPS to OFA route pubsub information	
209800	Info	Physical link up: port [port:%s], [duplex:%s] duplex, speed [speed:%s]	Successful link-level communication has been established for the port	
235005	Info	Function: [function:%s] [x:%s]	NA	
235008	Info	Function: [function:%s] Interface [slot:%d]/[port:%d] recieved lldpdu meant for slot [pktslot:%d] and ingress_idx [ingress_idx:%d]	NA	
235009	Info	Function: [function:%s] Interface [slot:%d]/[port:%d] Ingress_idx [ingress_idx:%d] is not enabled with LLDP RECEIVE	NA	
236201	Info	Dropping [pktType:%s] on intf [intf:%s] from router [rtr:%s] at IP [addr:%s]. Neighbor address is [nbraddr:%s]		
236203	Info	Dropping hello on intf [intf:%s] for router [rtr:%s] from IP [addr:%s]. Neighbor address is [nbraddr:%s]		
236224	Info	OSPF is enabled on interface [intf:%s]		
236225	Info	OSPF is disabled on interface [intf:%s]		
236226	Info	Neighbor [neigh:%s] is up on interface [intf:%s]		
236227	Info	Neighbor [neigh:%s] is down on interface [intf:%s]		
236403	Info	[log_msg:%s]	Wrapper for opensource pppd syslogs	
237505	Info	[msg:%s]		
237506	Info	[msg:%s]		
238505	Info	[msg:%s]		
243001	Info	LACP: Illegal LACPDU received on IntfNum [num:%d]	System received an LACPDU frame of illegal type	

243002	Info	LACP: Unknown LACPDU received on IntfNum [num:%d]	System received an LACPDU frame of unknown type	
200105	Notice	FIPS Notice: [msg:%s]	This is a FIPS notice log in network module.	
204230	Notice	Firewall: [config:%s] is [state:%s]	NA	
204231	Notice	Firewall: [config:%s] is enabled and threshold is [cnt:%d]	NA	
204266	Notice	Rehashing PIM RPs	NA	
204294	Notice	IPv6 packet processing is [state:%s]	NA	
236402	Notice	[log_msg:%s]	Wrapper for opensource pppd syslogs	
200000	Warning	Bad length for ethernet frame received from datapath: [len:%d]; Dropping	Mobility received bad length ethernet frame from datapath, packet will be Dropped	
200104	Warning	FIPS Warning: [msg:%s]	This is a FIPS warning log in network module.	
202084	Warning	[str:%s]	DHCP generic warning message	
203031	Warning	PAPI_Send failed. Dest: [DestPortNum:%d]	A warning message indicating PAPI is unable deliver the message. The message will be resent.	
204200	Warning	Received IGMP message with invalid Length [length:%d]	And invalid IGMP packet was received	
204208	Warning	Could not find IGMP interface for VLAN [vlan:%d]	VLAN interface state is out of sync for the specific VLAN	
204217	Warning	Could not allocate IP multicast group [group:%s], limit of [num:%d] reached	NA	
204221	Warning	Could not allocate IP multicast group member, limit of [num:%d] reached	NA	
204246	Warning	PIM JOIN/PRUNE [str:%s] not supported	NA	
204249	Warning	RPS do not match for group [ip:%pI4]	NA	
204252	Warning	Received fragmented PIM BOOTSTRAP message	NA	
204257	Warning	Received PIM fragment	NA	
204258	Warning	Received unknown PIM message type [type:%d]	NA	
204406	Warning	Ping health check failed for ESI server [ip:%pI4]	ESI server failed to respond to ping request after retries. Server will be marked down	
204408	Warning	Could not send ping request to ESI server [ip:%pI4], error [err:%d]	System encountered an internal error while sending ping request to specified ESI server. The request will be retried	
207001	Warning	[str:%s]	NTP generic warning message	
208047	Warning	DHCPC:Bogus packet. Option fields too long	A warning message indicating that DHCP option field in the incoming packet was not correct	
208803	Warning	LACP: [str:%s]	This is an generic network debugging log for LACP.	
209801	Warning	Physical link down: port [port:%s]	Link has been lost on the port	
221000	Warning	Unable to bring LDAP server [s:%s] into service.	An error occurred when attempting to bring a LDAP server into service.	Check that the LDAP server is reachable and in working order.
221001	Warning	Error in connecting to LDAP server [s:%s].	An error occurred in connecting to LDAP server.	Check that the LDAP server is reachable and in working order.
235000	Warning	LLDP recieved PKT invalid opcode [opcode:%d]	NA	
235001	Warning	LLDP recieved PKT with invalid buflen [buflen:%d]	NA	
235006	Warning	Function: [function:%s] [x:%s]	NA	
236000	Warning	Bad length for ethernet frame received from datapath: [len:%d]; Dropping	NA	
236204	Warning	A [LsdbType:%s] range for [prefix:%s] [mask:%s] already exists on area [area:%s]		
236401	Warning	[log_msg:%s]	Wrapper for opensource pppd syslogs	
239500	Warning	VRRP invalid	NA	

ID	Type	Message	Description	Action
100101	Alert	FIPS Alert: [msg:%s]	This is a FIPS alert log in security module.	
100102	Critical	FIPS Critical: [msg:%s]	This is a FIPS critical log in security module.	
118000	Critical	Certificate [certname:%s] is expired.	The certificate has expired.	
118005	Critical	[string:%s]	This shows a critical error message in Cert Mgr.	
118013	Critical	Certificate [certname:%s] is going to expire in less than 60 days.	Certificate [certname:%s] is going to expire in less than 60 days.	
118016	Critical	[string:%s]	This shows a critical error message in Cert Mgr for EST.	
124058	Critical	Random number generator function failed.	The Random number generator function failed.	
124061	Critical	The system has reached its capacity of firewall rules.	The system has reached its firewall rule capacity.	Delete or consolidate the existing firewall rules to free up space for more rules.
132002	Critical	Enabling dot1x termination for AP [mac:%m] [auth_profile:%s] before cert download	Termination is being enabled before certificate is downloaded	
132014	Critical	AP [bssid:%m] [apname:%s] Incomplete AP configuration.Check if WEP Key, WEP Transmit Key or WPA Passphrase is not configured	AP's configuration is not complete. Either WEP key/WEP Transmit Key/WPA Passphrase is not configured	
132135	Critical	Failed to create SSL_CTX	System failed to create SSL Context	
132136	Critical	Loading Certificate from [fname:%s] failed	Failed to load the Certificate for 802.1x termination	
132137	Critical	Private key does not match cert	Private key is not found in the certificate	
132138	Critical	Failed to alloc BIO in	Failed to allocate BIO structure	
132139	Critical	Failed to alloc BIO out	Failed to allocate BIO out structure	
132140	Critical	Failed to set the cipher - ssl3_get_cipher_by_char	Failed to set the cipher using ssl3_get_cipher_by_char	
132141	Critical	Failed to create buf - BUF_MEM_new	Failed to create a buffer using BUF_MEM_new	
132142	Critical	ssl3_output_cert_chain returned error	Failed to output the certificate chain	
132143	Critical	Failed to download MODEXP for dot1x-termination	Failed to download MODEXP to datapath for 802.1x termination	
132144	Critical	Failed to download the cert for dot1x-termination	Failed to download the server certificate for dot1x termination	
132145	Critical	BIO_read failed len [ln:%d]	BIO read failed	
132146	Critical	ssl_get_server_send_cert failed	ssl_get_server_send_cert failed	
133016	Critical	Failed to create the Internal User Database; [errmsg:%s]	System failed to create the internal user database	Contact customer support
133020	Critical	Failed to update the NASIP field for User [name:%s]	System encountered an error while updating NASIP field in user database record.	Contact customer support
133031	Critical	Failed to execute the database import command (errno = [errno:%d])	System encountered the specified error while importing user database	Contact technical support
133033	Critical	Failed to import the Internal User Database from file [name:%s]	System encountered an error while importing user database from the specifed file	Contact technical support
133045	Critical	Unsupported schema version in legacy database; skipping upgrade	The existing version 2 database is not one that is supported for automatic upgrade	
133052	Critical	[function: %s] Failed to allocate memory of [size: %zu] [name: %s]	AUTH DB_API failed to allocate memory	
133118	Critical	Internal argumenet error while upgrading database; Skipping upgrade	Invalid argument(s) are used for automatic upgrade	
133119	Critical	Internal error while handling userdb database ([taget:%s]) - OBSOLETED IMPLEMENTATION	Internal error	
137037	Critical	Random number generator function failed.	The Random number generator function failed.	
142009	Critical	[message:%s]	L2TP generic critical.	
100107	Debug	FIPS Debug: [function:%s], [file:%s]:[line:%d]: [msg:%s]	This is a FIPS debugging log in security module.	
103013	Debug	IKE Phase 1 failed to negotiate transform from [IP:%s]	Failure in negotiation of IKE SA due to misconfigured ISAKMP policy. Please look at output of show crypto isakmp policy and compare that to the peer/client	
103038	Debug	Unable to find L2TP/IPSEC for deletion. [IP:%s], IPSec-SPI [spi:0x%x], L2TP tunnel [tid:%d]		
103044	Debug	IKE: Too many xauth requests, throttling due to pending responses from AUTH process	IKE has exceeded the maximum number of XAUTH VPN Authentication requests to the AAA server. Please check the AAA server to see if it is not responding to the VPN authentication requests	
103049	Debug	Although this does not affect operations, the Switch is not [action:%s] IP routes for IPSec map due to absence of VPN license		

103050	Debug	IKE module Can not get local-conductor configuration		
103060	Debug	[prefix:%s] [file:%s]:[function:%s]:[line:%d] [message:%s]	To be filled out	
103063	Debug	[prefix:%s] [message:%s]	To be filled out	
103071	Debug	IKE: Too many UDB requests, throttling due to pending response from UDB process	IKE has exceeded the maximum number of Allowlist requests to the UDB server. It appears the UDB server is busy or not responding.	
103075	Debug	IKE: Too many Certificate Revocation requests, throttling due to delayed response from Certmanager process	IKE has exceeded the maximum number of Certificate Revocation requests to the Certmanager process. Please check the CERTMGR process to see why it is not responding	
103104	Debug	[ip:%s] [message:%s]	Peer debugging in IKE module	
109000	Debug	[msg:%s]	This is an internal LDAP debug log	
109001	Debug	LDAP Server [name:%s]: Initialization completed successfully	Initialization completed successfully for a LDAP server	
118003	Debug	[string:%s]	This shows an internal debug message in Cert Mgr.	
118012	Debug	Serial=[serial:%s], Revocation Status=[status:%s]	This prints a DEBUG-level log message with certificate serial number and revocation status.	
118014	Debug	[string:%s]	This shows an internal debug message in Cert Mgr for EST.	
121020	Debug	[func:%s](): Prepare Radius Interim Accounting [option:%s] counts for user [uname:%s]	Prepare RADIUS Interim Accounting Reqest Message	
121031	Debug	[[file:%s]:[line:%d]] [message:%s]	aaa module's debug message	
121037	Debug	[func:%s]: sta_add_rad_class_attr failed.	This shows an internal debug message	
121038	Debug	Save Class in station for MAC [mac:%s].	This shows an internal debug message	
121039	Debug	[func:%s]: sta_update_last_authserver failed.	This shows an internal debug message	
121040	Debug	[func:%s]: last_authserver [authserver:%s].	This shows an internal debug message	
121041	Debug	User [user:%s] MAC=[mac:%s] not found.	This shows an internal debug message	
121042	Debug	[func:%s]: Server FQDN is '[server:%s]', IP Address is '[ipaddr:%s]'.	This shows an internal debug message	
121043	Debug	[func:%s]: Server FQDN '[fqdn:%s]' not found in hash.	This shows an internal debug message	
121044	Debug	Radius authenticate user ([user:%s]) PAP query using server [server:%s].	This shows an internal debug message	
121045	Debug	[func:%s]: sta_update_last_srv_grp failed.	This shows an internal debug message	
121046	Debug	[func:%s]: last_srv_grp [last_srv_grp:%s].	This shows an internal debug message	
121050	Debug	[msg:%s]	This is an internal RADIUS debug log	
122020	Debug	[[file:%s]:[line:%d]] [message:%s]	aaa module's debug message	
122027	Debug	[function : %s] [line : %d] UserName:'[uname:%s]' CurPath:'[path:%s]' CmdStr:'[cmdstr:%s]' ServerGrp:'[svrgrp:%s]'	TACACS+ Command Authorization Data	
123000	Debug	[[file:%s]:[line:%d]] [message:%s]	aaa module's debug message	
124001	Debug	Regenerate ACL for policy [name:%s] tunnel [id1:%d]/[id2:%d]	Regenerate firewall rules due to tunnel up or down event	
124002	Debug	Regenerate ACL for policy [name:%s] ESI Group [group:%s]/[id:%d]	Regenerate firewall rules due to ESI group add or del event	
124004	Debug	[string:%s]	This shows an internal debug message	
124007	Debug	avpair_assign: MAC string is [strvalue:%s] ([macstr:%s])	This shows an internal error message	
124016	Debug	vp -> [name:%s] [lvalue:%d] [value:%s]	This shows an internal error message	
124018	Debug	vp -> [name:%s] [value:%s]	This shows an internal error message	
124028	Debug	[string:%s]	This shows Kerberos debug message	
124029	Debug	[string:%s]	This shows NTLM debug message	
124046	Debug	VLAN derivation. New rule position=[newrule:%d], Old rule position=[oldrule:%d].	This shows an internal debug message	
124048	Debug	VLAN derived from DHCP will be enforced. New VLAN = [newvlan:%d].	This shows an internal debug message	
124067	Debug	TACACS+ Accounting Successful: result=[rs:%s]([ri:%d]), method=[m:%s], username=[name:%s] source=[ip:%s] auth server=[sg:%s]	TACACS+ accounting successful	
124070	Debug	No PEF-NG license, and user defined role '[role:%s]' can be applied only to VPN/VIA users.	This shows an internal debug message	
124071	Debug	User [user:%s]: AUTH acl [auth:%d] SOS acl [sos:%d].	This shows an internal debug message	

124072	Debug	User [user:%s]: AUTH upstream contract [auth:%d] SOS upstream contract [sos:%d].	This shows an internal debug message	
124073	Debug	User [user:%s]: AUTH downstream contract [auth:%d] SOS downstream contract [sos:%d].	This shows an internal debug message	
124074	Debug	Invalid message length for MsgCode : DHCP_AUTH_ANYIP_RESP.	This shows an internal debug message	
124075	Debug	IP lookup failed for IP=[ip:%s], MAC=[mac:%s], action=[act:%d].	This shows an internal debug message	
124076	Debug	IP=[ipaddr:%s], MAC=[mac:%s], Invalid action=[act:%d].	This shows an internal debug message	
124077	Debug	Configuring IP=[ipaddr:%s] as ANYIP, MAC=[mac:%s].	This shows an internal debug message	
124078	Debug	Sibyte UA message: mac=[mac:%s] ip=[ipaddr:%s], ua_str=[ua_str:%s].	This shows an internal debug message	
124079	Debug	Dropping user miss for [mac:%s]/[ipaddr:%s] due to lack of layer 2 user (etype [etype:%x] proto [proto:%x] ingress [ingress:%x] vlan [vlan:%d]).	This shows an internal debug message	
124080	Debug	Dropping dhcp packet for [mac:%s] vlan derivation.	This shows an internal debug message	
124081	Debug	Dropping RAP user miss for [mac:%s]/[ipaddr:%s] due to lack of layer 2 user (ingress [ingress:%x] vlan [vlan:%d]).	This shows an internal debug message	
124082	Debug	Bandwidth contract changed for [users:%d] users with role [role:%s].	This shows an internal debug message	
124083	Debug	Bandwidth contract modified for [users:%d] users with role [role:%s].	This shows an internal debug message	
124084	Debug	Not updating user [user:%s]'s mac address to special mac address [mac:%s].	This shows an internal debug message	
124086	Debug	Create macuser [macuser:%p] and user [user:%p].	This shows an internal debug message	
124087	Debug	mac_station_free Null mac_user.	This shows an internal debug message	
124088	Debug	mac_station_free: mac [mac:%s] not found or inconsistent, passed [passedmac:%p], derived [derivedmac:%p].	This shows an internal debug message	
124089	Debug	mac_station_free Null user for [mac:%s].	This shows an internal debug message	
124090	Debug	Free macuser [macuser:%p] and user [user:%p] for mac [mac:%s].	This shows an internal debug message	
124091	Debug	[function:%s]: mac [mac:%s] encr-algo:[encr:%x].	This shows an internal debug message	
124092	Debug	[function:%s]: delete ACR station.	This shows an internal debug message	
124093	Debug	Called mac_station_new() for mac [mac:%s].	This shows an internal debug message	
124094	Debug	DEBUG :: Assign user to vlan [vlan:%d] ([vlanname:%s]) based on role [role:%s].	This shows an internal debug message	
124095	Debug	MAC: [mac:%s], No L2 auth configured, L2 Deauthenticate skipped for station.	This shows an internal debug message	
124096	Debug	Sending denylist message; station=[mac:%s]/[mactdot1x:%s].	This shows an internal debug message	
124097	Debug	Setting authserver '[authserver:%s]' for user [user:%s], client [client:%s].	This shows an internal debug message	
124098	Debug	Setting authstate '[authstate:%s]' for user [user:%s], client [client:%s].	This shows an internal debug message	
124099	Debug	Setting auth type '[authtype:%s]' for user [user:%s], client [client:%s].	This shows an internal debug message	
124100	Debug	Setting auth subtype '[subtype:%s]' for user [user:%s], client [client:%s].	This shows an internal debug message	
124101	Debug	Trying to set aaa profile to NULL user, reason: [reason:%s].	This shows an internal debug message	
124102	Debug	Trying to set NULL aaa profile to user, reason: [reason:%s].	This shows an internal debug message	
124103	Debug	Setting user [mac:%s] aaa profile to [name:%s], reason: [reason:%s].	This shows an internal debug message	
124104	Debug	ifmap-ua: mac=[mac:%s], ip=[ip:%s].	This shows an internal debug message	
124105	Debug	MM: mac=[mac:%s], state=[state:%d], name=[name:%s], role=[role:%s], dev_type=[dev:%s], ip=[ip:%s], new_rec=[new_rec:%d].	This shows an internal debug message	
124106	Debug	GUT :: **************************************.	This shows an internal debug message	
124107	Debug	GUT :: conductor ip [conductorip:%s], switch ip [switchip:%s].	This shows an internal debug message	

124108	Debug	GUT :: display the results.	This shows an internal debug message	
124109	Debug	GUT :: continue show ([startNum:%d])th.	This shows an internal debug message	
124110	Debug	GUT :: display query status.	This shows an internal debug message	
124111	Debug	GUT :: register a session for the new query.	This shows an internal debug message	
124112	Debug	GUT :: number of LMS [numLms:%d].	This shows an internal debug message	
124113	Debug	GUT :: Send GUT request to local switch [lms:%s].	This shows an internal debug message	
124114	Debug	GUT :: Failed to send GUT request to conductor switch [conductorip:%s].	This shows an internal debug message	
124115	Debug	GUT :: Failed to send GUT request to local switch [localip:%s].	This shows an internal debug message	
124116	Debug	GUT :: the num of user exceeds maximum ([maxuser:%d]).	This shows an internal debug message	
124117	Debug	GUT :: handle gut request. send packet ([user:%d] user entries).	This shows an internal debug message	
124118	Debug	GUT :: handle gut request. total num of matched users ([user:%d]).	This shows an internal debug message	
124119	Debug	GUT :: a([PhyA:%d]) b([PhyB:%d]) g([PhyG:%d]).	This shows an internal debug message	
124120	Debug	GUT :: receive GUT response from ([ipstr:%s]), msglen ([msglen:%d]).	This shows an internal debug message	
124121	Debug	GUT :: rsp is related to session ([session:%d]).	This shows an internal debug message	
124122	Debug	GUT :: switch([switch:%s]) return ([user:%d]) user.	This shows an internal debug message	
124123	Debug	GUT :: a([PhyA:%d]) b([PhyB:%d]) g([PhyG:%d]).	This shows an internal debug message	
124124	Debug	GUT :: session status : status ([status:%d]), total user ([users:%d]), buffered user entry ([userentry:%d]).	This shows an internal debug message	
124125	Debug	GUT :: release session ([sessionId:%d]).	This shows an internal debug message	
124126	Debug	GUT :: num of buffered user ([numBufUser:%d]).	This shows an internal debug message	
124127	Debug	GUT :: user([user:%d]) : [ipstr:%s].	This shows an internal debug message	
124128	Debug	GUT :: Starting show at ([num:%d])th user.	This shows an internal debug message	
124129	Debug	GUT :: build user row.	This shows an internal debug message	
124130	Debug	GUT :: Stopping show at ([nth:%d])th user.	This shows an internal debug message	
124131	Debug	GUT :: all user entries have been displayed.	This shows an internal debug message	
124132	Debug	GUT :: display complete results ([globaluser:%d] users).	This shows an internal debug message	
124133	Debug	GUT :: display partial results ([globaluser:%d] users).	This shows an internal debug message	
124134	Debug	GUT :: session ([sessionid:%d]) timeout.	This shows an internal debug message	
124135	Debug	GUT :: take an available session ([session:%d]).	This shows an internal debug message	
124136	Debug	GUT :: no available session. expire the oldest session ([session:%d]).	This shows an internal debug message	
124137	Debug	GUT :: current session id ([session:%d]), concurrent sessions ([numsession:%d]).	This shows an internal debug message	
124138	Debug	GUT :: same as a previous query whose results have been retrieved.	This shows an internal debug message	
124139	Debug	GUT :: same as a previous query which has got all info.	This shows an internal debug message	
124140	Debug	GUT :: same as a previous query with expired timer.	This shows an internal debug message	
124141	Debug	GUT :: same as a previous query which is still waiting for info.	This shows an internal debug message	
124142	Debug	GUT :: query related session ([session:%d]).	This shows an internal debug message	
124143	Debug	GUT :: TX: msgtype [msgtype:%d], datalen [datalen:%d].	This shows an internal debug message	
124144	Debug	GUT :: set the flag largePapiInProgress.	This shows an internal debug message	
124145	Debug	GUT :: PAPI_SendLarge [count:%d]th try failed.	This shows an internal debug message	
124146	Debug	GUT :: Error in sending large PAPI message.	This shows an internal debug message	
124147	Debug	GUT :: reset the flag largePapiInProgress.	This shows an internal debug message	
124148	Debug	Create ipuser [userip:%s] for user [mac:%s].	This shows an internal debug message	
124150	Debug	Create ipuser and user [user:%s].	This shows an internal debug message	
124151	Debug	Publish Mac User and User Channels for User([user:%m]). Either FT_ROAM or no need to do MBA/Dot1x.	This shows an internal debug message	
124152	Debug	Delete ipuser [ipuser:%s] due to too many IPv6 address.	This shows an internal debug message	
124153	Debug	Free ipuser [ipuser:%p] ([ipstr:%s]) for user [user:%p].	This shows an internal debug message	
124154	Debug	Free user [user:%p].	This shows an internal debug message	
124155	Debug	No macuser for ip [ipaddr:%s], mac [mac:%s].	This shows an internal debug message	
124156	Debug	Called ip_user_new() for ip [ipaddr:%s].	This shows an internal debug message	

124157	Debug	[function:%s]: user not found.	This shows an internal debug message	
124158	Debug	[function:%s]: delete user [user:%s].	This shows an internal debug message	
124159	Debug	[function:%s]: Aborted sending Radius Accounting Stop for user=[user:%s] as user has more than one active IP addresses.	This shows an internal debug message	
124160	Debug	Dropping user miss for [mac:%s]/[ipaddr:%s] due to layer 2 user marked for deletion (etype [etype:%x] proto [proto:%x] ingress [ingress:%x] vlan [vlan:%d]).	This shows an internal debug message	
124162	Debug	Enforcing L2 check for mac [mac:%s].	This shows an internal debug message	
124163	Debug	download-L3: ip=[ipuser:%s] acl=[acl1:%d]/[acl2:%d] role=[role:%s], Ubwm=[up:%d], Dbwm=[down:%d] tunl=[tunl:%x], PA=[proxyarp:%d], HA=[homeagent:%d], RO=[roaming:%d], VPN=[outerip:%d], MAC=[mac:%m].	This shows an internal debug message	
124164	Debug	Remote UA message: mac=[mac:%s] ip=[ipaddr:%s], ua_str=[ua_str:%s].	This shows an internal debug message	
124165	Debug	{ACL} Downloading Bulk BWM Msg {[bulkBWMsgLen:%d] len} {[bwms:%d] bw-contracts} and {[users:%d] users} to sibyte.	This shows an internal debug message	
124166	Debug	Deleting sessions for users with role [rolename:%s].	This shows an internal debug message	
124167	Debug	Show user with authtype [authstr:%s] ([authtype:%d]).	This shows an internal debug message	
124168	Debug	Show mobile user [user:%s].	This shows an internal debug message	
124169	Debug	Show user name [user:%s].	This shows an internal debug message	
124170	Debug	Show user role [user:%s].	This shows an internal debug message	
124171	Debug	Show user devtype [devtype:%s].	This shows an internal debug message	
124172	Debug	Show user rows between [start:%d] and [end:%d].	This shows an internal debug message	
124173	Debug	Continuing show at [i:%d], [j:%d], [numusers:%d] [l:%d], unique [unique:%p].	This shows an internal debug message	
124174	Debug	show_user: skipping [a:%d] entries.	This shows an internal debug message	
124175	Debug	Stopping show at [i:%d], [j:%d], [numusers:%d], [l:%d].	This shows an internal debug message	
124176	Debug	show_user: [user:%s].	This shows an internal debug message	
124177	Debug	Continuing show at [i:%d], totstations [stations:%d].	This shows an internal debug message	
124178	Debug	Stopping show at [i:%d].	This shows an internal debug message	
124179	Debug	cleared counter for [mac:%s].	This shows an internal debug message	
124180	Debug	[func:%s]: ip=[ipaddr:%s], delete bridge: [delbridge:%s], MAC [mac:%s], VLAN [vlan:%u].	This shows an internal debug message	
124181	Debug	[func:%s]: ip=[ipaddr:%s].	This shows an internal debug message	
124182	Debug	{[ipaddr:%s]} role [role:%s] for outer=[extip:%s], count=[outerip:%d], auth type=[authtype:%d]->[vpnauthtype:%d], subtype=[authsubtype:%d], server=[vpnauthserver:%s].	This shows an internal debug message	
124184	Debug	{[utype:%s]} Authenticating Server is [serverName:%s].	This shows an internal debug message	
124185	Debug	[func:%s] line:[line:%d] roleName:[rolename:%s].	This shows an internal debug message	
124186	Debug	Create user with authtype [authstr:%s] ([authtype:%d]).	This shows an internal debug message	
124187	Debug	All XAUTH VPN client users deleted from Auth.	This shows an internal debug message	
124188	Debug	Deleting all users from datapath.	This shows an internal debug message	
124201	Debug	AP [ap_name:%s],: BSSID [bssid:%s] ESSID [essid:%s] aaa profile [aaa_prof_name:%s]	This shows an internal debug message	
124202	Debug	[func:%s](): Detected AP (f/l [first_or_last:%d]) with ip [ip:%s] slotport [slotport:%d] status [status:%d] txkey [tx_wkey:%d]	This shows an internal debug message	
124203	Debug	ENET msg: ENET Tunnel UP, (f/l [fast_or_last:%d]) ip: [ip:%s], dp_slotport:[slotport:%d] tunId:[t_id:%x], slot/port: [enet_slot:%u]/[enet_port:%u], ap_type [enet_ap_type:%d], ap_name [enet_ap_name:%s]	This shows an internal debug message	
124204	Debug	Adding to Mux table - ip: [ip:%s], tunId:[t_Id:%d], slot/port:[enet_slot:%u]/[enet_port:%u]	This shows an internal debug message	

124205	Debug	ENET msg: ENET Tunnel DOWN, (f/l [fast_or_last:%d]) ip: [ip:%s], dp_slotport:[slotport:%d] tunId:[t_id:%x], slot/port: [enet_slot:%u]/[enet_port:%u], ap_type [enet_ap_type:%d], ap_name [enet_ap_name:%s]"	This shows an internal debug message	
124206	Debug	Removing from Mux table - ip: [ip:%s], tunId:[t_Id:%d], slot/port:[enet_slot:%u]/[enet_port:%u]	This shows an internal debug message	
124207	Debug	[_functon_:%s]: Processing attribute [myvp_name:%s]	This shows an internal debug message	
124208	Debug	Updating AP authentication status, mac: [username:%s] by: [authen_username:%s] status: [status:%s]	This shows an internal debug message	
124209	Debug	[_function_:%s]:[_line_:%d] Updating vlan usage for MAC=[mac:%s] with vlan [vlan:%d] apname [apname:%s]	This shows an internal debug message	
124210	Debug	DEBUG :: Assign user to vlan [assigned_vlan:%d] ([vlanName:%s]) based on role [name:%s]	This shows an internal debug message	
124211	Debug	receive ([uNumSta:%d]) bridge users seq_num=[seq_num:%u]	This shows an internal debug message	
124212	Debug	stm_rap_bridge_sta_message: receive action [buser_action:%d] for users [buser_mac:%s]	This shows an internal debug message	
124213	Debug	FT([_function_:%s]) auth received r0 key [pmk_r0:%s] for sta [sta_mac:%s] mob_domain_id [mob_dmn_id:%d]	This shows an internal debug message	
124214	Debug	FT([_function_:%s]) auth r0kh_id=[r0kh_id:%s], snonce=[snonce:%s] pmk-r0-name=[pmk_r0_name:%s]	This shows an internal debug message	
124215	Debug	FT([_function_:%s]) auth resp status=[status:%d], anonce=[anonce:%s]	This shows an internal debug message	
124216	Debug	FT([_function_:%s]) assoc_req s0kh-id=[s0khid:%s], snonce=[snonce:%s], anonce=[anonce:%s]	This shows an internal debug message	
124217	Debug	FT([_funciton:%s]): mac=[mac:%s], mic=[mic:%s], pmk-r1-name=[pmk_r1_name:%s],	This shows an internal debug message	
124218	Debug	FT([_function_:%s]) assoc_req ric=[ric:%s]	This shows an internal debug message	
124219	Debug	FT([_function_:_%s]) assoc-rsp len=[bl:%d], status=[fn_status:%d], mic_control=[mic_control:%d], mic=[mic:%s], GTK=[gtk:%s]	This shows an internal debug message	
124220	Debug	stm_message_handler : msg_type [msg_type:%d]	This shows an internal debug message	
124221	Debug	stm_message_handler : msg_type [msg_type:%d]	This shows an internal debug message	
124222	Debug	ENET msg: ENET Tunnel UP, ip: [ip:%s], tunId:[t_id:%x], slot/port: [enet_slot:%u]/[enet_port:%u], ap_type [enet_ap_type:%d] ap_name [enet_ap_name:%s]	This shows an internal debug message	
124223	Debug	AP State msg: ENET Tunnel UP, ip: [ip:%s], tunId:[t_id:%x], slot/port: [enet_slot:%u]/[enet_port:%u], ap_type [enet_ap_type:%d] ap_name [enet_ap_name:%s]	This shows an internal debug message	
124224	Debug	Updating Mux table - ip: [ip:%s], tunId:[t_Id:%d], slot/port:[enet_slot:%u]/[enet_port:%u]	This shows an internal debug message	
124225	Debug	[_function_:%s] Sending STM wired vlan info: vlan [vlan:%d], status [status:%s]	This shows an internal debug message	
124226	Debug	Internal Error : User not on system with IP:[user_ip:%s],mac:[user_mac:%s]	This shows an internal debug message	
124227	Debug	Internal Error : No aaa profile found for IP:[user_ip:%s],mac:[user_mac:%s]	This shows an internal debug message	
124228	Debug	Internal action:[action:%d] received for IP:[user_ip:%s],mac:[user_mac:%s]	This shows an internal debug message	
124229	Debug	[_function_:%s] Tunid [tunid:%x] vlan [vlan:%d] avlan [avlan:%d]	This shows an internal debug message	
124230	Debug	Rx message [messageCode:%d]/[msgtype:%d], length [msglen:%d] from [SrcIpAddr:%s]:[SrcPortNum:%d]	This shows an internal debug message	
124231	Debug	Ignore message [msgtype:%d] from [SrcIpAddr:%s]:[SrcPortNum:%d] len [msglen:%d]	This shows an internal debug message	

124232	Debug	Invalid message [msgtype:%d] from [SrcIpAddr:%s]:[SrcPortNum:%d] len [msglen:%d]	This shows an internal debug message	
124233	Debug	Tx message to Sibyte, flag [flag:%d]. Opcode = [opcode:%d], msglen = [msglen:%d] [action_str:%s]	This shows an internal debug message	
124234	Debug	Tx message to Sibyte, blocking with ack, Opcode = [opcode:%d], msglen = [totlen:%d] [action_str:%s]	This shows an internal debug message	
124235	Debug	Tx message to Sibyte, blocking with reply, Opcode = [opcode:%d], msglen = [totlen:%d] [action_str:%s]	This shows an internal debug message	
124236	Debug	Rx Packet Length [bufferLen:%d] bytes Opcode [opcode:%d]	This shows an internal debug message	
124237	Debug	Rx Packet Length [bufferLen:%d] bytes	This shows an internal debug message	
124238	Debug	Deleting station [mac:%s] from machine auth cache as the local-userdb entry is deleted	This shows an internal debug message	
124239	Debug	[msg:%s]	This shows an internal debug message	
124240	Debug	Received subcribed info : FIPS mode [fips_mode:%s]	This shows an internal debug message	
124241	Debug	[_function_:%s]:[_line_:%d] VLAN_POOL_ASSIGNMENT_TYPE_EVEN not supported for bridge. Performing hash to retrieve vlan-id	This shows an internal debug message	
124242	Debug	Check IPSEC Suite-B ACR license cookie:[cookie:%d] code:[suiteb_msgtype:%d] vers:[ike_version:%d] ip:[ipaddr:%s] port:[port:%d]	This shows an internal debug message	
124243	Debug	Deny IPSEC Suite-B ACR license cookei:[cookie:%d]	This shows an internal debug message	
124244	Debug	Allow IPSEC Suite-B ACR license cookei:[cookie:%d]	This shows an internal debug message	
124245	Debug	Decrement IPSEC Suite-B ACR license cookei:[cookie:%d]	This shows an internal debug message	
124246	Debug	Sending auth up message to IKE daemon	This shows an internal debug message	
124247	Debug	[_function_:%s]: publish ACL download finish message	This shows an internal debug message	
124248	Debug	[_function:%s]: NULL acl for acl ref msg	This shows an internal debug message	
124249	Debug	[_function:%s]: Error sending acl [accname:%s], ref msg rsp_len [replylen:%d]	This shows an internal debug message	
124250	Debug	Tx message to Sibyte, NON_BLOCKKING_W_ACK, Opcode = [opcode:%d], msglen = [totlen:%d] [action_str:%s]	This shows an internal debug message	
124270	Debug	[Function:%s]: Dormant Mac [Dormant:%s] not found.	This shows an internal debug message	
124271	Debug	l2role=[l2role:%s] l3role=[l3role:%s] server=[name:%s] role=[rname:%s] rptr=[r:%p] authtype=[atype:%d].	This shows an internal debug message	
124299	Debug	GUT :: total number of users exceeds maximum ([maxuser:%d]).	This shows an internal debug message	
124300	Debug	GUT :: copy only ([some:%d]) user entries.	This shows an internal debug message	
124303	Debug	[function:%s] VLAN [vlan:%d] is removed	This shows an internal debug message	
124304	Debug	[function:%s] Named VLAN [vlan:%s] is removed	This shows an internal debug message	
124306	Debug	[function:%s] Named VLAN [vlan:%s] not mapped	This shows an internal debug message	
124307	Debug	[function:%s]: user role [role:%s] update validity from [current:%d] to [new:%d]	This shows an internal debug message	
124308	Debug	sacl not found, acl not updated for profile [name:%s]	This shows an internal debug message	
124309	Debug	[function:%s] - publisher: Reset netservice table	This shows an internal debug message	
124310	Debug	[function:%s] - publisher: Add netservice [name:%s]	This shows an internal debug message	
124311	Debug	[function:%s] - publisher: sending netservice message - [total:%d]	This shows an internal debug message	
124312	Debug	[function:%s] - publisher: netservice [name:%s] - [action:%d]	This shows an internal debug message	
124313	Debug	Add service: [name:%s] [proto:%d] [fport:%d] [lport:%d] [alg:%s]	This shows an internal debug message	
124314	Debug	Service [name:%s] unchanged	This shows an internal debug message	
124315	Debug	New port(s) addition to netservice [name:%s] used [aces:%d] ace	This shows an internal debug message	
124316	Debug	add destination6 [name:%s] host [address:%s] invert not set	This shows an internal debug message	
124317	Debug	Destination6 [name:%s] unchanged	This shows an internal debug message	
124318	Debug	Add destination: [name:%s] [address:%s] [mask:%s] invert [invert:%d]	This shows an internal debug message	
124319	Debug	[function:%s] Add destination: [name:%s] hostname: [host:%s]	This shows an internal debug message	

124320	Debug	[function:%s] new entry addition to netdestination [name:%s] used [refcount:%d] aces	This shows an internal debug message	
124321	Debug	[function:%s] Add destination: [name:%s] [addess:%s] [mask:%s]	This shows an internal debug message	
124322	Debug	Setting tunnel destination to [idx:%x] for tunnel [tunnel:%d]	This shows an internal debug message	
124323	Debug	Converting tunnel [tunnel:%d] redirect to DENY rule	This shows an internal debug message	
124324	Debug	Setting SLB destination to [idx:%d] for group [group:%s]	This shows an internal debug message	
124325	Debug	Ignoring firewall rule with unknown SLB group [group:%s]	This shows an internal debug message	
124326	Debug	Converting policy to filters for session acl [name:%s]	This shows an internal debug message	
124327	Debug	Converting policy to filters for role [name:%s]	This shows an internal debug message	
124328	Debug	Adding [entries:%d] filters for access-list [name:%s] type [type:%s] to role [role:%s] curcnt [count:%d]	This shows an internal debug message	
124329	Debug	generating ACE entries for role [name:%s], ACL [num:%d]	This shows an internal debug message	
124330	Debug	Generating ACE entries for session-ACL [name:%s], ACL# [num:%d]	This shows an internal debug message	
124331	Debug	New policy used [count:%d] aces	This shows an internal debug message	
124332	Debug	Add rule in policy [name:%s] with action [action:%d]	This shows an internal debug message	
124333	Debug	Config destination [name:%s] [address:%s] netmask: [mask:%s] [invert:%s]	This shows an internal debug message	
124334	Debug	Removing std_acl : [num:%d], from Role: [name:%s]	This shows an internal debug message	
124335	Debug	Applying session acl [name:%s] to role [role:%s] used [count:%d] aces	This shows an internal debug message	
124336	Debug	Invalid service or destination	This shows an internal debug message	
124337	Debug	bw-contracts unchaged.	This shows an internal debug message	
124338	Debug	[function:%s]: role-name [role:%s] vlanstr [vlan:%s]	This shows an internal debug message	
124339	Debug	[functions:%s] : isVlanNameOrId : [nameorid:%d]	This shows an internal debug message	
124340	Debug	[functions:%s](Role:[name:%s]): Remove VLAN-Id:[id:%d] valid:[valid:%d]	This shows an internal debug message	
124341	Debug	[function:%s](Role:[name:%s]): VLAN-Id:[vlan:%d] is not configured	This shows an internal debug message	
124342	Debug	[function:%s](Role:[name:%s]): Config VLAN-Id:[vlan:%d] valid:[valid:%d]	This shows an internal debug message	
124343	Debug	[function:%s](Role:[name:%s]): Remove Named VLAN:"[vlan:%s]" valid:[valid:%d]	This shows an internal debug message	
124344	Debug	[function:%s](Role:[name:%s]): Named VLAN:"[vlan:%s]" does not exist	This shows an internal debug message	
124345	Debug	[function:%s](Role:[name:%s]): Config Named VLAN:"[vlan:%s]", valid:[valid:%d]	This shows an internal debug message	
124346	Debug	[function:%s]: sacl_add failed	This shows an internal debug message	
124347	Debug	Adding authserver [server:%s]-[policy:%s] to stateful ntlm policy	This shows an internal debug message	
124348	Debug	[function:%s]: role_del_sacl failed	This shows an internal debug message	
124349	Debug	Adding authserver [server:%s]-[policy:%s] to stateful kerberos policy	This shows an internal debug message	
124350	Debug	mask [mask:%x], daymask [daymask:%x], curtime [time:%d] start [start:%d], end [end:%d]	This shows an internal debug message	
124351	Debug	curtime [current:%d], start [start:%d], end [end:%d]	This shows an internal debug message	
124352	Debug	TR: ABS start [time: %ld]	This shows an internal debug message	
124353	Debug	TR timeout: day [day:%d], hhmm [time:%d]	This shows an internal debug message	
124354	Debug	Delete service: [service:%s]	This shows an internal debug message	
124355	Debug	Delete destination: [name:%s]	This shows an internal debug message	
124356	Debug	invalid delete policy, matched: source [src:%d], dest [dest:%d], service [service:%d]	This shows an internal debug message	
124357	Debug	service [service:%s] and policy added in sys-ap-acl	This shows an internal debug message	
124358	Debug	service [service:%s] and policy deleted from sys-ap-acl	This shows an internal debug message	
124361	Debug	Ignoring firewall rule with unknown app [app:%s]	This shows an internal debug message	
124362	Debug	Regenerate ACL for policy [name:%s] app [app:%s]	Regenerate firewall rules due to application add or del event	

124363	Debug	Regenerate bwc for role [name:%s] app [app:%s]	Regenerate role-bandwidth-contract due to application add or del event	
124405	Debug	AUTH GSM: ADD bss [bssid:%s]: event=[ev:%d]	This shows an internal debug message	
124406	Debug	AUTH GSM: DEL bss [bssid:%s]: fol=[fol:%d]	This shows an internal debug message	
124407	Debug	AUTH GSM: ADD wired-ap [apip:%s]: event=[ev:%d]	This shows an internal debug message	
124408	Debug	AUTH GSM: DEL wired-ap [apip:%s]: fol=[fol:%d]	This shows an internal debug message	
124410	Debug	[func:%s](): IP:[bip:%s] exists in Bridge-User:[bmac:%s], Ignore it!	This shows an internal debug message	
124412	Debug	Replace bridge-ipuser [bipaddr:%s] with [newip:%s] due to too many IP[version:%s] address.	This shows an internal debug message	
124413	Debug	Free Bridge-ipuser [ipuser:%p] ([ipstr:%s]).	This shows an internal debug message	
124418	Debug	SNMP user entry request key [key:%x], ipaddr [ipaddr:%s].	This shows an internal debug message	
124419	Debug	SNMP user [user:%s] not found.	This shows an internal debug message	
124420	Debug	SNMP user entry request key [key:%x], ipaddr [ipaddr:%s].	This shows an internal debug message	
124423	Debug	SNMP station table request, MAC [mac:%s], BSSID [bssid:%s].	This shows an internal debug message	
124424	Debug	SNMP station [mac:%s], [bssid:%s] not found.	This shows an internal debug message	
124425	Debug	SNMP Essid table request, Essid [essid:%s].	This shows an internal debug message	
124432	Debug	[msg:%s]	This shows an internal debug message	
124433	Debug	cached vpn role is [role:%s]	This shows an internal debug message	
124434	Debug	fork failed, Cant change VLAN of user :[user:%s]	This shows an internal debug message	
124435	Debug	VIA: Failed to set default role for VIA Authentication Profile [profile:%s]	This shows an internal debug message	
124436	Debug	VIA: Next pin mode for user [user:%s]	This shows an internal debug message	
124437	Debug	VIA: Sending state attribute (len [len:%d]) in PAP response	This shows an internal debug message	
124438	Debug	VIA: Sending reply attribute (len [len:%d]) in PAP response	This shows an internal debug message	
124439	Debug	[function:%s]: user name [user:%s], check_cp_single_session ret [value:%d]	This shows an internal debug message	
124440	Debug	AP Authentication success. MAC: [mac:%s]	This shows an internal debug message	
124441	Debug	[function:%s]: vpnflags:[flags:%d]	This shows an internal debug message	
124442	Debug	Next pin mode for user [user:%s]	This shows an internal debug message	
124443	Debug	Sending state attribute (len [len:%d]) in PAP response	This shows an internal debug message	
124444	Debug	Sending reply attribute (len [len:%d]) in PAP response	This shows an internal debug message	
124445	Debug	auth_eap_resp_raw: sending resp ip:[ip:%s] cookie:[cookie:%d] len:[len:%d] result:[result:%d] radcode:[code:%d]	This shows an internal debug message	
124446	Debug	mschap2: found chap2 success attribute	This shows an internal debug message	
124447	Debug	[function:%s]: user name [user:%s], check_vpn_cp_single_session ret [result:%d]	This shows an internal debug message	
124448	Debug	VIA Authentication Profile is [profile:%s]	This shows an internal debug message	
124449	Debug	[function:%s]: Add user [user:%s] failed	This shows an internal debug message	
124450	Debug	[function:%s]: user [user:%s] not found	This shows an internal debug message	
124451	Debug	mschapv2 = [use:%u]	This shows an internal debug message	
124452	Debug	auth_eap_raw: recvd request ip:[address:%s] cookie:[cookie:%d] eaplen:[len:%d]	This shows an internal debug message	
124453	Debug	[function:%s]: response user:[user:%s] ip:[address:%s] cookie:[cookie:%d]	This shows an internal debug message	
124454	Debug	[function:%s]: recvd request user:[user:%s] ip:[address:%s] cookie:[cookie:%d]	This shows an internal debug message	
124455	Debug	[function:%s]: response result [result:%d], role [role:%s], user [user:%s]	This shows an internal debug message	
124456	Debug	[function:%s]: derive svr grp [group:%s], vp [attribute:%pI4]	This shows an internal debug message	
124457	Debug	[function:%s]: server grp [name:%s]	This shows an internal debug message	
124458	Debug	IP UP int: [address:%s], ext:[externalip:%s] flags [flags:%x]	This shows an internal debug message	
124459	Debug	IP DN int: [internalip:%s], ext:[externalip:%s]	This shows an internal debug message	
124460	Debug	[function:%s] No Radius Code ... ignoring pkt	This shows an internal debug message	

124461	Debug	[function:%s]:Invalid Radius Code [code:%d] ... ignoring pkt	This shows an internal debug message	
124462	Debug	[function:%s]: no valid radius secret	This shows an internal debug message	
124463	Debug	[function:%s]: no valid radius authenticator	This shows an internal debug message	
124464	Debug	[function:%s]: Got send key of len [len:%d]	This shows an internal debug message	
124465	Debug	[function:%s]: Got recv key of len [len:%d]	This shows an internal debug message	
124466	Debug	[function:%s]: Got chap key of len [len:%d]	This shows an internal debug message	
124467	Debug	Framed IP: found [ip:%x] (mask [mask:%x])	This shows an internal debug message	
124468	Debug	IP UPDATE int: [address:%s], old ext:[externalip:%s] new ext:[externalip2:%s]	This shows an internal debug message	
124469	Debug	RADIUS: DAC request received from DAC ip: [dac_ip:%s] with unsupported value [attr_val:%d] for service-type attribute	Aruba OS supports service-type attribute with value "Authorize Only" only. It will throw an error for any other value.	
124470	Debug	Disconnect type DAC request received from [dac_ip:%s] with service-type attribute	RFC 5176 specifies, service type attribute must not be included in Disconenct type DAC requests.	
124471	Debug	Silent Discard: DAC request received from DAC ip: [dac_ip:%s] with stale timestamp [timestamp:%d]	DAC request received with timestamp older than the configured window-duration, will be silently discarded	
124472	Debug	Duplicate DAC request received from the DAC ip: [dac_ip:%s], port: [port_no:%d] and radius identifier: [rad_identifier:%d]	Duplicate DAC request is received from the DAC.	
124473	Debug	Event timestamp attribute is missing in the DAC request from server [dac_ip:%s]	Event timestamp is configured as required in "aaa rfc-3576-server" configurations. With "event-timestamp-required" option enabled, error will be thrown for missing timestamp.	
124474	Debug	RADIUS: State attribute missing for COA type request from DAC [dac_ip:%s] with service-type attribute present.	For CoA type DAC request. If the service-type attribute is present and its value is "Authorize Only". Error cause 402 will be thrown	
124475	Debug	CoA type DAC request received from [dac_ip:%s] with State attribute, sending NACK	CoA type DAC request is received with State attribute and Service-type attribute value "Authorize Only". Negative acknowledgement will be sent back to DAC along with state attribute	
124499	Debug	Local-Override NetDestination:[dest:%s] VLAN:[vlan:%u] Offset:[offset:%u] TO IP:[ipaddr:%s].	This shows an internal debug message	
124501	Debug	Local-Override NetDestination:[dest:%s] VLAN:[vlan:%u] TO IP:[ipaddr:%s] MASK[mask:%s].	This shows an internal debug message	
124517	Debug	[enabledisable:%s] Rx DHCP for client: [mask:%d], sos-enable: [sosenable:%d].	This shows an internal debug message	
124518	Debug	No AAA profile found, [file:%s]:[line:%d].	This shows an internal debug message	
124519	Debug	dhcp_process_opt_77: Cannot find option 77 rule for client: [mac:%s]. ingress vlan is [vlan:%d].	This shows an internal debug message	
124521	Debug	DHCP OPT77: vlan=[vlan:%d] curvlan=[currvlan:%d] ingress_vlan=[ingressvlan:%d] native_vlan=[native:%d] assigned_vlan=[assigned:%d].	This shows an internal debug message	
124522	Debug	[func:%s]: Unable to lookup user [user:%s]	This shows an internal debug message	
124524	Debug	DHCP pkt received of len=[len:%d]	This shows an internal debug message	
124525	Debug	Error receiving packet from datapath, len=[len:%d]	This shows an internal debug message	
124526	Debug	Ignoring DHCP packet from trusted port: [portindex:%d]	This shows an internal debug message	
124527	Debug	ifmap modify:DHCP from user [mac:%s], op=[op:%d], len=[len:%d] packet=[dhcpone:%x]/[dhcptwo:%x].	This shows an internal debug message	
124528	Debug	rx_dhcp: DHCPRELEASE received.	This shows an internal debug message	
124529	Debug	[func:%s]: radius server '[name:%s]' host set to IP address '[radhost:%s]'.	This shows an internal debug message	
124530	Debug	[func:%s]: radius server '[name:%s]' host set to FQDN '[radhost:%s]'.	This shows an internal debug message	
124531	Debug	Select server for method=[method:%s], user=[user:%s], essid=[essid:%s].	This shows an internal debug message	
124532	Debug	matching FQDN '[fqdn:%s]' ...	This shows an internal debug message	
124533	Debug	Server=[serverip:%s], ena=[enable:%d], ins=[ins:%d] type=[type:%s].	This shows an internal debug message	
124534	Debug	essid_list:[essidlist:%s].	This shows an internal debug message	

124535	Debug	fqdn_list:[fqdnlist:%s].	This shows an internal debug message	
124536	Debug	Select fail-thru server for method=[method:%s], user=[user:%s], essid=[essid:%s], cur server=[server:%s].	This shows an internal debug message	
124537	Debug	skip server=[server:%s], ena=[enable:%d], ins=[ins:%d] type=[type:%s].	This shows an internal debug message	
124538	Debug	Unknown Server type ([type:%d]) in Server List: [serverlist:%s].	This shows an internal debug message	
124539	Debug	Adding authserver [name:%s]-[ipaddr:%s]:[authport:%d] to stateful dot1x policy.	This shows an internal debug message	
124540	Debug	Removing authserver [name:%s]-[ipaddr:%s]:[authport:%d] from stateful dot1x policy.	This shows an internal debug message	
124541	Debug	Bring all servers in server group [grpname:%s] back in service.	This shows an internal debug message	
124543	Debug	TACACS+ accounting successful result=[rs:%s]([ri:%d]), method=[m:%s] for user [user:%s] server [server:%s].	This shows an internal debug message	
124544	Debug	Timed Out to [timeout:%s].	This shows an internal debug message	
124545	Debug	Fail-thru to [servername:%s].	This shows an internal debug message	
124546	Debug	[func:%s] user:[username:%s] vpnflags:[vpnflags:%d].	This shows an internal debug message	
124547	Debug	[func:%s] server_group:[grpname:%s].	This shows an internal debug message	
124548	Debug	Invalid server type in : "[srvgrp:%s]", Skipping TACACS+ [tacacs_type:%s].	This shows an internal debug message	
124549	Debug	init_acl: publish ACl download start message.	This shows an internal debug message	
124550	Debug	{ACL} Generate [count:%d] ace entries for acl ([aclnum:%d],[aclname:%s]) @ [aclindex:%d].	This shows an internal debug message	
124552	Debug	{ACL} GENACL([aclname:%s]:[aclnum:%d]): need [count:%d], available [avail:%d], free [aclfree:%d].	This shows an internal debug message	
124553	Debug	Reinitializing ACL table.	This shows an internal debug message	
124554	Debug	Reinitialize: Auth Config Time: [tvsec:%ld].[tvusec:%ld] sec.	This shows an internal debug message	
124555	Debug	Reinitialize: Downloads to SOS :: ACL: [acl:%d] ACE: [ace:%d].	This shows an internal debug message	
124556	Debug	{ACL} Free ace entries: (acl [acl:%d]).	This shows an internal debug message	
124557	Debug	aces [aces:%d] @ index [index:%d], next [next:%d].	This shows an internal debug message	
124559	Debug	{ACL} Generating ACE for access-list [aclname:%s] (ACL [aclnum:%d]).	This shows an internal debug message	
124560	Debug	{ACL} [acebuf:%s].	This shows an internal debug message	
124561	Debug	{ACL} Downloading ACL number/ACE(s) [acl:%d]/[entries:%d] -> index [index:%d] to sibyte acl_num [aclnum:%d].	This shows an internal debug message	
124562	Debug	{ACL} Downloading Bulk ACL Msg {[msglen:%d] len} {[acls:%d] acls} and {[aces:%d] aces} to sibyte. Accumulated download counts: acl [acl:%d] ace [ace:%d].	This shows an internal debug message	
124563	Debug	ACLHIT: acl([acl:%s])=[aclnum:%d] (type [acltype:%s]), index=[index:%d], TableId=[tableid:%d], index0=[index0:%d].	This shows an internal debug message	
124564	Debug	hits{[index:%d]}=[hits:%d].	This shows an internal debug message	
124565	Debug	ACLHIT: acl([acl:%s])=[aclnum:%d] (type [acltype:%s]), index=[index:%d], TableId=[tableid:%d], index0=[index0:%d], hits=[hit:%d].	This shows an internal debug message	
124566	Debug	Port ACLHIT: acl([acl:%s])=[aclnum:%d] (type [acltype:%s]), index=[index:%d], TableId=[tableid:%d], index0=[index0:%d], hits=[hit:%d].	This shows an internal debug message	
124567	Debug	[insert:%s] standard ACL [aclname:%s].	This shows an internal debug message	
124568	Debug	ACL [name:%s] (#[aclnum:%d]) [insert:%s].	This shows an internal debug message	
124569	Debug	[insertdelete:%s] Extended ACL [aclname:%s].	This shows an internal debug message	
124570	Debug	Source Port [sport:%d]-[sport16:%d], Op [srcop:%d] ACE count [srcace:%d].	This shows an internal debug message	
124571	Debug	Destination Port [dport:%d]-[dport16:%d], Op [dstop:%d] ACE count [dstace:%d].	This shows an internal debug message	

124572	Debug	Source IP [sip:%s], Wildcard bits [wildbits:%s].	This shows an internal debug message	
124573	Debug	Destination IP [dip:%s], Wildcard bits [wildbits:%s].	This shows an internal debug message	
124574	Debug	ICMP config type [icmptype:%s] code [icmpcode:%s].	This shows an internal debug message	
124575	Debug	ICMP config msg [msg:%s] (index=[index:%d]).	This shows an internal debug message	
124576	Debug	ICMP type [icmptype:%d], code [icmpfcode:%d]-[lcode:%d].	This shows an internal debug message	
124577	Debug	IGMP config type [igmptype:%s].	This shows an internal debug message	
124578	Debug	IGMP config msg [msg:%s] (index [index:%d]).	This shows an internal debug message	
124579	Debug	IGMP type [type:%d].	This shows an internal debug message	
124580	Debug	action flag [action:%d].	This shows an internal debug message	
124581	Debug	Generating [ace:%d] ace entries.	This shows an internal debug message	
124582	Debug	ACL [num:%s] (#[no:%d]) [insdel:%s].	This shows an internal debug message	
124583	Debug	[insdel:%s] MAC ACL [acl:%s].	This shows an internal debug message	
124584	Debug	Source MAC [mac:%s] mask [mask:%s].	This shows an internal debug message	
124585	Debug	[insdel:%s] ETHERTYPE ACL [aclname:%s].	This shows an internal debug message	
124586	Debug	Ethertype [ether:%x], Wildcard bits [wildbits:%x].	This shows an internal debug message	
124587	Debug	[insdel:%s] QINQ ACL [name:%s].	This shows an internal debug message	
124588	Debug	acl [accname:%s], [insdel:%s]: outer-vlan [outermin:%d]-[outermax:%d], inner-vlan [innermin:%d]-[innermax:%d], action1 [outeract:%d]([outervlan:%d]), action2 [inneract:%d]([innervlan:%d]).	This shows an internal debug message	
124589	Debug	Sending remove acl [name:%s]:[aclnum:%d] to fpapps.	This shows an internal debug message	
124590	Debug	Sending insert acl [name:%s]:[aclnum:%d] to fpapps.	This shows an internal debug message	
124591	Debug	{ACL} Sending pkt trace ACL [acl:%d] -> [index:%d] to sibyte tmask [tmask0:%x] [tmask1:%x].	This shows an internal debug message	
124592	Debug	Configuring pkttrace ACL for tracing packets "matching the ACL '[name:%s]' [trace:%s].	This shows an internal debug message	
124593	Debug	{ACL} Sending packet trace info [acl:%d] -> [index:%d] to sibyte tmask [tmask0:%x] [tmask1:%x].	This shows an internal debug message	
124594	Debug	RAP Packet-trace Disable: AP: [apip:%s].	This shows an internal debug message	
124595	Debug	RAP Packet-trace Enable: Type: [type:%u], AP: [apip:%s], ACL-Id: [val:%u], Ingress: [devname:%s], TraceMask: [mask:%x].	This shows an internal debug message	
124600	Debug	No Fail-thru because it is dot1x without termination.	This shows an internal debug message	
124601	Debug	Switch to Survival-Server:[svr:%s] due to [reason:%s].	This shows an internal debug message	
124602	Debug	[func:%s]([proto:%s]): Sent Access credential([type:%s]) to Survival-Server for station:[st:%s] username:[uname:%s] survMethod:[smethod:%x].	This shows an internal debug message	
124604	Debug	[func:%s]([proto:%s]): Sent Deleting Access credential to Survival-Server for station:[st:%s] username:[uname:%s] survMethod:[smethod:%x].	This shows an internal debug message	
124607	Debug	[func:%s](): response=[resp:%d] from Auth server '[svr:%s] for client:[client:%d] proto:[proto:%d] eap-type:[eaptype:%d]'.	This is an internal debug message	
124609	Debug	[func:%s](): Time-Out on Auth-server '[svr:%s]'.	This is an internal debug message	
124610	Debug	[func:%s](): Not storing Survival credential for zero-mac, ip:[ip:%s] username:'[uname:%s]'.	This is an internal debug message	
124611	Debug	[func:%s](): Not deleting Survival credential for zero-mac, ip:[ip:%s] username:'[uname:%s]'.	This is an internal debug message	
124612	Debug	[func:%s](authsurv:[enabled:%d]): Entered, proto:[proto:%d] eap-type:[eaptype:%x] for username:'[uname:%s]' auth-server:'[authsvr:%s]' server-group:'[sg:%s]' AnyRadLdapInOOS:'[inoos:%s]'.	This is an internal debug message	
124613	Debug	[func:%s](authsurv:[enabled:%d]): Can not use Survival-server with DOT1X and non-Termination for username:'[uname:%s]'.	This is an internal debug message	

124614	Debug	[func:%s]([proto:%s]): EAP-Type([type:%s]) is NOT supported in Auth-Survivability for station:[st:%s] username:[uname:%s].	This indicates an EAP-Type is NOT supported for Auth-Survivability	
124615	Debug	[func:%s](proto:[proto:%d]): Sending to '[sname:%s]' with survMethod:[smeth:%x].	Sending an authentication request to Survival Server	
124616	Debug	[func:%s](RAW-PEAP): Could NOT obtain ARUBA_USER_NAME or ARUBA_NT_HASH from Server:'[svrname:%s]' for station:[st:%s] username:[uname:%s].	This shows an internal debug message	
124617	Debug	[func:%s](): No-Action on Access Credential for Un-Supported protocol([proto:%d]) in Auth-Surv.	This shows an internal debug message	
124626	Debug	Sending auth up message to web server	This shows an auth security internal debug message	
124627	Debug	Sending acl download complete message to fastpath server	This shows an auth security internal debug message	
124628	Debug	Send update message to emweb (type [type:%d], len [len:%d])	This shows an auth security internal debug message	
124629	Debug	Updating acl to redirect captive portal request for profile:[prof_name:%s]	This shows an auth security internal debug message	
124630	Debug	Updating acl to redirect captive portal request for profile:[prof_name:%s] to mswitch	This shows an auth security internal debug message	
124631	Debug	Updating V6 acl to redirect captive portal request for profile:[prof_name:%s]	This shows an auth security internal debug message	
124632	Debug	Updating V6 acl to redirect captive portal request for profile:[prof_name:%s] to mswitch6	This shows an auth security internal debug message	
124633	Debug	Opened CP customization file [line:%s]	This shows an auth security internal debug message	
124634	Debug	theme=[msg_theme:%d], logo=[logo:%s], logintext=[logintext:%s], policytext=[policytext:%s]	This shows an auth security internal debug message	
124635	Debug	custom color=[custom_color:%s], background=[background:%s] login_page=[login_page:%s] welcome_page=[welcome_page:%s]	This shows an auth security internal debug message	
124636	Debug	Received CP/WISPr cfg request from station:[station:%s] ip:[ip:%s]	This shows an auth security internal debug message	

124637	Debug	Received CP/WISPr cfg with userip NULL station:[station:%s] This shows an auth security internal debug message 124638@cp_dns_ip: [cp_dnsip:%s] This shows an auth security internal debug message 124639@station=[mac:%s],ip=[userip:%s], prof=[prof:%s], essid=[essid:%s], login=[login:%s], wispr_enable=[wispr_enable:%d] This shows an auth security internal debug message 124640@Received Captive Portal/WISPr config request for [cpdns_ip:%s] This shows an auth security internal debug message 124641@Got update from emweb [msg_type:%d],[msg_len:%d],[msg_value:%s] This shows an auth security internal debug message 124642@Sygate configuration file [fp:%s] This shows an auth security internal debug message 124643@-> [line::%s] This shows an auth security internal debug message 124644@Sending config msg ([type:%d]) for CP profile '[cp_prof_name:%s]' (wl=[wl:%d], bl=[bl:%d] This shows an auth security internal debug message 124645@WG WL [wl:%s] This shows an auth security internal debug message 124646@[cp:%s] This shows an auth security internal debug message 124647@Received WG request This shows an auth security internal debug message 124648@Trigger WG config update (destination '[name:%s]') This shows an auth security internal debug message 124649@Missing CP profile [cp_prof:%s]"	This shows an auth security internal error message	
124650	Debug	Station :[mac:%s] Remove user :[user_ip:%s] from datapath because it is not found in AUTH	This shows an auth security internal error message	
124651	Debug	Missing WISPr profile [wispr_prof_name:%s] for station:[mac:%s] ip:[ip:%s]	This shows an auth security internal error message	
124652	Debug	Missing CP profile [cp_prof:%s] for station:[mac:%s], ip:[userip:%s]	This shows an auth security internal error message	
124653	Debug	Internal Error occurred while showing web-server protocol configuration	This shows an auth security internal error message	
124654	Debug	Internal Error occurred while saving web-server protocol configuration	This shows an auth security internal error message	
124655	Debug	Internal Error occurred while saving cpdns configuration	This shows an auth security internal error message	
124656	Debug	Missing user entry for IP address "[ip:%s]"	This shows an auth security internal error message	
124657	Debug	Internal Error occurred while saving sygate configuration	This shows an auth security internal error message	
124684	Debug	AAA restarted.	This shows an internal debug message	
124687	Debug	AP-GROUP:[groupid:%d] Group Name: [grpname:%s] released.	This shows an internal debug message	
124688	Debug	AP-GROUP:[groupid:%d] Name: [grpapname:%s] AP-Name: [apname:%s] added.	This shows an internal debug message	
124689	Debug	AP-GROUP:[apgroupid:%d] Name: [groupname:%s] AP-Name: [apname:%s] freed.	This shows an internal debug message	
124690	Debug	Couldn't create/find bandwidth-contract for [contractname:%s] ap-Group [apgroup:%s] role [role:%s] return-code [retcode:%d].	This shows an internal debug message	
124691	Debug	AP-GROUP:[apgroup:%d] Name: [apname:%s] Role Name: [rolename:%s] BW-ID: [bwid:%d] allocated, Caller:[caller:%p].	This shows an internal debug message	
124692	Debug	AP-GROUP:[apgroup:%d] Name: [groupname:%s] Role Name: [rolename:%s] BW-ID: [bwid:%d] incremented, Caller:[caller:%p].	This shows an internal debug message	

124693	Debug	AP-GROUP:[apgroup:%d] Name: [apgroupname:%s] BW-ID: [bwid:%d] decremented, Caller:[caller:%p].	This shows an internal debug message	
124694	Debug	AP-GROUP:[apgroup:%d] AP-Name:[apgroupname:%s] released BW Contract:[bwcontract:%d].	This shows an internal debug message	
124695	Debug	AP-GROUP:[apgroup:%d] released role :[role:%s].	This shows an internal debug message	
124696	Debug	AP-GROUP:[apgroup:%d] BW Contract:[bwcontract:%d] freed.	This shows an internal debug message	
124698	Debug	cfg_netdst: user can not modify netdestination vrrp_ip	This shows an internal error message	
124699	Debug	User can't modify pre-defined netdestination [netdestname:%s].	This shows an internal error message	
124700	Debug	cfg_netdst: insert=[insert:%d], addr=[address:%x], mask=[mask:%x], type=[type:%d].	This shows an internal error message	
124701	Debug	cfg_netdst([line:%d]): Config destination [name:%s] host/network/range [addr:%x] [mask:%x] [invertstr:%s].	This shows an internal error message	
124702	Debug	New entry addition to netdestination '[name:%s]' used [ace:%d] aces.	This shows an internal error message	
124703	Debug	Continuing show_netdst from [start:%s].	This shows an internal error message	
124705	Debug	setup_pppeapctx: creating pppeapctx cookie:[cookie:%d].	This shows an internal error message	
124706	Debug	free_pppeapctx: deleting pppeapctx cookie:[cookie:%d].	This shows an internal error message	
124804	Debug	VIA: auth_profile '[auth:%s]' is NULL.	This shows an internal error message	
124805	Debug	VIA: ssid_profile '[ssid:%s]' is NULL.	This shows an internal error message	
124806	Debug	VIA: wlan_profile '[wlan:%s]' is NULL.	This shows an internal error message	
124807	Debug	VIA: Error sending message MSG_VIA_IPSEC_CONFIG_REQ to IKE_DAEMON.	This shows an internal error message	
124808	Debug	fw_add_name: i'[name:%s]' found; reusing ID [id:%d]).	This shows an internal error message	
124809	Debug	Assign hostname id [id:%d] to name '[name:%s]'.	This shows an internal error message	
124810	Debug	fw_del_name: invalid ID [id:%d] for deletion.	This shows an internal error message	
124811	Debug	Delete hostname id [host:%d] from name '[name:%s]'.	This shows an internal error message	
124813	Debug	Downloading DNS name {action=[action:%d], id=[id:%d], name=[name:%s]} to sibyte.	This shows an internal error message	
124814	Debug	[string:%s]	This shows captive-portal internal debug message	
124817	Debug	IAP subnet add: [address:%s], [mask:%s]	This shows an internal debug message	
124818	Debug	IAP subnet del: [address:%s], [mask:%s]	This shows an internal debug message	
124820	Debug	[_function_:%s] Sending STM deauth: AP [bssid:%s] [mac:%s]	This shows an internal debug message	
124823	Debug	Null sacl or policy received by policy_uncfg	This shows an internal debug message	
124824	Debug	Null sacl or acl received by generate_acl_sacl	This shows an internal debug message	
124825	Debug	Invalid: [authtype:%d] OR [msgtype:%d].	This shows an internal debug message	
124829	Debug	ENET msg: ENET Tunnel DOWN, ip: [ip:%s], port: [enet_port:%u]	This shows an internal debug message	
124832	Debug	Dldb Role [name: %s]: Role version [number: %d], is deprecated	This shows an internal debug message	
124833	Debug	Dldb Role [name: %s]: Role has no user references	This shows an internal debug message	
124834	Debug	Dldb Role [name: %s]: Waiting for removal of deprecated older version	This shows an internal debug message	
124835	Debug	Dldb Role [name: %s]: Request for role from first user	This shows an internal debug message	
124836	Debug	Dldb Role [name: %s]: Role request sent to CPPM at [ip: %s]	This shows an internal debug message	
124837	Debug	Dldb Role [name: %s]: Curl cleanup done for role request	This shows an internal debug message	
124838	Debug	Dldb Role [name: %s]: Start timer type [str: %s]([type: %d]) duration [time: %u]	This shows an internal debug message	
124839	Debug	Dldb Role [name: %s]: Timer type [type: %d] expired	This shows an internal debug message	
124840	Debug	Dldb Role [name: %s]: Received role	This shows an internal debug message	
124841	Debug	Dldb Role [name: %s]: Role transformation done	This shows an internal debug message	
124842	Debug	Dldb Role [name: %s]: Sent cmd "[cmd: %s]" to reset mode	This shows an internal debug message	
124843	Debug	Dldb Role [name: %s]: Sent cmd idx: [idx: %d] "[cmd: %s]"	This shows an internal debug message	
124844	Debug	Dldb Role [name: %s]: Sent last cfg cmd, no more commands	This shows an internal debug message	
124845	Debug	Dldb Role [name: %s]: Cmd exec retry [count: %d] times	This shows an internal debug message	

124846	Debug	Dldb Role [name: %s]: cmd idx [idx: %d] ACK recvd	This shows an internal debug message	
124847	Debug	Dldb Role [name: %s]: Sent last revert cmd, no more commands	This shows an internal debug message	
124848	Debug	Dldb Role [name: %s]: Old role version removed	This shows an internal debug message	
124849	Debug	[Dormant:%s] Dldb Role [name: %s]: Last departure from role, start destroy	This shows an internal debug message	
124850	Debug	[Dormant:%s] Dldb Role [name: %s]: Dequeue pending users, total enqueued [count: %d]	This shows an internal debug message	
124851	Debug	Dldb Role [name: %s]: Role locked from modifications	This shows an internal debug message	
124852	Debug	Dldb Role [name: %s]: Start destroying role	This shows an internal debug message	
124853	Debug	Dldb Role [name: %s]: Skip destroy role, [reason: %s]	This shows an internal debug message	
124854	Debug	Dldb Role [name: %s]: Role sucessfully destroyed	This shows an internal debug message	
124855	Debug	Dldb Role [name: %s]: Admin requested role removal	This shows an internal debug message	
124859	Debug	Auth GSM : IP_USER publish for IP [ip: %s] uuid [uuid: %s]	This shows an internal debug message	
124861	Debug	Auth GSM : IP_USER delete for IP [ip: %s]	This shows an internal debug message	
124862	Debug	Auth GSM : IP_USER delete failed for IP [ip: %s] result [res: %s]	This shows an internal debug message	
124863	Debug	Auth GSM : IP_USER notify for mac [mac:%s] ip:[ip:%s] pan-integ:[pn:%s] - [auth:%s]	This shows an internal debug message	
124868	Debug	[string:%s]	This shows an amon auth internal debug message	
124871	Debug	Dldb Role [name: %s]: Not replaying - deleting as referred role is invalid	This shows an internal debug message	
124872	Debug	Dldb Role [name: %s]: Not replaying - config transform has failed	This shows an internal debug message	
124873	Debug	Dldb Role [name: %s]: Role reset, replaying	This shows an internal debug message	
124875	Debug	Continuing show_user_role_references from [start:%s].	This shows an internal error message	
124878	Debug	[_function_:%s]:[_line_:%d] Updating vlan usage for MAC=[mac:%s] with vlan [vlan:%d] apname [apname:%s]	This shows an internal debug message	
124882	Debug	Auth GSM : IP USER publish Success for IP [ip: %s] [rep_key: %d]	This shows an internal security debug message	
124884	Debug	Auth GSM : IP USER change repkey Success for IP [ip: %s] [rep_key: %d]	This shows an internal security debug message	
124885	Debug	[string:%s]	This shows an internal cluster debug message	
124886	Debug	Auth recvd DHCP packet from [mac:%s] with client hardware address 0, ignoring packet	This shows an internal error message	
124887	Debug	USER roamed to a different AP. Ignoring handle_rap_bridge_user old bss:[obss: %s] new bss:[nbss: %s]	This shows an internal security debug message	
124890	Debug	Added the [mac:%s] to the AP sta list [ip:%s]	This shows an internal error message	
124894	Debug	[func:%s]: Executing internal cmd [cmd:%s]	This shows an internal error message	
124895	Debug	[func:%s]: action [action:%s] for appname [appname:%s] id [appid:%d]	This shows an internal debug message	
124896	Debug	[Dormant:%s] Dldb Role [name: %s]: Last via user departs from role, start destroy	This shows an internal debug message	
124897	Debug	[function:%s]: User query received user [user:%s] server-group [svrgrp:%s]	This shows an internal debug message	
124898	Debug	[function:%s](): Set dynamic group bwm contract '[bname:%s]' ([type:%d]/[id:%d]) to [rate:%llu] bits/sec	This shows an internal debug message	
124899	Debug	[function:%s](): Set dynamic individual bwm contract '[bname:%s]' ([type:%d]/[id:%d]) to [rate:%llu] bits/sec	This shows an internal debug message	
124901	Debug	[file:%s][line:%d]: Sending port shutdown request to fpapps for user [mac:%s] [port:%s] [port_down_time:%d]s	Send port bounce request to FPAPPS for the wired user	
124902	Debug	[function:%s](): Received VSA value, port downtime [time:%d]s	This shows an internal debug message	
124904	Debug	[function:%s]: Skipping port bounce VSA as user mac [mac:%s] is not a wired user	This shows an internal debug message	
124905	Debug	[function:%s]: Received PAPI response after sending port bounce: [ret:%d] for wired user [mac:%s]	This shows an internal debug message	

124906	Debug	Sending netdestination update to SOS - Name:[name:%s] action:[action:%d] id:[id:%d] v6:[v6:%d] index:[index:%d] count:[count:%d] curr_count:[curr_count:%d] more:[more:%d] offset:[offset:%d] multipart:[multipart:%d]	This shows an internal debug message	
124907	Debug	Sending netdestination update to STM - Name:[name:%s] action:[action:%d] id:[id:%d] v6:[v6:%d] index:[index:%d] count:[count:%d] curr_count:[curr_count:%d] more:[more:%d] offset:[offset:%d] multipart:[multipart:%d]	This shows an internal debug message	
124910	Debug	User Delete Response received from local switch [localip:%s], with inactive or invalid request ID: [request_id:%d]	This shows an internal debug message	
124911	Debug	User delete request, command string : [req:%s] , is received from conductor	This shows an internal debug message	
124912	Debug	Stale response to aaa user delete request id: [request_id:%d], received at conductor from the local switch [localip:%s]	This shows an internal debug message	
124913	Debug	Timeout value for user delete request to local switches, changed to [Timeout:%d] minutes	This shows an internal debug message	
124917	Debug	Received timeout for ACL msg - acl [acl:%d]	This shows an internal debug message	
124918	Debug	Received timeout for ACE msg - ace [ace:%d]	This shows an internal debug message	
124919	Debug	Received timeout for BULK_ACL_ACE msg with num_acls [acls:%d] num_aces [aces:%d]	This shows an internal debug message	
124920	Debug	Received timeout for BULK_ACL msg with num_acls [acls:%d]	This shows an internal debug message	
124921	Debug	Received timeout for BULK_ACE msg with num_aces [aces:%d]	This shows an internal debug message	
124922	Debug	Reconstruct ACL msg for acl id [acl:%d] name [aclname:%s]	This shows an internal debug message	
124923	Debug	Reconstruct ACE msg for ace [ace:%d]	This shows an internal debug message	
124924	Debug	Received OpenFlow msg type [type:%d]; Stats: msgs [msg:%d] rsp [rsp:%d] init [init:%d] add_mod [add:%d] del [del:%d] upd_acl_ver [aclver:%d]	This shows an internal debug message	
124928	Debug	Allocated alias-rule hits for ACL name [aclname:%s] type [type:%s]	This shows an internal debug message	
124929	Debug	Freed alias-rule hits for ACL name [aclname:%s] type [type:%s]	This shows an internal debug message	
124930	Debug	Allocated id [id:%d] for netdestination [destname:%s]	This shows an internal debug message	
124931	Debug	Freed id [id:%d] set for netdestination [destname:%s]	This shows an internal debug message	
124933	Debug	Reconstruct netdest msg for netdestination id [dstid:%d] name [dstname:%s]	This shows an internal debug message	
125015	Debug	Notify auth: [operation:%s] mgmt-role '[role_name:%s]'	Debug message notification on add/delete of management user	
125016	Debug	[callback] Notify auth: mgmt-role '[role_name:%s]' added	Internal message subscription request on adding of management user	
125019	Debug	Checking for Radius Authentication	Debug message to indicate that a check is being performed for radius authentication	
125026	Debug	Radius Authentication is enabled	Debug Message indicating that the radius authentication is enabled	
125027	Debug	mgmt-auth: [user_name:%s], [result:%s], [role_name:%s], [priv_mode:%d]	Debug Message displaying management user details	
125029	Debug	Checking for Radius Authentication	Debug Message indication the call flow that a check for radius authentication is being made	
125034	Debug	Starting AAA...	Debug message indicating the initiation of AAA	
125035	Debug	Syncing with Config Manager...	Debug message indicating the start of internal initiation of AAA	
125036	Debug	Retrieving Config from Config Manager...	Debug message indicating the start of internal receiving of configuration	
125037	Debug	Done Retrieving Config from Config Manager...	Debug message indicating the success of internal receiving of configuration	
125038	Debug	Done Syncing with Config Manager...	Debug message indicating the completion of internal sync of configuration	
125039	Debug	AAA task is initialized	Debug message indicating AAA is ready	
125050	Debug	[[file:%s]:[line:%d]] [message:%s]	aaa module's debug message	
129001	Debug	[msg:%s]		

132007	Debug	Clearing Station state on AP [bssid:%m]	Station is forced to be cleared from the AP's stations table	
132022	Debug	Station [mac:%m] [bssid:%m] sent 802.1x packet before association/l2 miss - dropping packet	Received an EAP packet from the station before receiving an association/l2 miss message. This log-message is generated when we detect a race-condition between STM, SOS and AUTH. AUTH is receiving association-request messages from STM before it received the L2-Miss message from SOS. If symptoms persist, then AUTH is either not receiving or not processing L2-Miss messages from SOS. Restart the AUTH process by executing "process restart auth" or reload the controller.	
132047	Debug	Disabling Stateful 802.1x - removing all Stateful Config entries	Removing all the stateful dot1x config entries that was created	
132213	Debug	Failed to perform revocation check for client cert	Auth failed to contact certmgr to perform revocation check for client cert	
132214	Debug	Client certificate for mac [mac:%m] and bssid [bssid:%m] has been revoked	Client certificate has been revoked	
132215	Debug	Client certificate for mac [mac:%m] and bssid [bssid:%m] has NOT been revoked	Client certificate has not been revoked	
132216	Debug	Revocation check request for mac [mac:%m] and bssid [bssid:%m] sent to certmgr	Auth sent a revocation check request to certmgr process	
132220	Debug	Debug Log	Debug Log	
132223	Debug	EAP-ID mismatched [id1:%d]:[id2:%d] for station [mac:%m] [bssid:%m]	Mismatch between the eapid station sent and what was expected	
132227	Debug	EAPOL-Logoff ignored for station [mac:%m] [bssid:%m]	EAPOL-Logff ignored for the specific station	
132228	Debug	Station [mac:%m] got stm-msg with bssid = [bssid:%m] while sap-bssid = [sapbssid:%m]	Should not delete the specified station for this station down	
132231	Debug	Client-Cert[[cert:%s]] verification failed with Issuer Not found - [errstr:%s]([err:%d]). Try to check if it's trusted	Client cert failed verification due to Issuer not found	
132232	Debug	Client-Cert[[cert:%s]] verification OK with Trusted IntermediateCA[[errcert:%s]]	Overrule the Client cert verification to be OK since the IntermediateCA is trusted	
132234	Debug	Failed to verify Client-Cert[[cert:%s]], error=[errstr:%s]([err:%d])	Client cert failed verification	
133028	Debug	[func:%s]([sip:%s]:[sport:%u] ==> [dip:%s]:[dport:%u] PktType:[pktp:%x] SeqNum:[seq:%u] MsgCode:[mcode:%u]): Received udb_msg with msgtype:[msgtype:%u] id:[id:%u] reqtype:[reqtype:%d] dbtype:[dbtype:%d]	This indicates a udb-msg is received at udbserver with detailed info	
133032	Debug	[func:%s]: Sending Fetch-Req on WL-entry for mac [mac:%s] to [dip:%s]:[dport:%u] with msgtype:[msgtype:%u] id:[id:%u] reqtype:[reqtype:%u] dbtype:[dbtype:%u]	This shows deatils about a Fetch-Request message is sent from udbserver to conductor	
133050	Debug	Client process called auth_db_response_handler [msgtype: %d] [name: %s]	Client process executed auth_db_query_db_async()	
133051	Debug	[function: %s] Received unknown [msgtype: %d] [name: %s]	AUTH DB_API cannot process unknow message-type	
133053	Debug	[function: %s] Cannot process unknown [datatype: %d] [name: %s]	AUTH DB_API cannot process unknown data type	
133054	Debug	[function: %s] Cannot create hash table [msgtype: %d] [name: %s]	AUTH DB_API failed to create hash table	
133055	Debug	[function: %s] Failed to insert entry into hash table [msgtype: %d] [name: %s]	AUTH DB_API failed to insert entry into hash table	
133058	Debug	[function: %s] Name too long [name: %s]	AUTH DB_API primary key too long	
133059	Debug	[function: %s] Failed to create tracking state [name: %s]	AUTH DB_API failed to create tracking state	
133060	Debug	[function: %s] Failed to find valid tracking state [name: %s][msgtype: %d]	AUTH DB_API failed to find valid tracking state	
133061	Debug	[function: %s] Failed to find tracking state [name: %s][msgtype: %d]	AUTH DB_API failed to find tracking state	
133062	Debug	[function: %s] Failed [name: %s]	AUTH DB_API call failed	
133063	Debug	[function: %s] Received invalid msg from [SrcAddr: %s] [SrcPort: %d] [code: %d]. Bad Magic number.	AUTH DB_API received invalid msg. Bad Magic number	
133066	Debug	[function: %s] Querying for highest sequence number [table: %s] [seqnum: %d]	LOCALDB_SYNC querying for highest sequence number	
133089	Debug	[function: %s] Sending AP_DOWN msg to SAPM [mac: %s]	Sending AP_DOWN msg to SAPM	

133090	Debug	[function: %s] Failed to parse CLI request	Failed to parse CLI request	
133091	Debug	[function: %s] Processing ADD request [name: %s]	Processing ADD request	
133092	Debug	[function: %s] Processing DEL request [name: %s]	Processing DEL request	
133093	Debug	[function: %s] Processing UPDATE request [name: %s]	Processing UPDATE request	
133094	Debug	[function: %s] Processing QUERY request [name: %s]	Processing QUERY request	
133095	Debug	[function: %s] UDB API process failure. [name: %s] [error: %d] [dp: %d]	Upgrading database	
133108	Debug	[string:%s]	This shows an internal debug message	
133112	Debug	[string:%s]	This shows an internal database transaction debug message	
133113	Debug	Querying local switch list	LOCALDB_SYNC querying local switch list	
133122	Debug	[func:%s]: Sending response to [dip:%s]:[dport:%u] with msgtype:[msgtype:%u] id:[id:%u] reqtype:[reqtype:%u] dbtype:[dbtype:%u]	This shows deatils about a response message is sent from udbserver	
133125	Debug	Unsupported message(MsgCode:[mcode:%u]) from [sip:%s]:[sport:%u] is received at udbserser.	This indicates unsupported message is received at udbserver	
133128	Debug	[func:%s]: Sending request to [dip:%s]:[dport:%u] with msgtype:[msgtype:%u] id:[id:%u]	This shows details about a request message is sent to udbserver	
133508	Debug	Setting [switch_list_tbl:%s] [macaddr:%s] [ipaddr:%s] seq_num=[seq_num:%d] r_seq_num=[remote_seq_num:%d] r_last_seq=[r_last_seq:%d] null_count=[null_count:%d]	Create/Update switch-list-entry	
133509	Debug	Purging sequence-numbers in [switch_list_tbl:%s]	Purging sequence-numbers in switch-list-tbl	
133510	Debug	Sending db_sync msg msg_type=[msg_type:%d] to [ipaddr:%s] msg_size=[msg_len:%d]	Sending message to remote switch	
133511	Debug	Received db_sync msg msg_type=[msg_type:%d] from [ipaddr:%s] msg_size=[msg_len:%d]	Received db_sync message from remote switch	
133516	Debug	Permanently deleting entries in [db_tbl:%s] seq_num less than or equal to [seq_num:%d]	Delete entries in db_tbl marked for deletion	
133517	Debug	Syncronizing virtual-clock with system clock [ti_delta:%d]	Syncronizing virtual-clock with system clock	
133518	Debug	Scan [db_type:%s] for [entry:%s] and begin db_sync time=[time:%d]	Start db_sync scan	
133519	Debug	Send sync_req message to [ipaddr:%s] [db_type:%s] [switch_db_type: %s] prev_seq=[prev_seq:%d] seq_num=[seq_num:%d] num_rec=[num_recs:%d] t_i=[ti:%d] t_c=[time:%d]	Send db_sync request	
133520	Debug	Received sync_req message from [ipaddr:%s] [db_type:%s] [switch_db_type: %s] prev_seq=[prev_seq:%d] seq_num=[seq_num:%d] num_rec=[num_recs:%d] r_t_i=[ti:%d] r_t_c=[time:%d]	Receive db_sync request	
133521	Debug	Send sync_rsp message to [ipaddr:%s] [db_type:%s] [switch_db_type: %s] seq_num=[seq_num:%d] t_c=[time:%d] result=[result:%d]	Send db_sync response	
133522	Debug	Received sync_rsp message from [ipaddr:%s] [db_type:%s] [switch_db_type: %s] seq_num=[seq_num:%d] r_t_c=[time:%d] result=[result:%d]	Receive db_sync response	
133526	Debug	Skipping db_sync for [ipaddr:%s] [macaddr:%s]	Skipping db_sync for a switch	
133530	Debug	[string:%s]	This shows an internal CPSEC debug message	
133532	Debug	[string:%s]	This shows an internal WL Sync debug message	
133533	Debug	Skipping db_sync for [ipaddr:%s] [macaddr:%s]. Expecting [expectedmacaddr:%s]	Skipping db_sync for a switch	
133534	Debug	Skipping db_sync for [ipaddr:%s] [macaddr:%s]. Controller not present in cpsec_lms_list	Skipping db_sync for a switch	
134113	Debug	off-loader: GSM is initialized.	This is internal debugging message.	
134114	Debug	OFFLDR GSM: replay of GSM objects for [num:%d] channels.	This is internal debugging message.	

134116	Debug	OFFLDR GSM: Start receiving Replaying events.	This is internal debugging message.	
134119	Debug	[func:%s](): GSM pmk_cache channel: station=[mac:%s] bssid=[bss:%s] event-type=[type:%s].	This indicating error condition while receiving GSM events.	
134133	Debug	[func:%s](): GSM bss channel: bssid=[bss:%s] event-type=[type:%s].	This indicating error condition while receiving GSM events.	
134134	Debug	[func:%s](): Station=[mac:%m] BSS=[bss:%m] input PMKID [iP1:%x] [iP2:%x] [iP3:%x] [iP4:%x] cached PMKID [cP1:%x] [cP2:%x] [cP3:%x] [cP4:%x] result [result:%d]	This provides visibiity into the PMKID check	
135001	Debug	[func:%s]([line: %d]) [msg:%s]	Generic debug log	
135003	Debug	[func:%s]([line: %d]): station= [mac:%s] [event: %s]	Event log on parent process	
135004	Debug	[func:%s](thread-id: [thread: %d]): station= [mac:%s] Initiating retransmission.	Event log on parent process	
135005	Debug	[func:%s](thread-id: [thread: %d]): station= [mac:%s] Processing offloader message.	Event log on parent process	
135006	Debug	[func:%s](thread-id: [thread:%d]): station= [mac:%s] Sending [msg:%s]	Event log on parent process	
135008	Debug	[func:%s]([line: %d])(thread-id: [thread: %d]): station= [mac:%s] Current open greater than open threshold. [msg:%s]	Event log on parent process	
135009	Debug	[func:%s]([line: %d])(thread-id: [thread: %d]): station= [mac:%s] Received SAE message: [recv:%s]	Event log on parent process	
135010	Debug	[func:%s]([line: %d])(thread-id: [thread: %d]): [msg:%s] station= [mac:%s]	Event log on parent process	
135011	Debug	[func:%s]([line: %d])(thread-id: [thread: %d]): [msg:%s] current open transactions. curr_open = [curr_open:%d]	Event log on parent process	
135013	Debug	[func:%s]([line: %d])(thread-id: [thread: %d]): Sending PMK to auth on [dest:%s]	Event log on parent process	
135015	Debug	[func:%s]([line: %d])(thread-id: [thread: %d]): Deleting station= [mac:%s] [msg:%s]	Event log on parent process	
135017	Debug	[func:%s]([line: %d])[mac:%s]: [msg:%s] [var:%s]	Event log on parent process	
135902	Debug	[func:%s]([line: %d]), station= [mac:%s] [msg:%s]		
135903	Debug	[func:%s], station= [mac:%s] Retransmitting [msg:%s]		
135904	Debug	[func:%s], station= [mac:%s]		
135905	Debug	[func:%s], station= [mac:%s] Received [message:%s] in authentication frame, peer in state [state:%s]		
135907	Debug	[func:%s], station= [mac:%s] Sending message [msg:%s] with seq num [seq:%d] to offloader		
135909	Debug	[func:%s], station= [mac:%s] Received response for [msg:%s]. Seq num [seq:%d]. Peer has [peerSeq:%d]		
135910	Debug	[func:%s], station= [mac:%s] Received duplicate message for station. Discarding		
135911	Debug	[func:%s], station= [mac:%s] Checking for token. Error: [msg:%s]		
136005	Debug	[func:%s](): Successfully insert attribute:'[attname:%s]' into [tblname:%s] for station:'[st:%s]' user:'[uname:%s]' survMethod:[smethod:%x].	This is an internal debugging message.	
136007	Debug	[func:%s](): Successfully delete from [tblname:%s] for station:'[st:%s]' user:'[uname:%s]' survMethod:[smethod:%x].	This is an internal debugging message.	
136008	Debug	[func:%s](): Max Number of users in RAD-DB:[max:%lu].	This is an internal debugging message.	
136032	Debug	[func:%s](): Successfully purged [num:%llu] [tblname:%s] entries older than [hr:%d] hours.	This is an internal debugging message.	
136034	Debug	UPD-RadDB([req:%lu]@[worker:%s]): Updating RAD-DB for station:'[st:%s]' user:'[user:%s]' survMethod:[smethod:%x].	This is an internal debugging message.	
136035	Debug	UPD-RadDB([req:%lu]@[worker:%s]): Successfully Updated RAD-DB for station:'[st:%s]' user:'[user:%s]' survMethod:[smethod:%x].	This is an internal debugging message.	

136037	Debug	DEL-RadDB([req:%lu]@[worker:%s]): Deleting RAD-DB for station:'[st:%s]' user:'[user:%s]' survMethod:[smethod:%x].	This is an internal debugging message.	
136038	Debug	DEL-RadDB([req:%lu]@[worker:%s]): Successfully Deleted station:'[st:%s]' user:'[user:%s]' survMethod:[smethod:%x] from RAD-DB.	This is an internal debugging message.	
136041	Debug	RESTART-RADIUSD([req:%lu]@[worker:%s]): Restarting radiusd.	This is an internal debugging message.	
136043	Debug	[func:%s](): Successfully clear [tblname:%s] for station:'[st:%s]' user:'[uname:%s]'.	This is an internal debugging message.	
137031	Debug	[[file:%s]:[line:%d]] [message:%s]	Radius module's debug message	
142003	Debug	[message:%s]	L2TP generic debug.	
199800	Debug	[function:%s], [file:%s]:[line:%d]: [error:%s]	This is an internal security debugging log.	
199801	Debug	[msg: %s]	This is an internal security debugging log.	
199803	Debug	[function:%s], [file:%s]:[line:%d]: [error:%s]	This is an internal cluster debugging log.	
100100	Emergency	FIPS Emergency: [msg:%s]	This is a FIPS emergency log in security module.	
142010	Emergency	[message:%s]	L2TP generic emergencies.	
100103	Error	FIPS Error: [msg:%s]	This is a FIPS error log in security module.	
103001	Error	Cannot create IPSec map on [switch:%s]	Internal error if IPSEC map for Conductor-Local or Conductor-Conductor is not created	
103002	Error	Cannot create ISAKMP PSK on [switch:%s]	Internal error if IKE PSK for Conductor-Local or Conductor-Conductor is not created	
103010	Error	VPN IKE Phase 1 failed: multiple SA or proposal payloads. Illegal client request from [IP:%s]	System received malformed SA transform negotiation message from client. IKE requires that only one SA with only one proposal exists. Message consisted of multiple SA or proposal payloads.	
103014	Error	IKE Phase 1 failed, received a malformed message from [IP:%s]	Failure in negotiation of IKE SA due to receipt of malformed IKE packet. Please look at the client/peer implementation	
103016	Error	Received incorrect IKE Phase-1 ID	Failure in negotiation of IKE SA due to incorrect IKE Phase 1 ID	
103020	Error	IKE Quick Mode failed: could not match with a map in Conductor-Local VPN	Failure to negotiate IPSEC SA due to internal error of missing IPSEC map for Conductor-Local or Conductor-Conductor tunnel	
103023	Error	IKE Quick Mode failed, payload malformed in first IKE quick mode packet from client [IP:%s]	Failure in IPSEC SA negotiation due to malformed IKE Quick mode packet. Please check the implementation of peer/client	
103025	Error	IKE Quick Mode failed, payload malformed from [IP:%s]	Failure in IPSEC SA negotiation due to IKE Quick mode packet that is missing ID payload. Please check the client/peer implementation	
103027	Error	IKE Quick Mode failed can't handle ID type [id:%d]	Failure in IPSEC SA negotiation due to IKE Quick mode packet that has invalid ID type. Please check the client/peer implementation	
103031	Error	IKE Quick Mode failed from peer [IP:%s]	General Failure in IPSEC SA negotiation. Please check the client/peer implementation and logs	
103032	Error	IKE Quick Mode failed in adding message payload for client [IP:%s]	Internal error due to failure in adding Payload during IPSEC SA negotiation.	
103036	Error	Mismatch from L2TP: [IP:%s], IPSec-SPI [spi:0x%x]	Internal error where IPSEC SA is not found for corresponding L2TP tunnel	
103037	Error	Unable to update datapath with L2TP/IPSEC info. [IP:%s], IPSec-SPI [spi:0x%x], L2TP tunnel [tid:%d]	Internal error in IKE messaging to Datapath during IPSEC tunnel creation	
103039	Error	Error Sending L2TP DOWN for [IP:%s]	Internal error in IKE messaging to L2TP during IPSEC tunnel deletion	
103041	Error	NOT SUPPORTED IN THIS VERSION...L2TP down admin request for [IP:%s] (External [extIP:%s])	Internal error in IKE messaging to AUTHMGR for XAUTH IP down event	
103043	Error	IPSEC tunnel mode with bad inner [IP:%s], cannot add IPSEC SA to datapath	Internal error when IPSEC SA is created without an Inner-IP assigned to the Client	
103045	Error	IKE: Failed to get address from L2TP	Failure to get an Inner IP for VPN client	Check the IP pool configuration using command "show vpdn l2tp configuration"
103046	Error	IKE XAuth client UP failed [IP:%s] (External [extIP:%s])	Internal error in IKE messaging to AUTHMGR for XAUTH IP up event	
103048	Error	IKE XAuth failed for [user:%s]	VPN authentication failed for XAUTH user	
103052	Error	Failed to enable IPSec SA	Internal error in creating IPSEC SA	
103055	Error	Failed to [action:%s] [type:%s] IPSEC routes	Internal error in adding/deleting Routes for Conductor Local tunnel	

103058	Error	Unable to inform datapath to delete L2TP/IPSEC for [IP:%s] L2TP [tunid:%d]	L2TP tunnel was deleted but could not find corresponding IPSEC SA for VPN client	
103061	Error	[prefix:%s] [message:%s]	General internal errors in IKE module	
103067	Error	IKE XAuth failed as the AP [user:%s] is not in allowlist	Xauth failure as the AP is not in allowlist	
103068	Error	IKE XAuth failed as the AP [user:%s] is not in approved-state in allowlist	Xauth failure as the AP is not in approved-state in allowlist	
103073	Error	Error Sending License Check for ACR	Internal error in IKE ACR License check message to AUTH during IPSEC tunnel establishment	
103088	Error	IKEv2 Cert Verification failed for peer [IP:%s]:[Port:%d]	IKEv2 Cert Verification failed for the specified peer	
103094	Error	failed to generate key pair--Called from IPSEC for peer [IP:%s]	Unable to generate asymmetric key pair for specified peer	
103095	Error	failed to generate HMAC--Called from IPSEC for peer [IP:%s]	Unable to generate HMAC correctly for specified peer	
103096	Error	failed to generate hash--Called from IPSEC for peer [IP:%s]	Unable to generate hash correctly for specified peer	
103097	Error	RSA Sign operation failed--Called from IPSEC for peer [IP:%s]	Unable to do RSA Sign correctly for specified peer	
103098	Error	RSA Verify operation failed--Called from IPSEC for peer [IP:%s]	Unable to do RSA Verify correctly for specified peer	
103099	Error	ECDSA Sign operation failed--Called from IPSEC for peer [IP:%s]	Unable to do ECDSA Sign correctly for specified peer	
103100	Error	ECDSA Verify operation failed--Called from IPSEC for peer [IP:%s]	Unable to do ECDSA Verify correctly for specified peer	
105002	Error	PPP/VPN Authentication failed for RSA/token user. Must have a loopback IP defined for securID new/next PIN mode to work [user:%s]	PPP/VPN Authentication failed for RSA/token user. Must have a loopback IP defined for securID new/next PIN mode to work.	
105003	Error	PPP/VPN Authentication failed [user:%s] [IP:%s] [type:%s]. Please check authentication server radius/ldap/tacacs logs.	PPP/VPN Authentication failed. Please check authentication server radius/ldap/tacacs logs.	
105005	Error	PPP/VPN caching of RSA/token user failed [user:%s] [IP:%s]. Connectivity will be fine but user will not be able roam without retyping in token. Please check connectivity to master switch	PPP/VPN caching of RSA/token user failed [user:%s] [IP:%s]. Connectivity will be fine but user will not be able roam without retyping in token. Please check connectivity to master switch	
109020	Error	LDAP: Error retrieving the Distinguished Name of entry	System encountered an error retrieving Distinguished Name of the entry returned by the search result. This could happen if user could not be found. The Key Attribute or the Base DN configured for the server may be incorrect.	
109022	Error	LDAP Server [name:%s]: Error in Authenticating User [uname:%s]: key attribute not configured	System could not authenticate user because Key attribute was not configured for the server. Check the LDAP server configuration.	
118001	Error	Certificate [certname:%s] is not yet valid.Please check the controller time and the cert validity period.	The certificate is not yet valid.Please check the controller time and the cert validity period.	
118002	Error	CRL [crl:%s] is expired.	The CRL has expired.	
118004	Error	[string:%s]	This shows an error message in Cert Mgr.	
118006	Error	OCSP URL or Responder cert not configured for CA [string:%s]	OCSP URL or Responder Certificate is not configured for given CA.	
118007	Error	OCSP Client's cleanup timer failed to initialize.	OCSP Client's cleanup timer failed to initialize.	
118008	Error	Periodic certificate expiry check timer failed to initialize.	Periodic certificate expiry check timer failed to initialize.	
118015	Error	[string:%s]	This shows an error message in Cert Mgr for EST.	
121000	Error	Failed to calculate the HMAC-MD5 digest	Controller failed to calculate the HMAC-MD5 digest for RADIUS packet due to an internal error	Please contact Aruba tech-support if this problem persists.
121001	Error	Error [errno:%d],[errstr:%s] receiving packet [packet_len:%d], fd=[fd:%d]	An socket error occurred while receiving RADIUS server response	Please contact Aruba tech-support if this problem persists.
121002	Error	An error occurred while receiving RADIUS server response	An error occurred while receiving RADIUS server response	Please contact Aruba tech-support if this problem persists.
121003	Error	Discarding unknown response from server	RADIUS Server has returned a response that does not match the request or the packet could be corrupt	Validate RADIUS server configuration. Please contact Aruba tech-support if this problem persists.
121005	Error	An error occurred while receiving RADIUS server response on port 3799 (RFC 3576)	An error occurred while receiving RADIUS server response on port 3799 (RFC 3576)	Please contact Aruba tech-support if this problem persists.
121008	Error	RADIUS: Error [errno:%d],[errstr:%s] creating client socket	Internal error occurred while initiating connection with the RADIUS server	Please contact Aruba tech-support if this problem persists.

121009	Error	RADIUS: Error ([errno:%d]:[errstr:%s]) in bind for server [server:%s]([ipstr:%s])	Internal error occurred while connecting with the RADIUS server	Please contact Aruba tech-support if this problem persists.
121010	Error	Error [errno:%d],[errstr:%s] sending [data_len:%d] bytes on radius socket [sockfd:%d]	Internal error occurred while sending data to the RADIUS server	Please contact Aruba tech-support if this problem persists.
121011	Error	Received RADIUS server response with invalid length [len:%d]	The expected length of a RADIUS server response packet is between 20 and 4096 bytes.	Please check the length of response packet from the RADIUS server.
121012	Error	Not enough buffer space to verify RADIUS server response packet with length [totallen:%d]	The internal buffer is not big enough for the RADIUS response packet and RADIUS secret	Please check the length of the RADIUS response packet from the RADIUS server and the length of RADIUS secret.
121013	Error	Received non-matching ID in RADIUS server response [id:%d], expecting [seq_nbr:%d]	Received a response from the RADIUS server, but the sequence number doesn't match the request	Please check the RADIUS server is configured properly.
121014	Error	Received invalid reply digest from RADIUS server	The reply digest received from the RADIUS server doesn't match the calculated digest	Please check the RADIUS server is configured properly and verify shared secret configuration on the controller matches that on the RADIUS server
121016	Error	RADIUS server [server:%s],[fqdn:%s][ipaddr:%s] is out of sequence numbers	The PENDING request buffer to RADIUS server is already full (256). Response from RADIUS server seems to be slower than the rate at which the users are coming in	Please check the RADIUS server is configured properly and the connectivity between Aruba controller and RADIUS server is good.
121018	Error	Unknown RADIUS attribute ID [attrid:%d] in [func:%s]	The RADIUS attribute is not known	Please use "show aaa radius-attributes" command to check if the attribute ID is supported.
121019	Error	Received attribute with invalid length [attrlen:%d] in [func:%s]	Received RADIUS attribute with invalid length, while extracting the attribute-value pairs	Please check the RADIUS server is configured properly and the connectivity between Aruba controller and RADIUS server is good.
121021	Error	RADIUS attribute [name:%s] has unknown type [type:%d] in [func:%s]	Received unknown RADIUS attribute type, while extracting the attribute-value pairs	Please check the supported RADIUS attribute type.
121022	Error	Unknown RADIUS attribute name [name:%s] in [func:%s]	Received unknown RADIUS attribute name, while extracting the attribute-value pairs	Please use "show aaa radius-attributes" command to check if the attribute name is supported.
121023	Error	Unknown RADIUS attribute [attr_value:%s] in [func:%s]	Controller received an unknown RADIUS attribute while extracting the attribute-value pairs from Radius server response	Please use "show aaa radius-attributes" command to check if the attribute value is supported.
121024	Error	Internal Error: [action:%s] RADIUS Message-Authenticator attribute is not implemented for code:[code:%u]	Controller does not support RADIUS Message-Authenticator for certain RADIUS message	
121025	Error	Value pair is NULL or empty attribute [id:%d] in [func:%s]	Internal error occurred while converting the attribute-value pairs received in RADIUS response to strings	Please contact Aruba tech-support if this problem persists.
121026	Error	RADIUS: Error in getting available Sequence Number for Server:[server:%s] ([reason:%s])	Error occurred while getting available Sequence Number with the RADIUS server	Please contact Aruba tech-support if this problem persists.
121029	Error	RADIUS: Error [errno:%d], [errstr:%s] creating rfc3576 socket	Internal error occurred while initiating connection with RADIUS server	Please contact Aruba tech-support if this problem persists.
121030	Error	RADIUS: Error [errno:%d], [errstr:%s] in rfc3576 bind	Error occurred while connecting to RADIUS server	Please contact Aruba tech-support if this problem persists.
121033	Error	rc_pack_list: Attribute list exceeds 32768 bytes, dropping request	rc_pack_list: Attribute list exceeds 32768 bytes, dropping request	
121036	Error	RADIUS: Error [errno:%d],[errstr:%s] setting client socket options	Internal error occurred while setting connection options with the RADIUS server	Please contact Aruba tech-support if this problem persists.
121047	Error	Failed to add user Port ID in the Radius Accounting Pkt [pkt:%s].	This shows an internal debug message	
121048	Error	Unknown result type [resultType:%d].	This shows an internal debug message	
121049	Error	Failed to add user Port ID in the Radius Accounting Start Pkt [portStr:%s].	This shows an internal debug message	

121051	Error	DA Server: Error [errno:%d], [errstr:%s] while setting socket option IP_PKTINFO for port [port:%d]	Error occurred while setting socket option IP_PKTINFO for dynamic authorization server udp port	Please contact Aruba tech-support if this problem persists.
121052	Error	DA Server: Error [errno:%d], [errstr:%s] while setting socket option IPV6_V6ONLY for port [port:%d]	Error occurred while setting socket option IPV6_V6ONLY for dynamic authorization server udp port	Please contact Aruba tech-support if this problem persists.
121053	Error	DA server: Error [errno:%d], [errstr:%s] while setting socket option SO_REUSEADDR for port [port:%d]	Error occurred while setting socket option SO_REUSEADDR for dynamic authorization server udp port	Please contact Aruba tech-support if this problem persists.
122000	Error	TACACS servers is not configured	TACACS server is not configured	Please use "aaa authentication-server tacacs" command to configure TACACS server
122004	Error	Received unexpected packet type from TACACS server. Received type [r_type:%d], expected type [e_type:%d]	The TACACS packet header type is not expected. The packet could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122005	Error	Received unexpected packet sequence number. Received [seq_no:%d], expect 2	The TACACS packet header sequence number is not expected. The reply could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122006	Error	Received unexpected packet session ID. Received [r_session_id:%d], expect [s_session_id:%d]	The TACACS packet header session ID is not expected. The reply could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122007	Error	Failed in binding socket for TACACS+ server:[servaddr:%s] on source address:[hostaddr:%s]. Error:[errstr:%s]	Internal Error occurred while binding the socket	
122008	Error	Short write on TACACS CMD-Authorization body. User:[user:%s], CMD:'[cmd:%s]' CMD-ARG:'[cmdarg:%s]'. Wrote [w:%d] bytes of packet length [pkt_len:%d]	Error occurred while sending body portion of the request to TACACS server, Link to TACACS server or TACACS server could be down	Please check network connection to the TACACS server.
122009	Error	Short write on TACACS PAP body. User [user:%s], Password [pass:%s], TTY [tty:%s]. Wrote [w:%d] bytes of packet length [pkt_len:%d]	Error occurred while sending body portion of the request to TACACS server, Link to TACACS server or TACACS server could be down	Please check network connection to the TACACS server.
122010	Error	Error reading TACACS PAP authentication packet header. Received [r:%d] bytes of header length [TAC_PLUS_HDR_SIZE:%d]	Authentication Failed. Error occurred while receiving header portion of the reply from TACACS server, The reply could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122011	Error	Error reading TACACS PAP authentication packet body. Received [recvd:%d] bytes, expect [len_from_header:%d] bytes	Authentication Failed. Error occurred while receiving body portion of the reply from TACACS server. The reply could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122012	Error	The message body length mismatched.	Authentication Failed, Error occurred in the reply from TACACS server, The reply body length does not match with the length defined in the header	Please check your TACACS server configuration and network connection to the TACACS server.
122014	Error	Error sending TACACS accounting packet header. Wrote [w:%d] bytes of header length [TAC_PLUS_HDR_SIZE:%d]	Error occurred while sending header portion of the TACACS accounting request to TACACS server. Link to TACACS server or TACACS server could be down	Please check your TACACS server configuration and network connection to the TACACS server.
122015	Error	acct body send failed: wrote [w:%d] of [pkt_len:%d]	Error occurred while sending body portion of the TACACS accounting request to TACACS server, Link to TACACS server or TACACS server could be down	
122016	Error	received short PAP acct header, [recvd:%d] of [TAC_PLUS_HDR_SIZE:%d]	Accounting Failed, Error occurred while receiving header portion of the accounting reply from TACACS server, The reply could be corrupt	
122017	Error	incomplete message body, [recvd:%d] bytes, expected [len_from_header:%d]	Accounting Failed, Error occurred while receiving body portion of the reply from TACACS server, The reply could be corrupt	
122018	Error	invalid reply content, incorrect key?	Accounting Failed, Error occurred in the reply from TACACS server, The reply body length does not match with the length defined in the header	
122019	Error	accounting failed, server reply was [ret:%d], [msg:%s]	TACACS accounting failed	
122021	Error	Short write on TACACS authorization request body. User [user:%s]. Wrote [w:%d] bytes of packet length [pkt_len:%d]	Error occurred while sending body portion of the request to TACACS server, Link to TACACS server or TACACS server could be down	Please check network connection to the TACACS server.

122022	Error	Error reading TACACS authorization response packet header. Received [r:%d] bytes of header length [TAC_PLUS_HDR_SIZE:%d]	Authorization Failed. Error occurred while receiving header portion of the response from TACACS server, The response could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122023	Error	Error reading TACACS authorization packet body. Received [recvd:%d] bytes, expect [len_from_header:%d] bytes	Authorization Failed. Error occurred while receiving body portion of the response from TACACS server. The response could be corrupt	Please check your TACACS server configuration and network connection to the TACACS server.
122024	Error	The message body length mismatched.	Authorization Failed, Error occurred in the response from TACACS server, The response body length does not match with the length defined in the header	Please check your TACACS server configuration and network connection to the TACACS server.
124027	Error	Maximum number ([num:%d]) of [type:%s] entries is reached while adding '[name:%s]'.	This indicates an error that max number of netservice or netdestination is reached.	
124052	Error	Invalid certificate service type [type:%d].	A message was received that specified an incorrect service to use for the certificate.	Call Aruba Technical Support.
124053	Error	Invalid certificate message type in response message [type:%d].	A response message was expected, but a different message type was received.	Call Aruba Technical Support.
124054	Error	Certificate [cert:%s] was not found.	The requested certificate name was not found.	Upload the named certificate to the controller, or check the spelling of the certificate name.
124055	Error	The service type for the certificate in the request [req:%d] and response [rsp:%d] does not match.	Certificates can be used for various services. The requested certificate cannot be used for the desired service.	Call Aruba Technical Support.
124059	Error	Deleting a user IP=[ip:%s] with flags=[flags:%x] from the datapath that does not exist in auth.	A user was deleted even though the datapath and auth are inconsistent.	
124060	Error	Internal Error: Unknown authentication [type:%s]		
124062	Error	No server group for MAC=[mac:%s] IP=[ip:%s] in authentication profile [p1:%s], method=[m:%s] AAA profile=[p2:%s] found.	The server group used to authenticate the user could not be found.	Call Aruba Technical Support.
124063	Error	Message to [ip:%s]:[port:%d]([app_name:%s]) with MsgCode [msg_code:%d], Msglen [len:%d], and Msgtype [msg_type:%d] failed with Errno [errno:%d], Errstr [errstr:%s]		
124064	Error	Authentication Server type([type:%s]) is initialized.	Certain Authentication-Server type is NOT initialized.	
124069	Error	Invalid Server group '[sg:%s]' which contains an unknown server '[sname:%s]'.	The server included in server group is not configured.	
124085	Error	Failed to create MAC user entry and user entry due to too many user entries [users:%d].	The MAC user entry could not be created as the maximum number of user entries has been reached.	
124149	Error	Failed to create [string:%s] IP user entry and user entry due to too many user entries [users:%d].	The IP user entry could not be created as the maximum number of user entries has been reached.	
124189	Error	Role for user [mac:%s] set to 'logon' since configured role '[role:%s]' not found.	This shows an internal debug message	
124190	Error	Role for user [user:%s] set to 'logon' since AAA profile not found.	This shows an internal debug message	
124191	Error	Role for user [mac:%s] set to 'logon' since existing role '[role:%s]' not found.	This shows an internal debug message	
124192	Error	Role for user [mac:%s] set to 'logon' since configured role '[role:%s]' not found.	This shows an internal debug message	
124194	Error	{[mac:%s]-[ipaddr:%s]-[name:%s]} bogus acl=[acl:%d] (role=[role:%s]), bwm=[bwm:%d], tunl=[tunl:%x], PA=[pa:%d], HA=[ha:%d], RO=[ro:%d], VPN=[vpn:%d].	This shows an internal debug message	
124195	Error	Error in mobility update message (params [params:%d], status [status:%d]).	This shows an internal debug message	
124196	Error	Unknown role '[role:%s]' for mobility update for user [user:%s].	This shows an internal debug message	
124197	Error	{[mac:%s]-[ipaddr:%s]} Unknown role for outer=[outer:%s], count=[count:%d], auth type=[authtype:%d], subtype=[subtype:%d], server=[server:%s].	This shows an internal debug message	

124198	Error	{[mac:%s]-[question:%s]} Missing server in attribute list, auth=[authtype:%s], utype=[utype:%s].	This shows an internal debug message	
124199	Error	Internal Error : Invalid args, skipping role derivation based on user attributes.	This shows an internal debug message	
124200	Error	[func:%s](): Invalid mic-length:[ml:%ld] for ap-opmode:[aom:%d].	This shows an internal error message	
124251	Error	error creating ENET entry in Mux table	This shows an internal error message	
124252	Error	L2 Miss on Switch MAC, dropping the packet	This shows an internal error message	
124253	Error	register failed for id = [id:%d], name = [name:%s]	This shows an internal error message	
124254	Error	missing default wired profile	This shows an internal error message	
124255	Error	stm_ap_provision_state_rsp: PAPI_Send failed. MAC: [username:%s]	This shows an internal error message	
124256	Error	Setting the vlan/port,Unknown SAP ([ip:%s])	This shows an internal error message	
124257	Error	Failed to get aaa profile [wired_or_wl:%s] station [mac:%s]:[bssid:%s][vlan:[vlan:%u] ingress:[ingress:%x]]	This shows an internal error message	
124258	Error	Failed to add [wire_or_wl:%s] station [mac:%s] bss/group [bssid:%s]	This shows an internal error message	
124259	Error	Dropping Station up, no aaa profile found for user [mac:%s], bssid [bssid:%s]"	This shows an internal error message	
124260	Error	Station setup failed for [wired_or_wl:%s] station [mac:%s]:[bssid:%s]	This shows an internal error message	
124261	Error	Can't create netdestination [dst_name:%s]. Fails to add policy to acl [acl_name:%s]	This shows an internal error message	
124262	Error	Internal error, invalid user info	This shows an internal error message	
124263	Error	Datapath-User[act_str:%s]([type_str:%s]) failed: mac=[mac:%s] IP=[ip_uV4:%s], action=[action:%x]	This shows an internal error message	
124264	Error	[_function:%s] Send ACR license value to IKE failed	This shows an internal error message	
124265	Error	Msg from AUTH to Sibyte in NON_BLOCKING_W_ACK FAILED. Opcode = [opcode:%d], Len = [len:%d]	This shows an internal error message	
124266	Error	Failed to send [msg_type_opcode:%s] msg to SOS	This shows an internal error message	
124267	Error	Failed to send [msg_type_opcode:%s] msg to SOS	This shows an internal error message	
124268	Error	Internal Error : while retriving AAA profile for MAC: [macaddr:%s].	This shows an internal debug message	
124275	Error	IP address not found in AUTH @ Monitor.	This shows an internal debug message	
124276	Error	AUTH User [user:%s] missing in SOS.	This shows an internal debug message	
124277	Error	Failed to send interim statistics.	This shows an internal debug message	
124278	Error	Internal error while creating RAP user : [user:%s], mac : [mac:%s].	This shows an internal debug message	
124279	Error	[function:%s] [line:%d] Internal error: server group is null internal: [internal:%d] vpn-auth-underway: [vpnauthunderway:%d] IP: [IP:%s] mac: [mac:%s] vpn_authserver: [vpn_authserver:%s] vpn_flags: [vpn_flags:%c] vpn-auth-type: [vpnauthtype:%c] auth-type: [authtype:%c].	This shows an internal error message	
124280	Error	failed to get aaa-profile for client [user:%s]-[mac:%s]-[name:%s].	This shows an internal debug message	
124281	Error	snapshot: unknown role [role:%s], IP=[ipaddr:%s].	This shows an internal debug message	
124282	Error	snapshot station: unknown role [role:%s].	This shows an internal debug message	
124283	Error	Tunnel Update ACL failed.	This shows an internal debug message	
124284	Error	Not creating user [user:%s] due to license failure.	This shows an internal debug message	
124285	Error	l2role is null for mac:[mac:%s] IP:[ipaddr:%s].	This shows an internal debug message	
124286	Error	Denylist failure count hit an internal maximum for the server group (auth_type [authtype:%d]).	This shows an internal debug message	
124287	Error	Error allocating memory for denylist hash entry for station [mac:%s] authtype [authtype:%d].	This shows an internal debug message	
124288	Error	AP wired users failure count hit an internal maximum for the server (auth : '[authtype:%s]').	This shows an internal debug message	
124289	Error	[func:%s]: PAPI_Send failed.	This shows an internal debug message	
124290	Error	GUT :: Failed to register the session.	This shows an internal debug message	

124291	Error	GUT :: Invalid message length.	This shows an internal debug message	
124292	Error	GUT :: Invalid message type.	This shows an internal debug message	
124293	Error	GUT :: Error allocating memory ([bytes:%zu]) bytes.	This shows an internal debug message	
124294	Error	GUT :: Failed to send GUT reply to conductor switch.	This shows an internal debug message	
124295	Error	GUT :: Invalid message length.	This shows an internal debug message	
124296	Error	GUT :: Invalid message type.	This shows an internal debug message	
124297	Error	GUT :: no matched session.	This shows an internal debug message	
124298	Error	GUT :: switch info not available.	This shows an internal debug message	
124301	Error	user is NULL. Returning.	This shows an internal debug message	
124302	Error	GUT :: large papi in progress. Drop the packet.	This shows an internal debug message	
124359	Error	L2 Miss on Zero MAC, dropping the packet	This shows an internal error message	
124360	Error	Dot1x context is still valid, freeing it now	This shows an internal error message	
124372	Error	Policy not updated, http flag is not set	This shows an internal debug message.	
124373	Error	std_acl is NULL.	This shows an internal debug message.	
124374	Error	Reached maximum policy count 500 in ACL [name:%s].	This shows an internal debug message.	
124375	Error	Internal Error Occurred, while acquiring reference. acl:[name:%s], qos-profile:[profile:%s], ErrCode :[err:%d], ErrStr:[string:%s].	This shows an internal debug message.	
124376	Error	Internal Error Occurred, while acquiring reference. acl:[name:%s], pol-profile:[profile:%s], ErrCode :[err:%d], ErrStr:[string:%s].	This shows an internal debug message.	
124377	Error	Internal Error Occurred, while releasing reference. ACL:[name:%s], qos-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124378	Error	Internal Error Occurred, while releasing reference. ACL:[acl:%s], pol-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[string:%s].	This shows an internal debug message.	
124379	Error	VIA: Internal Error Occurred while releasing reference. Role:[role:%s], VIA_Profile:[via:%s],Errcode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124380	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], qos-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124381	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], qos-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124382	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], Policer-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124383	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], policer-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124384	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], voip-Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124385	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], CP_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124386	Error	VIA: Internal Error Occurred, while acquiring reference. Role:[role:%s], VIA_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124387	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], NTLM_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124388	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], NTLM_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124389	Error	Unknown stateful-ntlm profile [profile:%s].	This shows an internal debug message.	
124390	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], KERBEROS_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124391	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], KERBEROS_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124392	Error	Unknown stateful-kerberos profile [profile:%s].	This shows an internal debug message.	
124393	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], WISPR_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	

124394	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], WISPR_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124395	Error	Unknown wispr profile [profile:%s].	This shows an internal debug message.	
124397	Error	Internal Error Occurred while releasing reference. Role:[role:%s], CP_Profile:[profile:%s], ErrCode :[err:%d],ErrStr:[str:%s].	This shows an internal debug message.	
124398	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], VOIP_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal debug message.	
124399	Error	Memory allocation failed for dhcp opt role cache.	This shows an internal error message.	
124400	Error	Memory allocation failed for dhcp opt vlan cache.	This shows an internal error message.	
124401	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], Acl:[acl:%s], ap_group:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal error message.	
124402	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], Acl:[acl:%s], ap_group:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal error message.	
124403	Error	Internal Error Occurred, while acquiring reference. Role:[role:%s], TC_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal error message.	
124404	Error	Internal Error Occurred, while releasing reference. Role:[role:%s], TC_Profile:[profile:%s], ErrCode :[err:%d], ErrStr:[str:%s].	This shows an internal error message.	
124411	Error	[func:%s](): Error in creating Bridge-IP-List for Station:[bmac:%s]	Internal System Error	
124421	Error	Found stale user entry in SNMP tree: [mac:%s] [ipaddr:%s].	This shows an internal debug message	
124422	Error	Failed to get SOS user entry for SNMP [mac:%s] [ipstr:%s] in [func:%s].	This shows an internal debug message	
124426	Error	[func:%s]: null station pointer in user node.	This shows an internal debug message	
124427	Error	Invalid authentication protocol [proto:%d] for RADIUS.	This shows an internal debug message	
124428	Error	[func:%s]: Radius server lookup failed. Server=[servername:%s].	This shows an internal debug message	
124429	Error	[func:%s]: Server [servername:%s] type [type:%d] did not match Radius.	This shows an internal debug message	
124430	Error	IP user lookup failed for station with IP [ipaddr:%s].	This shows an internal debug message	
124431	Error	Station UP failed for station [mac:%s] [bssid:%s]	This shows an internal debug message	
124488	Error	[function:%s]:[line:%d] Memory allocation failed.	This shows an internal debug message.	
124489	Error	[errno:%d] - [errstr:%s], encounterd, while seting the permission for [script:%s].	This shows an internal debug message.	
124490	Error	Cant change VLAN of user :[user:%s].	This shows an internal debug message.	
124491	Error	Setting the user : [user:%s] from port: [port:%s] to new vlan failed, Error : [errno:%d] : [errstr:%s].	This shows an internal debug message.	
124492	Error	AP Authentication PAPI Send failed. MAC: [mac:%s].	This shows an internal debug message.	
124493	Error	AP Authentication failed. MAC: [mac:%s].	This shows an internal debug message.	
124494	Error	Auth request for unknown user (name='[name:%s]' IP=[ip:%s], method=[method:%s]).	This shows an internal debug message.	
124495	Error	Error decoding mppe-send-key (code = [code:%d]).	This shows an internal debug message.	
124496	Error	Error decoding mppe-recv-key (code = [code:%d]).	This shows an internal debug message.	
124497	Error	[function :%s] failed setup_pppeapctx.	This shows an internal debug message.	
124498	Error	[function :%s] failed eap_pkt_new.	This shows an internal debug message.	
124500	Error	Failed to Override NetDestination:[dest:%s] VLAN:[vlan:%u] Offset:[offset:%u]. Please check IP-Addresses configuration for 'interface vlan [vlan2:%u]'.	This indicates subnet IP-Addresses were not configured for the specified interface-vlan	
124502	Error	Failed to Override NetDestination:[dest:%s] VLAN:[vlan:%u]. Please check IP-Addresses configuration for 'interface vlan [vlan2:%u]'.	This indicates subnet IP-Addresses were not configured for the specified interface-vlan	
124520	Error	failed to add station [mac:%s]:[mswitch:%s].	This shows an internal debug message	
124542	Error	TACACS+ accounting failed result=[rs:%s]([ri:%d]), method=[m:%s] for user [user:%s] server [server:%s].	This shows an internal debug message	
124551	Error	Cant generate_acl, Invalid acl:[invalidacl:%d].	This shows an internal debug message	
124558	Error	Invalid acl [acl:%s] to generate ACL.	This shows an internal debug message	

124596	Error	No macuser for mac [mac:%s].	This shows an internal debug message	
124597	Error	Intra move for unknown user [mac:%s]:[ipstr:%s].	This shows an internal debug message	
124598	Error	Inter move for unknown user [mac:%s]:[ipaddr:%s].	This shows an internal debug message	
124599	Error	Failed to move [mac:%s]:[ipstr:%s].	This shows an internal debug message	
124608	Error	[func:%s](): Invalid server type [type:%d]'.	This indicates an invalid server type is received in the response message	
124618	Error	/proc/stat open failed: [reason:%s].	This shows an internal debug message	
124619	Error	Failed to add opcode SOS_MSG_OPCODE_KERBEROS.	This shows an internal debug message	
124620	Error	Failed to remove opcode SOS_MSG_OPCODE_KERBEROS.	This shows an internal debug message	
124621	Error	Kerberos: Failed to create rsm_entry.	This shows an internal debug message	
124622	Error	Kerberos: Failed to create rsm buffer.	This shows an internal debug message	
124623	Error	Kerberos: Failed to create rsm buffer.	This shows an internal debug message	
124624	Error	Received Kerberos packet that is too short: [msglen:%d].	This shows an internal debug message	
124625	Error	Unknown protocol/Sibyte Opcode [proto:%x]/[opcode:%x].	This shows an internal debug message	
124662	Error	Received Kerberos packet on TCP that is too short: [msglen:%d], tcp doff [doff:%d].	This shows an internal debug message	
124663	Error	Received Kerberos packet on UDP that is too short: [msglen:%d].	This shows an internal debug message	
124664	Error	Invalid Kerberos port src:[srcport:%d] dst:[dstport:%d].	This shows an internal debug message	
124665	Error	Kerberos: Failed to create a new user entry.	This shows an internal debug message	
124666	Error	Kerberos: Failed to create new krb ctx.	This shows an internal debug message	
124667	Error	Kerberos: Failed to create krb ctx session table.	This shows an internal debug message	
124668	Error	Kerberos: unknown protocol [proto:%d].	This shows an internal debug message	
124669	Error	krb_recv: failed to PAPI_Alloc.	This shows an internal debug message	
124670	Error	krb_recv: failed to send to DP.	This shows an internal debug message	
124671	Error	krb_recv: Dropping the packet.	This shows an internal debug message	
124672	Error	Kerberos: Failed to create krbdata.data.	This shows an internal debug message	
124673	Error	Received Kerberos AS-REQ packet that is too short: [len:%d].	This shows an internal debug message	
124674	Error	Received Kerberos AS-REP packet that is too short: [len:%d].	This shows an internal debug message	
124675	Error	Received Kerberos TGS-REQ packet that is too short: [len:%d].	This shows an internal debug message	
124676	Error	Received Kerberos TGS-REP packet that is too short: [len:%d].	This shows an internal debug message	
124677	Error	Received Kerberos ERR packet that is too short: [len:%d].	This shows an internal debug message	
124678	Error	Kerberos: Failed to decode the krb_as_req.	This shows an internal debug message	
124679	Error	Kerberos: Failed to decode the AS_REP.	This shows an internal debug message	
124680	Error	Kerberos: Failed to decode the krb_tgs_req.	This shows an internal debug message	
124681	Error	Kerberos: Failed to decode the krb_tgs_rep.	This shows an internal debug message	
124682	Error	Kerberos: Failed to decode AS_ERR.	This shows an internal debug message	
124683	Error	Kerberos: Trying to free NULL krb ctx.	This shows an internal debug message	
124686	Error	Too many AP Groups.	This shows an internal debug message	
124697	Error	Datapath-UserAction([type_str:%s]) failed, No error handling: mac=[mac:%s] IP=[ip_uV4:%s], action=[action:%x]	This shows an internal error message	
124704	Error	Datapath-UserAction([type_str:%s]) unknown: mac=[mac:%s] IP=[ip_uV4:%s], action=[action:%x]	This shows an internal error message	
124812	Error	fw_id_to_name: Invalid id [id:%d].	This shows an internal error message	
124815	Error	Failed to add role [role:%s] ACL [acl:%s] to AP group [apgroup:%s].	The controller was unable to add the role ACL to the AP group.	
124816	Error	Failed to delete role [role:%s] ACL [acl:%s] to AP group [apgroup:%s].	The controller was unable to delete the role ACL to the AP group.	
124819	Error	Invalid forward mode received for user : fw-mode: [fwmode:%d], [user:%s], mac : [mac:%s].	This shows an internal debug message	
124821	Error	RAP user-miss with disallowed MAC, potential loop detected: [user:%s], controller-mac : [controller_mac:%s].	This shows an internal debug message	
124822	Error	User device not found for user agent string: [useragentstring:%s].	Could not find the device in the pre-defined device database	
124826	Error	Snmp tree has a node with zero mac and no ip address	Encountered snmp tree node with zero mac while v6 snmpwalk and no ipv6 address	
124830	Error	Dldb Role [name: %s]: Users dequeued, role in incomplete state	This shows an internal error message	

124831	Error	Dldb Role [name: %s]: cmd idx [idx: %d] NACK recvd	This shows an internal error message	
124856	Error	Dldb Role: Invalid arguments to function [function: %s]	This shows an internal error message	
124857	Error	Dldb Role [name: %s]: Failed to start timer type [type: %s]	This shows an internal error message	
124858	Error	AP Group [g:%s] creation failed.	This shows ap group info could not be created in auth	
124860	Error	Auth GSM : IP_USER publish failed for IP [ip: %s] uuid [uuid: %s] result [res: %s]	This shows an internal error message	
124864	Error	Auth GSM : IP_USER notify failed for mac [mac:%s] ip:[ip:%s] result [res:%s]	This shows an internal error message	
124865	Error	Failed to derivce PTK for mac [mac:%s]	This shows an internal error message	
124866	Error	Failed to derivce GTK for mac [mac:%s]	This shows an internal error message	
124869	Error	Context buffer memory got corrupted while displaying route ACL in show run-config	Context buffer memory got corrupted while executing show running-config. Some Route ACL has too many ACEs.	
124874	Error	Mswitch IP has not been set. Dropping GUT request from conductor	This shows an internal error message	
124876	Error	Failed to add [wire_or_wl:%s] station [mac:%s]:[bssid:%s]	This shows an internal error message	
124877	Error	Dropping Station up, no aaa profile found for user [mac:%s], bssid [bssid:%s]"	This shows an internal error message	
124879	Error	Station setup failed for [wired_or_wl:%s] station [mac:%s]:[bssid:%s]	This shows an internal error message	
124880	Error	Cluster Channel lookup failed for Controller IP [ipaddr:%s].	This shows an internal debug message	
124881	Error	Auth GSM : IP USER publish failed for IP [ip: %s] [rep_key: %d] result [r: %s]	This shows an internal error message	
124883	Error	Auth GSM : IP USER repkey change failed for IP [ip: %s] [rep_key: %d] result [r: %s]	This shows an internal error message	
124888	Error	Per AP Station list create failed for AP-IP [ip:%s]	This shows an internal error message	
124889	Error	Removing the [mac:%s] from AP sta list for AP [ip:%s] failed	This shows an internal error message	
124891	Error	Remove the [mac:%s] from AP sta list failed	This shows an internal error message	
124892	Error	Invalid arguments to function [func:%s]: src [src:%s], dst [dst:%s], action [act:%d], nexthop [nh:%d]	This shows an internal error message	
124893	Error	[func:%s]: Failed to execute cmd [cmd:%s]	This shows an internal error message	
124900	Error	[function:%s](): Failed to get port info for user [mac:%s]	This shows an internal debug message	
124903	Error	[function:%s]: Get VSA failed	This shows an internal debug message	
124908	Error	[function:%s]: Config Error - Same inner and outer IP [str1:%s] for user with authtype [id: %d]	This shows an internal error message	
124909	Error	Failed to send response to conductor switch [conductorip:%s], for user delete request	This shows an internal debug message	
124914	Error	Failed to execute the CLI : [cmstr:%s] : received from conductor	This shows an internal debug message	
124915	Error	Failed to send aaa user delete request to local switch [localip:%s].	This shows an internal debug message	
124932	Error	Error in allocating id for netdestination [destname:%s]	This shows an internal debug message	
125000	Error	Error Converting Encrypted String	Internal error occurred while converting the encrypted string of management user	
125005	Error	Error creating file [file_name:%s]	Internal error when executing CLI command "ssh disable-dsa" to disable DSA. This issue could arise because there is no space on the file system	Delete un-needed files and try the CLI command again
125006	Error	Unable to delete SSH DSA Key	Internal error when executing CLI command "ssh disable-dsa" to disable DSA. This issue could arise because there is no space on the file system	Delete un-needed files and try the CLI command again
125007	Error	Unable to delete SSH DSA Pub Key	Internal error when executing CLI command "ssh disable-dsa" to disable DSA. This issue could arise because there is no space on the file system	Delete un-needed files and try the CLI command again
125008	Error	Failed to create DSA keys	Internal error when executing CLI command "no ssh disable-dsa" to re-enable DSA. This issue could arise because there is no space on the file system	Delete un-needed files and try the CLI command again
125009	Error	Failed to reconfigure SSH daemon	Internal error when executing CLI command "ssh disable-dsa" or "no ssh disable-dsa". System failed to refresh the configuration.	Please retry the command
125010	Error	No management user exist.	Internal error that can occur while saving configuration indicating the internal data corruption related to mgmt-users.	Re-Create all the management users or execute "process restart aaa"

125013	Error	Failed to set the status for user [user_name:%s]	Internal error that can occur while creating mgmt-user, indicating the failure of mgmt-user creation.	Re-Create the mgmt-users or execute "process restart aaa"
125020	Error	Server Authentication Failed, Checking mgmt-user config-db. State=[state:%d]	Debug message to indicate that Server authentication failed, the user is now authenticated against the mgmt-user database in the configuration	
125040	Error	Can't connect to database, Error [Error:%s]	Internal error occurred while initializing backend database connection, this results in cert user authentication failure	execute "process restart aaa"
125041	Error	Can't insert into database, Error [Error:%s]	Internal error occurred while creating mgmt-user for cert based authentication and saving the user information in the backend database	Delete mgmt-user, Re-Create the mgmt-users for certificate authentication.
125043	Error	Internal Error occurred performing file IO, Error No : [errorno:%d], Error String : [errstr:%s]	Internal error occurred while performing file IO	
125044	Error	Failed to update SSH configuration	Internal error, when executing CLI command "ssh mgm-auth public-key", indicating the configuration was not saved	Undo the ssh configuration and apply the config again
125045	Error	Failed to refresh SSH daemon	Internal error, when executing CLI command "ssh mgm-auth public-key", indicating the configuration didn't take effect	Execute "no ssh mgm-auth public-key" and apply the config again
125046	Error	Failed to refresh WebUI CA certificate bundle	Internal error occurred while creating mgmt-user for cert based authentication and unable to refresh the ca cert bundle used by controller WebUI.	Delete the mgmt-user, Re-Create the same mgmt-user for certificate authentication.
125047	Error	Failed to refresh ssh public key authorized keys file	Internal Error occurred while refreshing ssh public key authorized keys file	
125051	Error	[[file:%s]:[line:%d]] [message:%s]	Internal error occurred while creating/deleting mgmt-users for certificated based authentication, indicating out of memory on the controller	Check "show memory" to check the available memory
125052	Error	[[file:%s]:[line:%d]] Communication error occurred between [src:%s] and [dst:%s]	Internal error occurred while creating/deleting mgmt-users for certificated based authentication, indicating failure if internal messaging.	Check if process "certmgr" is running : "show process certmgr", if it is running, revert the command that was executed and redo the CLI command for certificate based mgmt-user authentication.
125053	Error	Error occurred while preparing the setup for certificate conversion	Internal error occurred when creating cert based mgmt-users for SSH CLI access.	revert the command that was executed and redo the CLI command for certificate based mgmt-user authentication.
125054	Error	Error occurred during certificate conversion to ssh keys	Internal error occurred when creating cert based mgmt-users for SSH CLI access	revert the command that was executed and redo the CLI command for certificate based mgmt-user authentication.
125055	Error	[message:%s]	Internal error occurred in aaa module, the error message would provide more details, it also couples with failure of creating or removing mgmt-user	
125062	Error	[message:%s]	Internal error occurred in aaa module, the error message would provide more details, password validation failed	
125073	Error	Error: Unprocessed CLI request received. srcport=[srcport:%d] dstport=[dstport:%d] packet_type=[packet_type:0x%x] packet_size=[packet_size:%d] payload=[p0:%x]-[p1:%x]-[p2:%x]-[p3:%x]-[p4:%x]-[p5:%x]-[p6:%x]-[p7:%x]-[p8:%x]-[p9:%x]		
125074	Error	DB prepare statement error for query [query:%s]	DB prepare statement error	
125075	Error	Failed to open CLI sessions directory, Error=[errstr:%s]([errcode:%d])	It indicated a failure while opening CLI session directory.	
126000	Error	AP([RADIO_MAC:%m]@[NAME:%s]): Rogue AP: An AP classified an access point(BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as rogue because it matched the MAC ([IDS_EV_MATCHED_MAC:%m]) with IPv4 ([IDS_EV_MATCHED_IP:%pI4]) and/or IPv6([IDS_EV_MATCHED_IPV6:%s]).	This event indicates that an unauthorized access point is connected to the wired network. The access point is declared Rogue because it was matched to a MAC address.	This alert indicates an event that may affect your wireless infrastructure.

126001	Error	AP([RADIO_MAC:%m]@[NAME:%s]): Cleared Rogue AP: An AP that previously classified an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as rogue, no longer considers it rogue or it was removed from the network.	This event indicates that a previously detected access point, classified as Rogue, is no longer present in the network.	This alert indicates an event that may affect your wireless infrastructure.
126002	Error	Rogue AP: The system classified an access point(BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as rogue. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an unauthorized access point is connected to the wired network. The access point is classified as Rogue by the system.	This alert indicates an event that may affect your wireless infrastructure.
126003	Error	Cleared Rogue AP: A previously classified rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is no longer considered rogue or it was removed from the network. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that a previously detected access point, classified as Rogue, is either no longer present in the network or it changed its state.	This alert indicates an event that may affect your wireless infrastructure.
127000	Error	AP([RADIO_MAC:%m]): Rogue AP: An AP classified an access point(BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as rogue because it matched the MAC ([IDS_EV_MATCHED_MAC:%m]) with IPv4 ([IDS_EV_MATCHED_IP:%pI4]) and/or IPv6([IDS_EV_MATCHED_IPV6:%s]).	This event indicates that an unauthorized access point is connected to the wired network. The access point is declared Rogue because it was matched to a MAC address.	This alert indicates an event that may affect your wireless infrastructure.
127001	Error	AP([RADIO_MAC:%m]): Cleared Rogue AP: An AP that previously classified an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as rogue, no longer considers it rogue or it was removed from the network.	This event indicates that a previously detected access point, classified as Rogue, is no longer present in the network.	This alert indicates an event that may affect your wireless infrastructure.
129002	Error	[msg:%s]		
132003	Error	xSec vlan not configured for [port:%s]	xSec vlan is not configured for the specified port	Configure VLAN that supports XSEC on specified port
132004	Error	Unknown AP [mac:%m] [bssid:%m] [menc:%s] [vlan:%d]	Authentication process has detected an unknown AP	Execute "show ap database" to determine if system is aware of the Access Point. Power-cycle the unknown AP.
132005	Error	AP [mac:%m] [apname:%s] is not enabled	Specified AP is not enabled	Configure AP with a valid virtual-AP or wired profile
132006	Error	Station Add failed [mac:%m] [bssid:%m] [apname:%s] [uenc:%s] [menc:%s]	Station failed to complete the security association with authentication process	Confirm that the SSID that the supplicant is associating to is configured to support 802.1X authentication and is configured correctly
132008	Error	Station delete failed, does not exists in the station table	Failed to clear the station from the AP's station table	Station does not exist in authentication process tables. Confirm by running "show station" command
132009	Error	Station's dot1x context not initialized [name:%s] [mac:%m] [bssid:%m]	Station's internal context is not completely initialized	Internal error. Clear the station by running "aaa user delete" and reconnect.
132010	Error	Multiple state attributes in RADIUS response packet. Drop the whole packet.	The RADIUS response packet is invalid because it contains multiple state attributes	
132013	Error	AP [bssid:%m] [apname:%s] Configuration not complete, No Transmit WEP Key set	AP's configuration is not complete. Check if the WEP transmit key is set	Check of the WEP transmit key is set in the ssid-profile

132015	Error	Failed to Deauthenticate the station [mac:%m] [name:%s]	Failed to deauthenticate the specified station	Internal error. Clear the station and reconnect.
132016	Error	Local Database Server not available to cache the machine auth for user [name:%s] [mac:%m]	Internal server is not available for caching the machine authentication for the specified User. Run "aaa test-server pap internal" to verify that local database server to verify connectivity to the local database server. If unavailability of local database server persists and controller is a local-controller, verify connectivity to conductor-controller. If all else fails, restart the udbserver process on the conductor-controller by executing "process restart udbserver" and restart the AUTH process on the local-controller by executing "process restart auth".	
132017	Error	Failed to update Machine Auth status to local DB for Station [mac:%m] [name:%s]	Failed to update the Machine authentication Status for the specified User because udbserver process is not responding. Run "aaa test-server pap internal" to verify that local database server to verify connectivity to the local database server. If unavailability of local database server persists and controller is a local-controller, verify connectivity to conductor-controller. If all else fails, restart the udbserver process on the conductor-controller by executing "process restart udbserver" and restart the AUTH process on the local-controller by executing "process restart auth".	
132018	Error	Station [mac:%m] [bssid:%m] was deleted before the response from the local database server	Station was deleted before receiving response from the Internal Server due to high latency between local-controller's AUTH process and conductor-controller's UDBSERVER process. Diagnose external IP-latency issues between conductor-controller and local-controller and have the client re-attempt their authentication-request.	
132023	Error	802.1x authentication is disabled in profile [prof:%s] Station [mac:%m] [bssid:%m]	802.1x authentication is disabled for the specified profile. Configure the specified aaa-profile to enable 802.1x authentication.	
132024	Error	Station [mac:%m] pre-authenticating with Unknown AP [bssid:%m] vlan [vl:%d]	Station is trying to pre-authenticate with an AP that is not registered. This log-message is generated when we detect a race-condition between STM, SOS and AUTH. AUTH is receiving EAP packets from SOS before it received the New-AP message from STM. Execute "show ap database" to determine if STM is aware of the AP. If not, try rebooting the AP by executing "apboot" or powercycling the AP. If symptoms persist, then AUTH is either not receiving or not processing New-AP messages from STM. If all else fails, restart the AUTH process by executing "process restart auth" or reload the controller.	
132025	Error	Station [mac:%m] [bssid:%m] is not enabled for pre-auth	Preauthentication is always disabled	
132026	Error	Station [mac:%m] [bssid:%m] trying to pre-authenticate with AP that does not have WPA2 enabled	Station trying to preauhenticate with AP that is not WPA2 enabled. Configure the ssid-profile to enable WPA2 and reload the AP.	
132027	Error	Station [mac:%m] associating to Unknown AP [bssid:%m] [menc:%d] [vl:%d]	Station is trying to associate with AP that is not registered. This log-message is generated when we detect a race-condition between STM, SOS and AUTH. AUTH is receiving EAP packets from SOS before it received the New-AP message from STM. If not, try rebooting the AP by executing "apboot" or powercycling the AP. If symptoms persist, then AUTH is either not receiving or not processing New-AP messages from STM. If all else fails, restart the AUTH process by executing "process restart auth" or reload the controller.	
132029	Error	Station [mac:%m] [bssid:%m] sent Unsupported EAPOL Type [type:%d]	Station sent an unsupported EAPOL packet. Ensure the station is configured properly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	

132032	Error	Invalid length in the [msg:%s] from Station [mac:%m] [bssid:%m] [len:%d]	Station sent the specified packet with invalid length. Ensure the station is configured properly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132033	Error	Invalid WPA Key Description Version [ver:%d] Station [mac:%m]	Station sent a WPA key message with invalid version. Ensure the station is configured properly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132035	Error	Invalid WPA2 Key Description Version [ver:%d] Station [mac:%m]	Station sent a WPA key message with invalid version. Ensure the station is configured properly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132036	Error	Station [mac:%m] [bssid:%m] sent Unknown EAP-Request [eaptype:%d]	Station send an EAP packet that is invalid. Ensure the station is configured properly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132037	Error	Station [mac:%m] [bssid:%m] sent username with length=[len:%d] which is not less than [MAX_USERNAME_SIZE:%d] or not able to be truncated	The user name sent by the station is larger than the maximum size supported or cannont be truncated. Configure station to use a shorter username and attempt authentication again.	
132038	Error	Station [mac:%m] [bssid:%m] sent Unsupported EAP type [eaptype:%d]	Station sent an EAP packet that is not supported. Ensure the station is configured correctly to perform an EAP authentication method that is supported by the Aruba controller. Ensure that the aaa-profile associated with the authentication request matches the authentication-method the client is sending to authenticate. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132039	Error	Station [mac:%m] [bssid:%m] sent Unsupported EAP Code [eapcode:%d]	Station send an EAP packet with unknown EAP code. Ensure the station is configured correctly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132042	Error	Sending empty username for user [mac:%m] - WPS is not enabled on AP [bssid:%m] [apname:%s]	Station sent no user name in the EAP Identity Request message. Ensure the station is configured correctly to perform EAP authentication. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132045	Error	Error remove stateful dot1x ACL	Failed to remove the ACLs configured for stateful dot1x authentication from the stateful_role or logon_role. This is because the "stateful-dot1x" ACL is not associated with the stateful_role or logon_role. Since we are disabiling stateful-dot1x anyway, no further action is required.	
132049	Error	Received Invalid digest from Server [srvip:%pI4], AP [ip:%pI4]	Received radius packet with invalid digest during stateful dot1x authentication. This error suggests a possible man-in-the-middle attack. Please contact your administrator to check status of your Radius server. Radius packet will be dropped.	
132050	Error	No Stateful configuration found that could verify the stateful response. [nasip:%pI4], [srvip:%pI4]	No server config entry was found for verifying the stateful dot1x response. Verify that the Radius server in question is configured in the applicable server-group on the controller.	
132051	Error	Failed to validate stateful radius response [nasip:%pI4] [srvip:%pI4] station [mac:%m]	Stateful dot1x authentication failed because validation failed. Please refer to previous log-message. If CONFIG_NOTFOUND, verify that the Radius server in question is configured in the applicable server-group on the controller. Otherwise, this may be a potential man-in-the-middle attack. Please contact your administrator to validate the status of your Radius sever.	

132055	Error	[__FUNCTION__:%s]: missing configuration for dot1x profile "[prof:%s]"	Specified Dot1x profile is not configured or has been deleted. Please validate that the controller configuration contains the specified dot1x profile.	
132056	Error	[__FUNCTION__:%s]: missing server-group configuration for dot1x in aaa-profile "[prof:%s]" for Station [mac:%m] [bssid:%m]	Specified server group for dot1x authentication in the aaa profile is not configured or has been deleted. Please validate that the controller configuration contains the specified server-group profile.	
132057	Error	Failed to send the radius request for Station [mac:%m] [bssid:%m]	Radius request for specified station is being dropped due to lack of system resources. Please free up system memory and other resources by throttling user-authentication requests.	
132059	Error	Multicast Key type of the AP [bssid:%m] [apname:%s] is not static-wep or dynamic-wep	Multicast key type is not static wep or dynamic wep for the specified AP. Please confirm that the specified ssid-profile is configured for WEP	
132060	Error	Unknown Multicast Key-type [menc:%d] for AP [mac:%m] [apname:%s]	The multicast key type for the specified AP is not known. Please validate the ssid-profile associated with the AP and reboot the AP.	
132061	Error	AP [bssid:%m] [apname:%s] configured with aaa profile [prof:%s] does not have an associated dot1x profile	No dot1x profile is configured for the specified aaa profile. Please configure a dot1x profile in the specified aaa profile.	
132062	Error	Wrong slot configured for AP [bssid:%m] [apname:%s]	Invalid key slot configured for the specified AP. This should never happen. If this happens, an internal error has occurred. Please reboot your controller.	
132063	Error	WPA Preshared Key not configured for AP [mac:%m]	WPA Preshared Key is not configured for the specified AP. Please configure a WPA Preshared Key for this AP.	
132064	Error	WPA Passphrase not configured for AP [bssid:%m] [apname:%s]	WPA passphrase not configured for the specified AP. Please configure a WPA Passphrase for this AP.	
132065	Error	AP [mac:%m] [apname:%s] configured with invalid static-wep key length [slot:%d] [size:%d]	AP is configured with invalid Static WEP key length. The valid key length is 40bits or 128bits. Please configure the AP with either a 40bit or 128bit key.	
132069	Error	No Radius server configuration with [srvip:%pI4] available for creating Stateful AP Configuration entry	While automatically creating stateful dot1x configuration entry the radius server specified was not found. Please configure the specified radius server configuration and try again.	
132073	Error	Wrong WPA OUI Element [oui:%d] from Station [mac:%m] [bssid:%m] [apname:%s]	Station sent WPA key message with invalid OUI element. Please identify the station and investigate why it is sending incorrect data.	
132074	Error	Version [stver:%d] does not match [apver:%d] in the [msg:%s] IE Elements from Station [mac:%m] [bssid:%m] [apname:%s]	Station sent WPA key message with invalid Version. Please identify the station and investigate why it is sending incorrect data.	
132075	Error	Multicast cipher from Station [mac:%m] [stmc:%X] does not match with AP [bssid:%m] [apmc:%X] [apname:%s]	Mismatch in the multicast ciphers specified by the station and AP. Please identify the station and investigate why it is sending incorrect data.	
132076	Error	Station [mac:%m] [bssid:%m] [apname:%s] sent invalid number of unicast ciphers [uc:%d]	Station sent invalid number of unicast cipher in the WPA IE element. Please identify the station and investigate why it is sending incorrect data.	
132077	Error	Station's [mac:%m] [stuc:%X] and AP's [bssid:%m] [apuc:%X] [apname:%s] unicast cipher suites does not match	Mismatch in the unicast cipher specified by the station and the AP	
132078	Error	Station [mac:%m] [bssid:%m] [apname:%s] sent invalid number of key management suite [km:%d]	Station sent invalid number of key management suite in the WPA IE element	
132079	Error	Station's [mac:%m] [stkm:%x] and AP's [bssid:%m] [apkm:%x] [apname:%s] key management suites does not match	Mismatch in the key management suite specified by the station and the AP	
132080	Error	Station [mac:%m] [bssid:%m] [apname:%s] did not specify the multicast cipher and the configured multicast cipher [mc:%X] did not match the default cipher TKIP	Station did not specify any multicast cipher and the multicast cipher specified by the is not TKIP	
132081	Error	Station [mac:%m] [bssid:%m] [apname:%s] did not specify the unicast cipher and the configured unicast cipher [mc:%X] did not match the default cipher TKIP	Station did not specify any unicast cipher and the multicast cipher specified by the AP is not TKIP	
132082	Error	Station [mac:%m] [bssid:%m] [apname:%s] did not specify the key management selector and the configured key management [km:%X] did not match the default - 802.1x	Station did not specify any key management selector and the configured key management on the AP is not 802.1x	

132083	Error	[Num:%d] TKIP Michael MIC failure was detected	Specified number of TKIP MIC failure was detected	
132084	Error	Two TKIP Michael MIC Failures were detected within [last_scan_time:%d] seconds.AP will be shutdown for next 60 seconds	Two MIC failures was received from the station within 60 secs. The AP must be shutdown for 60 secs	
132085	Error	Maximum number of %s Key exchanges attempted for station [name:%s] [mac:%m] [bssid:%m] [apname:%s]	Maximum number of key exchanges was attempted for the station	
132088	Error	Invalid WPA [ver:%d] Key message from Station [mac:%m] [bssid:%m] [apname:%s], reason:ACK bit set	WPA key message with ACK bit set was received from the station. This is invalid	
132089	Error	Invalid WPA [ver:%d] Key message from Station [mac:%m] [bssid:%m] [apname:%s],reason: Error flag without Request bit set	WPA key message with error flag without request bit set was received from the station. This is invalid	
132090	Error	Received TKIP Michael MIC Failure Report from the Station [mac:%m] [bssid:%m] [apname:%s]	Specified Station sent TKIP MIC failure report	
132091	Error	Wrong key type [kt:%d] in [msg:%s] from Station [mac:%m] [bssid:%m] [apname:%s]	Station sent wrong key type in the WPA key message	
132092	Error	Request bit set in [msg:%s] from Station [mac:%m] [bssid:%m] [apname:%s]	Station sent WPA key message with request bit set	
132093	Error	[msg:%s] from Station [mac:%m] [bssid:%m] [apname:%s] did not match the replay counter [stcnt1:%d][stcnt2:%d] vs [apcnt1:%d][apcnt2:%d]	Station and AP's replay counter does not match. The WPA key message from the station has to be dropped	
132099	Error	[msg:%s] from Station [mac:%m] [bssid:%m] [apname:%s] has invalid datalen [ln:%d] != 0]	Station sent WPA key message with invalid key length	
132104	Error	Invalid character in the passphrase [ch:%c]	Invalid characters in the WPA passphrase	
132105	Error	Invalid password len [ln:%zu]	Invalid WPA passphrase length	
132106	Error	Invalid ssid len [ln:%zu]	Invalid SSID length	
132113	Error	Station's [mac:%m] [strsn:%X] and AP's [bssid:%m] [aprsn:%X] [apname:%s] RSN Capability does not match	Station and AP's RSN capability does not match	
132114	Error	Failed to add xSec station [mac:%m] to AP [bssid:%m]	Failed to add xSec station to AP's station table	
132147	Error	Invalid length [ln:%d] during inner eap handling	Station sent invalid length in the inner eap	
132149	Error	MAC User Table Lookup Failed mac=[mac:%m] bssid=[bssid:%m]	Specified MAC is missing in the MAC User Table while trying to process the dot1x packet.	
132150	Error	Station [mac:%m] [bssid:%m] does not have 802.1x context	Station [mac:%m] [bssid:%m] does not have 802.1x context	
132152	Error	802.1x termination is disabled user [mac:%m], profile [dot1x_auth_profile:%s]	802.1x termination is disabled for the specified profile	
132155	Error	Station [mac:%m] [bssid:%m] sent inner EAP type [eaptype:%d] that is not supported	Station sent inner eap type that is not supported	
132156	Error	Station [mac:%m] [bssid:%m] sent inner EAP Start	Station sent inner eap start packet. This is invalid	
132157	Error	Station [mac:%m] [bssid:%m] sent inner EAP packet with more-fragments bit set	Station sent inner EAP packet with more fragment bit set. This is invalid	
132158	Error	Station [mac:%m] [bssid:%m] sent invalid EAP flag	Station sent invalid flag in the inner eap packet	
132159	Error	Station[mac:%m] [bssid:%m] sent invalid inner EAP Packet [eaplen:%d]	Station sent invalid len in the inner eap packet	
132161	Error	Station [mac:%m] [bssid:%m] sent Invalid TLS Record Layer Type [tlsrectype:%d]	Station sent invalid TLS record layer type	
132162	Error	Station [mac:%m] [bssid:%m] sent with unsupported TLS client version [ver:%X]	Station sent unsupported TLS client version	
132165	Error	Station[mac:%m] [bssid:%m] sent invalid MAC in the TLS Record layer	Station send invalid MAC in the TLS record layer	
132166	Error	Station[mac:%m] [bssid:%m] sent more than one TLS Application Data Record Layer	Station send more than one TLS application data record layer	
132167	Error	Verification of TLS Record Layer from Station [mac:%m] [bssid:%m] failed	Verification of the TLS record layer from the station failed	
132171	Error	Received EAP-NAK from Station [mac:%m] [bssid:%m], Station is configured with [eaptype:%s]	Station sent inner eap-nak	

132177	Error	Station [mac:%m] [bssid:%m] sent client finish is that is not 3DES encrypted	Station send client finish that is not 3DES encrypted. This is not supported	
132179	Error	Failed to decrypt the client finish message from Station [mac:%m] [bssid:%m]	Station sent the client finish message that failed to decrypt	
132180	Error	Station [mac:%m] [bssid:%m] sent Unknown SSL type in the client finish header [type:%d]	Station sent unknown SSL type in the client finish header	
132182	Error	Verify data sent by the Station [mac:%m] [bssid:%m] is not valid	Verify data sent by the specified station in not valid	
132185	Error	Failed to send the server finish for Station [mac:%m] [bssid:%m]	Failed to send server finish for the specified station	
132188	Error	No user-name found in the inner eap id response from Station [mac:%m] [bssid:%m]	Station did not send any user name in the inner eap id response	
132195	Error	Invalid EAP code [code:%d] in the EAP-TLV/Phase2 response from Station [mac:%m] [bssid:%m]	Station sent invalid eap code in the TLV response	
132196	Error	Invalid EAP TLV-Type [tlv_type:%d] in the EAP-TLV/Phase2 response from Station [mac:%m] [bssid:%m]	Station sent invalid TLV type	
132198	Error	Failed to load the CA List File [file:%s]	Failed to load the specified CA List File for 802.1x termination	
132199	Error	Failed to set up SSL buffers	Failed to set up SSL buffers	
132200	Error	Received TLS Client Finish but the client certificate [mac:%m][bssid:%m] is not verified	Received TLS Client Finish but the client certificate is not verified	
132201	Error	Failed to cache EAP-GTC authentication info of Station [name:%s] [mac:%m] [bssid:%m] in the Local Database Server	Failed to cache eap-gtc authentication information of the station in the Internal server	
132203	Error	Station [mac:%m][bssid:%m] sent a EAP-NAK, requesting unsupported inner-eap-type [type:%d]	Unsupported inner-eaptype requested by station	
132204	Error	Inner eapid mismatched [id1:%d]:[id2:%d] for station [mac:%m] [bssid:%m]	Mismatch between the eapid station sent and what was expected	
132205	Error	Invalid inner-eaptype configured [eaptype:%d]	Configured eaptype is not supported	
132206	Error	Multiple user name attributes in response packet.	The RADIUS response packet is invalid because it contains multiple user name attributes	
132208	Error	Station setup failed [mac:%m] [bssid:%m] [apname:%s] [uenc:%s] [menc:%s]	Station failed to start the security association	
132209	Error	No unicast ciphers supported by AP [bssid:%m] [apname:%s]	No unicast ciphers supported by AP with WPA2 opcode	
132210	Error	Error in cb msg processing, message to [ip:%s]:[port:%d]([app_name:%s]),[msg_code:%d], Msglen [len:%d], and Msgtype [msg_type:%d] failed with Errno [errno:%d], Errstr [errstr:%s]	error occurred during key propagation for a client in split/bridge/d-tunnel mode for DWEP/AES/TKIP encryption, the msg is corrupted, retry the authentication to resolve the issue.	
132211	Error	Station [mac:%m] [bssid:%m] sent a cert from which we couldn't extract the public key	Station sent a cert from which we couldn't extract the public key	
132212	Error	Station [mac:%m] [bssid:%m] certificate signature verification failed	Station sent a cert, but the certificate signature verification failed	
132217	Error	Failed to convert cert into DER format before sending to certmgr	Failed to convert cert into DER format before sending to certmgr	
132221	Error	Invalid EAP type [eaptype:%d] received for station[mac:%m][bssid:%m] configured in termination mode	Received invalid eap type for station that is configured in termination mode	
132222	Error	Received EAP packet on the wrong BSSID for station [mac:%m][bssid:%m]	Received eap packet on the wrong bssid	
132224	Error	Station [mac:%m] [bssid:%m] sent Unsupported EAP code [eapcode:%d]]	Station sent an EAP packet that is not supported. Ensure the station is configured correctly to perform an EAP authentication method that is supported by the Aruba controller. Ensure that the aaa-profile associated with the authentication request matches the authentication-method the client is sending to authenticate. If problem persists, check for packet-corruption by capturing sniffer-traces between client, AP and controller.	
132225	Error	MAC Authentication was not done for station [mac:%m] [bssid:%m]	MAC Authentication was not done for the specific station	
132226	Error	MAC Authentication was not successful and l2-fail-through is not enabled for station [mac:%m] [bssid:%m]	MAC Authentication was not successful and l2 fail thru knob was not enabled for the specific station	

132229	Error	Failed to publish PMK Cache to GSM channel for Station [mac:%m] [bssid:%m]	Failed to publish PMK Cache to GSM channel for the specified station	
132230	Error	Failed to publish Key Cache to GSM channel for Station [mac:%m]	Failed to publish Key Cache to GSM channel for the specified station	
132235	Error	[msg:%s] from Station [mac:%m] [bssid:%m] [apname:%s] the received msg isn't key4 message	received key message isn't key4 msg . The WPA key message from the station has to be dropped	
132236	Error	No unicast ciphers supported by WPA3 AP [bssid:%m] [apname:%s]	No unicast ciphers supported by AP with WPA3 opcode	
133000	Error	Internal Server instance not initialized, Dropping the response [msgtype:%d] from Internal User Database Server	To_be_filled_out	
133001	Error	No matching request for the response from Internal User Database Server [msgid:%d] [msgtype:%d]	To_be_filled_out	
133003	Error	Response from Internal User Database server failed validation	To_be_filled_out	
133006	Error	User [name:%s] Failed Authentication (Processing [act:%s] on [type:%s])	To_be_filled_out	
133009	Error	User [name:%s] [role:%s] Failed MSChapV2 Authentication	To_be_filled_out	
133013	Error	Unable to initialize Internal Database Server	To_be_filled_out	
133018	Error	User [name:%s] has multiple entries in the database	To_be_filled_out	
133019	Error	User [name:%s] was not found in the database	To_be_filled_out	
133021	Error	User [name:%s] is disabled in the database	To_be_filled_out	
133023	Error	Failed to set the standard output to file [name:%s]	To_be_filled_out	
133024	Error	Failed to execute the database export command [errno:%d]	To_be_filled_out	
133025	Error	[func:%s]([line:%d]): Database error '[errmsg:%s]' on command '[cmd:%s]'	To_be_filled_out	
133026	Error	Failed to export the Internal User Database to file [name:%s]	To_be_filled_out	
133027	Error	Failed in parsing DB query result for Table '[tbl:%s]'.	This indicats parsing error on user database query result.	
133030	Error	Failed to set the standard input to file [name:%s]	To_be_filled_out	
133035	Error	Database error [errmsg:%s]	To_be_filled_out	
133036	Error	Adding User [name:%s] failed, User already present in the database	To_be_filled_out	
133037	Error	Update user failed, no username specified	To_be_filled_out	
133043	Error	User [name:%s] is inactive in the database	To_be_filled_out	
133044	Error	Failed to delete the users from Internal User Database; [errmsg:%s]	To_be_filled_out	
133065	Error	[function: %s]: Failed to send PAPI message to [DstAddr: %s]:[DstPort: %d] code [msgtype: %d] error [errormsg: %s]	LOCALDB_SYNC failed to send PAPI message	
133099	Error	Hospitality User '[name:%s]' Failed Authentication	Failed the authentication of Hospitality user	
133100	Error	Hospitality User '[name:%s]' was not found in the database	Hospitality user not found	
133101	Error	Hospitality User '[name:%s]' has multiple entries in the database	Internal error, mulitiple hospitality user entries	
133102	Error	Internal database error, '[Call:%s]', Errno:[Errno:%d], Errstr:[Errstr:%s]	Internal error occoured while accessing hospitality database	
133103	Error	Hospitality User '[name:%s]' is disabled in the database	Hospitality user is disabled, internal error	
133106	Error	No matching request for the response from Internal Hospitality User Database Server, msgid=[msgid:%d], msgtype=[msgtype:%d]	To_be_filled_out	
133107	Error	Failed to start timer that resets cpsec_allowlist entry states from "approved" to "uncertified"	Failed to start timer that resets cpsec_allowlist entry states from "approved" to "uncertified"	
133110	Error	Could not create database schema [table:%s]	Internal error occoured while creating database schema	
133114	Error	Upgrading RAP allowlist to separate table failed.	This shows that attemped upgrade of RAP allowlist failed.	
133120	Error	Unable to initialize GSM	To_be_filled_out	
133123	Error	[func:%s]: Received Message with invalid length:[len:%d] from [sip:%s]:[sport:%u] MsgCode:[code:%u]([type:%s])	This indicates a message with invalid length is received at udbserver	
133124	Error	Failed to send Fetch-Request Message due to invalid length:[len:%d])	This indicates an error while sending fetch-request message due to invalid length at udbserver	
133127	Error	[func:%s]: Received AUTH_DB_REQ with invalid data-length:[len:%zu] from [sip:%s]:[sport:%u] MsgCode:[mcode:%u])	This indicates a message with invalid length is received at udbserver	
134103	Error	[func:%s](): Failed to send log level request to SYSLOGDWRAP.	This indicates error sending to syslogwrap.	
134111	Error	[func:%s](): PAPI_Init() returned failed.	This indicates error while doing PAPI_Init().	

134112	Error	[func:%s](): PAPI_AddLocking() returned failed.	This indicates error while doing PAPI_AddLocking().	
134115	Error	OFFLDR GSM: Error in requesting replay of existing GSM objects. Error:[err:%s].	This indicating error condition while requesting replay.	
134117	Error	OFFLDR GSM: Error in start receiving events. Error:[err:%s].	This indicating error condition while receiving GSM events.	
134118	Error	[func:%s](): failed in gsm_initialize() error:[err:%s].	This indicating error condition while receiving GSM events.	
134120	Error	[func:%s]([line:%d]): Error doing BN_CTX_new().	This indicating error condition while allocating a BN Context.	
134121	Error	[func:%s]([line:%d]): Error in creating ECC Group(group:[grp:%d], NID:[nid:%d]).	This indicating error condition while creating an EC Group.	
134122	Error	[func:%s]([line:%d]): Error in EC_POINT_set_compressed_coordinates_GFp(Group:[grp:%d], NID:[nid:%d]).	This indicating error condition while calling EC_POINT_set_compressed_coordinates_GFp().	
134123	Error	[func:%s]([line:%d]): Error in EC_KEY_generate_key(Group:[grp:%d], NID:[nid:%d]).	This indicating error condition while calling EC_KEY_generate_key().	
134124	Error	[func:%s]([line:%d]): Error in getting private or public key from EC generated key(Group:[grp:%d], NID:[nid:%d]).	This indicating error condition while getting private/public key.	
134125	Error	[func:%s]([line:%d]): Error in EC_POINT_get_affine_coordinates_GFp(Group:[grp:%d], NID:[nid:%d]).	This indicating error condition while calling EC_POINT_set_compressed_coordinates_GFp().	
134126	Error	[func:%s]([line:%d]): Error in ECDH_compute_key(Group:[grp:%d], NID:[nid:%d]).	This indicating error condition while calling EC_POINT_set_compressed_coordinates_GFp().	
134127	Error	[func:%s]([line:%d]): Error in new DhGrpHelper(Group:[grp:%d]).	This indicating error condition while allocating DH Group Helper().	
134130	Error	[func:%s]([line:%d]): Error in crypto operation while processing SAE data	This indicates crypto operation failure during SAE operations.	
134131	Error	[func:%s]([line:%d]): Resource allocation failed while processing SAE data	This indicates resource allocation failed during SAE operations.	
134132	Error	[func:%s]([line:%d]): Parsing of request message failed. Type:[type:%d]	This indicates problem in parsing of the offloader request message.	
135002	Error	[func:%s]([line: %d]): [msg:%s]	Generic debug log	
135007	Error	[func:%s](thread-id: [thread:%d]): station= [mac:%s] Sending [msg:%s].	Event log on parent process	
135012	Error	[func:%s]([line: %d])(thread-id: [thread: %d]): Peer creation failed for station= [mac:%s]. [msg:%s]	Event log on parent process	
135014	Error	[func:%s]([line: %d])(thread-id: [thread: %d]): Received fatal error for station= [mac:%s] while [msg:%s]	Event log on parent process	
135901	Error	[func:%s]([line: %d]), [msg:%s]	Unexpected condition occurred in SAE protocol library	
135906	Error	[func:%s], station= [mac:%s] State machine failed in [msg:%s]		
135908	Error	[func:%s], station= [mac:%s] Error while parsing [msg:%s] from offloader		
135912	Error	[func:%s], station= [mac:%s] Checking for token in group [grp:%d] but length is wrong. Expected [exp:%d]		
135913	Error	[func:%s],([line:%d]) station= [mac:%s] Error while assigning group to the peer. Reason: [msg:%s]		
135914	Error	[func:%s],([line:%d]) station= [mac:%s] Error while committing to peer. Reason: [msg:%s]		
135915	Error	[func:%s],([line:%d]) station= [mac:%s] Error while processing peer's commit. Reason: [msg:%s]		
135916	Error	[func:%s],([line:%d]) station= [mac:%s] Error while confirming to peer. Reason: [msg:%s]		
135917	Error	[func:%s],([line:%d]) station= [mac:%s] Error while process peer's confirm. Reason: [msg:%s]		
135918	Error	[func:%s],([line:%d]) station= [mac:%s] Error: [msg:%s]		
135919	Error	[func:%s],([line:%d]) station= [mac:%s] Error: [msg:%s]		

135920	Error	[func:%s],([line:%d]) station= [mac:%s] Error while computing PWE		
135921	Error	[func:%s],([line:%d]) ESSID= [essid:%s] Error while computing PT		
136001	Error	[func:%s](): Failed to initialize MySQL.	This indicated failure in initializing MySql.	
136002	Error	[func:%s](): Failed to connect to MySQL([dbname:%s]).	This indicated failure in connecting to MySql.	
136010	Error	[func:%s](): PAPI_Init() returned failed.	This indicates error while doing PAPI_Init().	
136011	Error	[func:%s](): PAPI_AddLocking() returned failed.	This indicates error while doing PAPI_AddLocking().	
136014	Error	[func:%s](): Failed to send log level request to SYSLOGDWRAP.	This indicates error sending to syslogwrap.	
136042	Error	RESTART-RADIUSD([req:%lu]@[worker:%s]): Failed to Restart radiusd.	This indicates an error while restarting radiusd.	
136045	Error	Invalid certificate '[cert:%s]' is used as Survival Server-certificate.	This indicates an invalid certificate is used by the Survival Server.	
136046	Error	[func:%s](): Failed to connect to PgSQL([dbname:%s]), connStatus:[status:%d] error:[err:%s].	This indicated failure in connecting to PgSql.	
137000	Error	Failed to calculate the HMAC-MD5 digest	Controller failed to calculate the HMAC-MD5 digest for RADIUS packet due to an internal error	Please contact Aruba tech-support if this problem persists.
137001	Error	Error [errno:%d],[errstr:%s] receiving packet [packet_len:%d], fd=[fd:%d]	An socket error occurred while receiving RADIUS server response	Please contact Aruba tech-support if this problem persists.
137002	Error	An error occurred while receiving RADIUS server response	An error occurred while receiving RADIUS server response	Please contact Aruba tech-support if this problem persists.
137003	Error	Discarding unknown response from server	RADIUS Server has returned a response that does not match the request or the packet could be corrupt	Validate RADIUS server configuration. Please contact Aruba tech-support if this problem persists.
137005	Error	An error occurred while receiving RADIUS server response on port 3799 (RFC 3576)	An error occurred while receiving RADIUS server response on port 3799 (RFC 3576)	Please contact Aruba tech-support if this problem persists.
137008	Error	RADIUS: Error [errno:%d],[errstr:%s] creating client socket	Internal error occurred while initiating connection with the RADIUS server	Please contact Aruba tech-support if this problem persists.
137009	Error	RADIUS: Error [errno:%d],[errstr:%s] in bind	Internal error occurred while connecting with the RADIUS server	Please contact Aruba tech-support if this problem persists.
137010	Error	Error [errno:%d],[errstr:%s] sending [data_len:%d] bytes on radius socket [sockfd:%d]	Internal error occurred while sending data to the RADIUS server	Please contact Aruba tech-support if this problem persists.
137011	Error	Received RADIUS server response with invalid length [len:%d]	The expected length of a RADIUS server response packet is between 20 and 4096 bytes.	Please check the length of response packet from the RADIUS server.
137012	Error	Not enough buffer space to verify RADIUS server response packet with length [totallen:%d]	The internal buffer is not big enough for the RADIUS response packet and RADIUS secret	Please check the length of the RADIUS response packet from the RADIUS server and the length of RADIUS secret.
137013	Error	Received non-matching ID in RADIUS server response [id:%d], expecting [seq_nbr:%d]	Received a response from the RADIUS server, but the sequence number doesn't match the request	Please check the RADIUS server is configured properly.
137014	Error	Received invalid reply digest from RADIUS server	The reply digest received from the RADIUS server doesn't match the calculated digest	Please check the RADIUS server is configured properly and verify shared secret configuration on the controller matches that on the RADIUS server
137016	Error	RADIUS server [server:%s],[fqdn:%s][ipaddr:%s] is out of sequence numbers	The PENDING request buffer to RADIUS server is already full (256). Response from RADIUS server seems to be slower than the rate at which the users are coming in	Please check the RADIUS server is configured properly and the connectivity between Aruba controller and RADIUS server is good.
137018	Error	Unknown RADIUS attribute ID [attrid:%d] in [func:%s]	The RADIUS attribute is not known	Please use "show aaa radius-attributes" command to check if the attribute ID is supported.
137019	Error	Received attribute with invalid length [attrlen:%d] in [func:%s]	Received RADIUS attribute with invalid length, while extracting the attribute-value pairs	Please check the RADIUS server is configured properly and the connectivity between Aruba controller and RADIUS server is good.

137021	Error	RADIUS attribute [name:%s] has unknown type [type:%d] in [func:%s]	Received unknown RADIUS attribute type, while extracting the attribute-value pairs	Please check the supported RADIUS attribute type.
137022	Error	Unknown RADIUS attribute name [name:%s] in [func:%s]	Received unknown RADIUS attribute name, while extracting the attribute-value pairs	Please use "show aaa radius-attributes" command to check if the attribute name is supported.
137023	Error	Unknown RADIUS attribute [attr_value:%s] in [func:%s]	Controller received an unknown RADIUS attribute while extracting the attribute-value pairs from Radius server response	Please use "show aaa radius-attributes" command to check if the attribute value is supported.
137025	Error	Value pair is NULL or empty attribute [id:%d] in [func:%s]	Internal error occurred while converting the attribute-value pairs received in RADIUS response to strings	Please contact Aruba tech-support if this problem persists.
137029	Error	RADIUS: Error [errno:%d], [errstr:%s] creating rfc3576 socket	Internal error occurred while initiating connection with RADIUS server	Please contact Aruba tech-support if this problem persists.
137030	Error	RADIUS: Error [errno:%d], [errstr:%s] in rfc3576 bind	Error occurred while connecting to RADIUS server	Please contact Aruba tech-support if this problem persists.
137033	Error	rc_pack_list: Attribute list exceeds 8192 bytes, dropping request	rc_pack_list: Attribute list exceeds 8192 bytes, dropping request	
137036	Error	RADIUS: Error [errno:%d],[errstr:%s] setting client socket options	Internal error occurred while setting connection options with the RADIUS server	Please contact Aruba tech-support if this problem persists.
137038	Error	Timer [tmr:%s] add/ remove routine failed. Error [err:%d]	Timer create or destroy routine failed.	
142005	Error	[message:%s]	L2TP generic error.	
199802	Error	[function:%s], [file:%s]:[line:%d]: [error:%s]	This log indicates that we encountered an internal security error. Technical support should be contacted with this information.	
199804	Error	[function:%s], [file:%s]:[line:%d]: [error:%s]	This log indicates that we encountered an internal cluster error. Technical support should be contacted with this information.	
100106	Info	FIPS Info: [msg:%s]	This is a FIPS info log in security module.	
103000	Info	[extsrcip:%s]->[extdstip:%s]([innerip:%s]) [type:%s]:[vpntype:%s]:[direction:%s]:TID [tunid:%d]:SPI [spi:%s]		
103003	Info	Failed to find matching ISAKMP PSK for Conductor-Local VPN	To be filled out	
103004	Info	No ISAKMP PSK found for peer [IP:%s]	ISAKMP key was not found for the specified peer. Validate configuration	
103005	Info	ISAKMP PSK is not defined for peer [name:%s]	ISAKMP key is not defined for the specified peer	
103006	Info	ISAKMP PSK is not defined for peer	ISAKMP key is not defined for the specified peer	
103007	Info	IKE Aggressive Mode Phase 1 succeeded for peer [IP:%s]	IKE Aggressive Mode Phase 1 succeeded for the specified peer	
103009	Info	IKE Main Mode Phase 1 succeeded for peer [IP:%s]	IKE Main Mode Phase 1 succeeded for the specified peer	
103015	Info	IKE Main Mode Phase 1 succeeded for peer [IP:%s]	IKE Main Mode Phase 1 succeeded for the specified peer	
103017	Info	Could not validate IKE Phase 1 ID of peer for Conductor-Local VPN	Failure in negotiation of IKE SA due to incorrect IKE Phase 1 ID	
103018	Info	IKE Phase 1 hash mismatch. Most likely because IKE pre-shared key or certificate mismatch.	IKE Phase 1 hash mismatch. Most likely because IKE pre-shared key or certificate mismatch	
103019	Info	IKE Quick Mode failed: selectors don't match Conductor-Local VPN	Failure to negotiate IPSEC SA because selector don't match Conductor-Local VPN	
103021	Info	IKE Quick Mode failed: selectors don't match Site-Site VPN	Failure to negotiate IPSEC SA because selector don't match Site-Site VPN	
103022	Info	IKE Quick Mode succeeded for peer [IP:%s]	IKE Quick Mode succeeded for the specified peer	
103024	Info	IKE Quick Mode failed, invalid hash from [IP:%s], possible attack.	Failure in IPSEC SA negotiation due to invalid hash from peer	
103026	Info	IKE Quick Mode failed, peer ID is not FQDN from [IP:%s]	Failure in IPSEC SA negotiation because peer ID is not FQDN	
103028	Info	IKE Quick mode failed, no proposal chosen from [IP:%s]. AH proposed without an algorithm		
103029	Info	IKE Quick Mode failed probably due to PFS config mismatch between client [IP:%s] and server.		
103030	Info	IKE Quick Mode failed: differing group descriptions in SAs from client [IP:%s]	IKE Quick Mode failed due to differing group descriptions in SAs from client	
103033	Info	IKE Quick Mode succeeded internal [IP:%s], external [extIP:%s]	IKE Quick Mode (XAuth) succeeded	
103034	Info	IKE Quick Mode succeeded from [IP:%s] external [extIP:%s]	IKE Quick Mode succeeded	
103035	Info	Initiator IKE Phase 2 Identity doesn't match for ipsec-map [name:%s]	Initiator IKE Phase 2 Identity doesn't match for specified ipsec-map	
103040	Info	IKE XAuth idle timeout for [IP:%s] (External [extIP:%s])	XAuth VPN connection terminated due to idle timeout	

103042	Info	IKE XAuth down admin request for [IP:%s] (External [extIP:%s])	XAuth VPN connection terminated due to admin request	
103047	Info	IKE XAuth succeeded for [IP:%s] (External [extIP:%s]) for [role:%s]	VPN authentication successful for XAUTH user	
103051	Info	IKE module gets local-conductor configuration	IKE module received local-conductor configuration	
103053	Info	Drop message from [IP:%s] due to invalid IKE shared-secret	System dropped IKE request from remote AP due to misconfigured PSK or client certificate	
103054	Info	Dropping IKE message drop from [IP:%s] [port:%d] due to notification type:[notify:%s]	System dropped IKE message due to notification type	
103056	Info	IKE XAuth client down IP:[xauthIP:%s] External [extIP:%s]		
103057	Info	[type:%s] SA is deleted due to expiry	Expired IKE/IPSec Security Association was deleted	
103059	Info	Responder IKE Phase 2 Identity doesn't match for map [name:%s]	To be filled out	
103062	Info	[prefix:%s] [message:%s]	To be filled out	
103066	Info	Sending Cluster role change code [code:%d] at time [timestamp:%f]	Cluster-Role has changed due to configuration	
103069	Info	IKE received AP DOWN for [IP:%s] (External [extIP:%s])	XAuth VPN connection terminated due to AP going down or rebooting	
103070	Info	Sending Cluster role change code [code:%d] at time [timestamp:%f] to subscriber [s:%d]	Sending Cluster role information when process initializes	
103076	Info	IKEv2 IPSEC Tunnel created for peer [IP:%s]:[Port:%d]	IKEv2 IPSEC Tunnel created for the specified peer	
103077	Info	IKEv2 IKE_SA succeeded for peer [IP:%s]:[Port:%d]	IKEv2 IKE SA succeeded for the specified peer	
103078	Info	IKEv2 CHILD_SA successful for peer [IP:%s]:[Port:%d]	IKEv2 CHILD SA succeeded for the specified peer	
103079	Info	IKEv2 IKE_SA failed for peer [IP:%s]:[Port:%d] error:[err:%d]	IKEv2 IKE SA failed for the specified peer	
103080	Info	IKEv2 CHILD_SA failed for peer [IP:%s]:[Port:%d] error:[err:%d]	IKEv2 CHILD SA failed for the specified peer	
103081	Info	IKEv2 DPD detected dead peer [IP:%s]:[Port:%d]	IKEv2 SAs deleted for the specified peer due to Dead-Peer-Detection	
103082	Info	IKEv2 Client-Authentication succeeded for [IP:%s] (External [extIP:%s]) for [role:%s]	IKEv2 VPN authentication successful for Client	
103083	Info	IKEv2 Client-Authentication failed for user: [u:%s]	IKEv2 VPN authentication failed for the specified user	
103084	Info	IKEv2 EAP-Authentication failed for peer [IP:%s]:[Port:%d]	IKEv2 VPN EAP authentication failed for the specified user	
103085	Info	IKEv2 EAP-Authentication succeeded for [IP:%s] (External [extIP:%s])	IKEv2 VPN EAP authentication successful for Client	
103086	Info	IKEv2 PSK match failed for peer [IP:%s]:[Port:%d]	IKEv2 PSK match failed for the specified peer	
103087	Info	IKEv2 Cert MAC match failed for peer [IP:%s]:[Port:%d]	IKEv2 Cert MAC match failed for the specified peer	
103089	Info	IKEv2 IKE Proposal mismatched for peer [IP:%s]:[Port:%d] error:[err:%d]	IKEv2 IKE SA failed due to Proposal mismatch for the specified peer	
103090	Info	IKEv2 CHILD Proposal mismatched for peer [IP:%s]:[Port:%d] error:[err:%d]	IKEv2 CHILD SA failed due to Proposal mismatch for the specified peer	
103091	Info	IKEv2 Digital Signature verification failed for peer [IP:%s]:[Port:%d]	IKEv2 Digital Signature verification failed for the specified peer	
103092	Info	IKEv2 failed to find IPSEC-MAP for peer [IP:%s]:[Port:%d]	IKEv2 failed to find matching IPSEC-MAP for the specified peer	
103101	Info	IPSEC SA deleted for peer [IP:%s]	IPSEC SA deleted for specified peer	
103102	Info	IKE SA deleted for peer [IP:%s]	IKE SA deleted for specified peer	
104004	Info	Suspected Unsecure AP with BSSID [bssid:%s] SSID [ssid:%s] has been reclassified as: [rap_type:%s]	A suspected unsecure AP identified by the SSID and BSSID, has been reclassified as indicated	
104005	Info	AP [bssid:%m] has matched Rule [name:%s] to classify to suspected rogue with confidence level increase of [conf:%d]	To be filled out	
104006	Info	AP [bssid:%m] has matched Rule [name:%s] to classify to known-interfering	To be filled out	
105000	Info	PPP portion of PPTP or L2TP authentication timed out [user:%s]	PPP timeout during authentication. Please check authentication(radius/ldap/tacacs) server.	
105001	Info	Received authentication challenge during RSA/token exchange [user:%s]	Received authentication challenge during RSA/token exchange.	
105004	Info	PPP/VPN Authentication succeeded [user:%s] [IP:%s] [type:%s] [role:%s]	PPP/VPN Authentication succeeded	
106009	Info	AM: Wired Containment: MAC:[mac_addr:%s] IP:[ip:%s]	To be filled out	
106011	Info	AM: Wired Containment Tagged: MAC:[mac_addr:%s] IP:[ip:%s] VLAN:[vlanid:%d] GW-MAC:[gw_mac:%s] GW-IP:[gw_ip:%s]	To be filled out	
109002	Info	LDAP Server [name:%s]: Reinitialization server	A LDAP server is being reinitialized	

109003	Info	LDAP Server [name:%s]: Starting Timer to Initialize Server in [time:%d] ms	An internal timer is being started to kickoff LDAP server Initialization	
109004	Info	LDAP Server [name:%s]: TLS connection established successfully	TLS connection established successfully with a LDAP server	
109005	Info	LDAP Server [name:%s]: Admin - Using Clear Text Connection	Clear Text Connection will be used with LDAP server	
109007	Info	LDAP Server [name:%s]: Admin - LDAPS connection established successfully to port [port:%d]	LDAPS connection established successfully with a LDAP server	
109008	Info	LDAP Server [name:%s]: User - LDAPS connection established successfully to port [port:%d]	LDAPS connection established successfully with a LDAP server	
109011	Info	LDAP Server [name:%s]: Binding Admin to server	System sent bind request as admin user to authentication server	
109015	Info	LDAP Server [name:%s]: Starting Timer to rebind to server in [time:%d] ms	An internal timer is being started to kickoff rebinding with down LDAP server	
109016	Info	LDAP Server [name:%s]: Setting Server In Service	LDAP server is in service	
109017	Info	LDAP Server [name:%s]: Setting Server Out of Service	LDAP server is out of service	
109018	Info	LDAP Server [name:%s]: Unbinding Admin Context from the server	System is unbinding admin context from the server for cleanup purpose	
109019	Info	LDAP Server [name:%s]: Unbinding User Context from the server	System is unbinding user context from the server for cleanup purpose	
109023	Info	LDAP Server [name:%s]: Server is Disabled	LDAP server is disabled	
118011	Info	[string:%s]	This shows an informational message in Cert Mgr.	
118018	Info	[string:%s]	This shows an informational message in Cert Mgr for EST.	
121034	Info	RADIUS attribute not sent: [attribute:%s]	Controller has a reference to a RADIUS attribute that will be dropped.	
121035	Info	RADIUS type not sent: [type:%s]	Controller has a reference to a RADIUS type that will be dropped.	
122013	Info	authentication failed, server reply was [r:%d] ([msg:%s])	TACACS server authentication failed	
122025	Info	authorization failed, server reply was [r:%d] ([msg:%s])	TACACS server authorization failed	
122026	Info	[function : %s] [line : %d] source-interface [source_address : %s] selected for outgoing requests to TACACS-server [server : %s]	Source-interface for outgoing request to TACACS server	
124000	Info	[action:%s] datapath service [name:%s], id=[id:%d] proto=[proto:%s], port=[port1:%d]-[port2:%d]	Add or Remove ALG (application layer gateway) processing for a network service on the specified procotol and ports	
124003	Info	Result=[rs:%s]([ri:%d]), method=[m:%s], server=[s:%s], user=[u:%s]	This shows the result of an user authentication attempt along with authentication method, server and user name	
124005	Info	Health check for server=[s:%s] response='[r:%s]'	This shows the result of a health check for a server	
124010	Info	Configured radius server [name:%s]:[fqdn:%s]:[ip:%s]	Configured named Radius server	
124011	Info	Test authenticating user [usr:%s]:[p:%s] using server [s:%s]	The system is sending PAP authentication request to named server for testing purpose	
124012	Info	Selected server=[s:%s] for method=[m:%s]; user=[u:%s], essid=[e:%s], domain=[d:%s]	An authentication server was selected for named user	
124013	Info	Selected fail-thru server=[s:%s] for method=[m:%s]; user=[u:%s], essid=[e:%s], domain=[d:%s]	A fail-thru authentication server was selected for named user	
124017	Info	LDAP server [s:%s] initialized successfully	The LDAP server initialized successfully	
124019	Info	Test server response: [usr:%s]	Test server command completed with indicated result	
124020	Info	Applying bwm contract [name:%s] (#[contract:%d], [rate:%llu] bits/sec) to interface	A bandwidth contract was configured on an interface	
124030	Info	Received XML API cmd=[cmd:%s], agent=[agent:%s] IP=[ip:%s]	System received an XML API command from external agent.	
124032	Info	XML command=[cmd:%s] ([cmdid:%d]) from agent [ag:%s] IP=[ip:%s] result=Ok'	XML command processing completed successfully	
124038	Info	[action:%s] server [n:%s] for method=[m:%s]; user=[u:%s], essid=[e:%s], domain=[f:%s], server-group=[g:%s]	A server was selected for user authentication	
124039	Info	Time-range [name:%s] activated	A configured time-range was activated	
124040	Info	Time-range [name:%s] deactivated	A configured time-range was deactivated	
124041	Info	Enabled port [port:%s] for xSec, vlan [vlan:%d]	A port was enabled for xSec authentication	
124042	Info	Disabled port [port:%s] for xSec	A port was disabled for xSec authentication	
124043	Info	Adding L3 entry for AP [ip:%s]:[mac:%s]	An internal L3 entry was created for an access point	
124044	Info	Snapshot: update L3 role information	This module is updating internal L3 state as a result of configuration update	

124045	Info	Snapshot: update L2 role information	This module is updating internal L2 state as a result of configuration update	
124047	Info	Sending accounting stop for authenticated users	System is sending Radius accounting STOP record for all authenticated users	
124051	Info	Sending shutdown APs request	A request to shutdown APs is generated as result of WPA countermeasure	
124066	Info	Administrative User result=[rs:%s]([ri:%d]), method=[m:%s], username=[name:%s] IP=[ip:%s] auth server=[sg:%s]	Management user authentication Successful	
124068	Info	[string:%s]	This shows an auth informational message	
124269	Info	[func:%s](): Clear Mux Tunnel Hash Table	This indicates Mux Tunnel Hash Table is cleared	
124606	Info	[func:%s](): Auth-Survivability State: [st:%s].	This indicates Auth-Survivability state is changed	
124707	Info	DenyList on station:[mac:%s], ARP-PKT:: smac:[smac:%s] oper:[oper:%x] sender-mac:[sha:%s] sender-ip:[sip:%s] target-mac:[tmac:%s] target-ip:[tip:%s]	This shows an ARP-spoof packet was denylisted	
124708	Info	DenyList due to PKT:[pkt:%s]	This dumps a denylisted packet	
124709	Info	Drop ARP-packet with unknown-IP: smac:[mac:%s] sender-mac:[smac:%s] sender-ip:[sip:%s]	This indicates an ARP-packet is dropped due to bad IP	
124710	Info	Drop IP-Spoofing ARP-packet: smac:[mac:%s] sender-mac:[smac:%s] sender-ip:[sip:%s] exsting-mac:[exist:%s]	This indicates an ARP-packet is dropped due to IP-Spoffing	
124711	Info	[func:%s](authsurv:[enabled:%d]): Can not use Survival-server - No OOS server in server-group:'[sgname:%s]'.	This indicates Survival-server will NOT be used due to no OOS server in the group.	
124828	Info	[func:%s](): Clear Enet SAP Hash Table	This indicates ENET SAP Table is cleared	
124916	Info	Received Conductor IP response from CFGM: SET CONDUCTOR IP to [ip:%s]([ipv4:%s])	This shows an internal debug message	
125001	Info	User will be inactive, management [role_name:%s] is not created yet	Management user is created, but would remain inactive as the corresponding management role is not created	
125014	Info	Changing the User Status [user_name:%s]	The specified user status has been updated	
125017	Info	User [user_name:%s] is available only from the console	The specified user is a management recovery user, and can login to the system only from the console	
125018	Info	Skipping Radius authentication for user [user_name:%s]	The specified user is a management recovery user, authentication is performed against the local database	
125025	Info	Authentication of management users via Radius is disabled	Message indicating that authentication of managment users via Radius is disabled	
125042	Info	Can't delete entries from database, Error [Error:%s]	Internal error occurred while deleting mgmt-user for cert based authentication and the references for the certificate has reached 0, and error occurred while updating the certificate information in the backend database	Re-Create the mgmt-users for certificate authentication and delete the user
125048	Info	CA certificate may not have been loaded on the switch	While configuring the management user for WebUI certificate authentication, user's CA certificate must be loaded first	
125049	Info	Users Public Key may not have been loaded on the switch	While configuring the management user for SSH public key authentication, user's public key must be loaded first	
125063	Info	User [user_name:%s] created, with management role [role_name:%s]	Management user is created	
125064	Info	User [user_name:%s] removed	Management user is removed	
125065	Info	User [user_name:%s] created, with management role [role_name:%s], serial [serial:%s], CA cert [ca_cert:%s]	Management Cert user is created	
125066	Info	User [user_name:%s] removed, with serial [serial:%s], CA cert [ca_cert:%s]	Management Cert user is created	
125067	Info	User [user_name:%s] created, with management role [role_name:%s], client public cert [client_cert:%s]	Management Cert user is created	
125068	Info	User [user_name:%s] removed, with CA cert [client_cert:%s]	Management Cert user is created	

125069	Info	User [user_name:%s] created, with management role [role_name:%s], client public cert [client_cert:%s], revocation check point [rcp_name:%s]	Management Cert user is created	
125070	Info	Authentication Succeeded for User [user_name:%s], connection type [conn_type:%s]	SSH Public Key user authentication completed successfully	
132000	Info	xSec is enabled wired users	xSec is enabled for wired users	
132001	Info	xSec is disabled for wired users	xSec is disabled for wired users	
132012	Info	[func:%s](): Skip Sending do-key-handshake to dot1x due to '[reason:%s]'	Suspend sending do-key-handshake to dot1x	
132019	Info	Station [name:%s] [mac:%m] was Machine authenticated	Station successfully authenticated the machine account	
132020	Info	Station [name:%s] [mac:%m] failed Machine authentication update role [rl:%s]	Station failed to authenticate the machine account	
132021	Info	Station [mac:%m] [bssid:%m] is in Held state	Authenticator is in the held state for the specified station. In this state no response from the station is accepted till the end of quiet period. This to avoid DOS attacks.	
132028	Info	Dropping EAPOL request from Station [mac:%m] reason:AP [bssid:%m] [apname:%s] only is configured for Static-WEP	Station is trying to send EAP packets to AP that is only configured with Static-WEP. Either configure your client to support static-WEP authentication or configure the ssid-profile on the controller to support an 802.1x authentication method.	
132030	Info	Dropping EAPOL packet sent by Station [mac:%m] [bssid:%m]	Dropping the EAPOL packet sent by the specified station. Check preceding log-messages to determine the reason the EAPOL packet is being dropped.	
132044	Info	Enabled Stateful Radius	Stateful Dot1x is enabled. Controller will start monitoring EAPOL frames to track authentication status.	
132048	Info	Disabled Stateful Radius	Stateful Dot1x is disabled. Controller will stop monitoring EAPOL frames to track authentication status.	
132053	Info	Dropping the radius packet for Station [mac:%m] [bssid:%m] doing 802.1x	Radius packet for the specified station is dropped. Either the station has disconnected, has already authenticated or it is busy. If reauthentication is required, the station will request authentication again.	
132066	Info	Station[mac:%m] [bssid:%m] [apname:%s] [vl:%d] [gretype:%d] VLAN has been updated	Station VLAN has been changed. This is because of VLAN derivation rules	
132067	Info	Cleaning up the Stateful AP Configuration	Clear all the stateful dot1x configuration entries	
132068	Info	Removing all the Stateful config entries	Remove all stateful dot1 configuration entries	
132070	Info	Removing trusted AP [mac:%m]	Remove the Trusted AP with the specified MAC address	
132071	Info	Added trusted AP [mac:%m]	Add the trusted AP with the specified MAC address	
132086	Info	WPA [ver:%d] Key exchange failed to complete, de-authenticating the station [mac:%m] associated with AP [bssid:%m] [apname:%s]	WPA key exchange failed to complete, deauthenticating the station	
132131	Info	FIPS mode is enabled	FIPS mode is enabled	
132132	Info	FIPS mode is disabled	FIPS mode is disabled	
132133	Info	WPA Countermeasure is enabled	WPA Countermeasure is enabled	
132134	Info	WPA Countermeasure is disabled	WPA Countermeasure is disabled	
132197	Info	Maximum number of retries was attempted for station [name:%s] [mac:%m] [bssid:%m], deauthenticating the station	Maximum number of retries was attempted for station to complete the authentication phase. Deauthenticating the station	
132202	Info	Successfully downloaded the certs [rootcert:%s] [servercert:%s] for EAP termination	Successfully downloaded the certificates for EAP termination	
132207	Info	RADIUS reject for station [name:%s] [mac:%m] from server [server:%s].	Radius packet for the specified station was rejected by the server.	
132218	Info	Skipping certificate common name check for username=[user:%s] MAC=[mac:%s]	Based on configuration settings, the check for the certificate common name against a AAA server was skipped.	
132219	Info	MAC=[mac:%s] Local User DB lookup result for Machine auth=[r3:%s]	Local user database lookup result for Machine authentication status.	
132233	Info	Delete ALL stations in sap [bssid:%s]	This shows an internal debug message	

133002	Info	Response from Internal User Database Server contains Unknown Message Type [msgtype:%d]	To_be_filled_out	
133004	Info	Received Authentication Request for User [name:%s]	To_be_filled_out	
133005	Info	User [name:%s] [role:%s] Successfully Authenticated	To_be_filled_out	
133007	Info	Received MSChapV2 Authentication request for User [name:%s]	To_be_filled_out	
133008	Info	User [name:%s] [role:%s] Successfully MSChapV2 Authenticated	To_be_filled_out	
133010	Info	Received request for adding User [name:%s] to the database	To_be_filled_out	
133011	Info	Failed to add User [name:%s] to the database	To_be_filled_out	
133014	Info	Starting Internal User Database Server	To_be_filled_out	
133015	Info	Current Internal User Database Server Version is [ver:%d]	To_be_filled_out	
133017	Info	Successfully created the Internal User Database	To_be_filled_out	
133022	Info	User [name:%s] entry has expired, deleting from the database	To_be_filled_out	
133029	Info	Successfully exported the Internal User Database to [filename:%s]	To_be_filled_out	
133034	Info	Successfully imported the Internal User Database from file [name:%s]	To_be_filled_out	
133039	Info	Syncing with Config Manager...	Debug message indicating the start of internal syncing of configuration	
133040	Info	Retrieving Config from Config Manager...	Debug message indicating the start of internal receiving of configuration	
133041	Info	Done Retrieving Config from Config Manager...	Debug message indicating the success of internal receiving of configuration	
133042	Info	Done Syncing with Config Manager...	Debug message indicating the completion of internal sync of configuration	
133046	Info	Client process called auth_db_add_entry_async() [name: %s]	Client process executed auth_db_add_entry_async()	
133047	Info	Client process called auth_db_del_entry_async() [name: %s]	Client process executed auth_db_del_entry_async()	
133048	Info	Client process called auth_db_update_entry_async() [name: %s]	Client process executed auth_db_update_entry_async()	
133049	Info	Client process called auth_db_query_db_async() [name: %s]	Client process executed auth_db_query_db_async()	
133056	Info	[function: %s] [SrcAddr: %s][SrcPort: %d] Sending PAPI message to [DstAddr: %s][DstPort: %d] [msgtype: %d] [name: %s]	AUTH DB_API sending PAPI message	
133057	Info	[function: %s] [SrcAddr: %s][SrcPort: %d] Failed to send PAPI message to [DstAddr: %s][DstPort: %d] [msgtype: %d] [name: %s]	AUTH DB_API failed to send PAPI message	
133064	Info	[function: %s] [SrcAddr: %s][SrcPort: %d] Sending PAPI message to [DstAddr: %s][DstPort: %d] [msgtype: %d] [name: %s]	LOCALDB_SYNC sending PAPI message	
133067	Info	Querying switch IP	LOCALDB_SYNC querying switchip	
133068	Info	[function: %s] Retrying switchip query [retries: %d]	LOCALDB_SYNC Retrying switchip query	
133069	Info	[function: %s] Received switchip response [switchip: %s]	LOCALDB_SYNC Received switchip response	
133070	Info	Querying conductor IP	LOCALDB_SYNC querying conductorip	
133071	Info	[function: %s] Retrying conductorip query [retries: %d]	LOCALDB_SYNC retrying conductorip query	
133072	Info	Received conductor IP response [conductorip: %s], switch role [role: %d]. Old IP [old_conductorip: %s], old switch role [old_role:%d]	LOCALDB_SYNC Received conductor IP response	
133073	Info	[function: %s] UDB_SERVER SAPI state is UP	UDB_SERVER SAPI state is UP	
133074	Info	[function: %s] Local-switch sending UDB SYNC Request to [conductorip: %s]	Local-switch sending UDB SYNC Request	
133075	Info	[function: %s] Local-switch resending UDB SYNC Request to [conductorip: %s]	Local-switch resending UDB SYNC Request	
133076	Info	[function: %s] Conductor-switch received UDB SYNC Request from [localip: %s]	Conductor-switch received UDB SYNC Request	
133077	Info	[function: %s] Conductor-switch sending UDB SYNC Response to [localip: %s]	Conductor-switch sending UDB SYNC Response	
133078	Info	[function: %s] Local-switch received UDB SYNC Response from [conductorip: %s]	Local-switch received UDB SYNC Response	
133079	Info	[function: %s] Local-switch failed to register with [conductorip: %s] [result: %d]	Local-switch failed to register with conductor-switch	
133080	Info	[function: %s] Local-switch received corrupt message from [srcip: %s]	Local-switch received corrupt message	

133081	Info	[function: %s] Conductor-switch sending request to fully-sync allowlist to [localip: %s]	Conductor-switch sending request to fully-sync allowlist	
133082	Info	[function: %s] Conductor-switch failed to read full-sync file for sync with [localip: %s] [file: %s]	Conductor-switch failed to read full-sync file	
133083	Info	[function: %s] Local-switch received request to fully-sync allowlist from [conductorip: %s]	Local-switch received request to fully-sync allowlist	
133084	Info	[function: %s] Local-switch failed to save full-sync request from [conductorip: %s]	Local-switch failed to register to save full-sync request	
133085	Info	[function: %s] Local-switch sending full-sync response to [conductorip: %s]	Local-switch sending full-sync response	
133086	Info	[function: %s] Conductor-switch received full-sync response from [localip: %s] [result: %d]	Conductor-switch received full-sync response	
133087	Info	[function: %s] Conductor-switch syncing [msgtype: %d] element with [localip: %s]	Conductor-switch syncing element with local	
133088	Info	[function: %s] Conductor-switch received sync-ack for [msgtype: %d] element from [localip: %s]	Conductor-switch syncing element with local	
133096	Info	[function: %s] Upgrading database [dbname: %s]	Upgrading database	
133097	Info	Received Authentication Request for Hospitality User [name:%s]	Internal message indicating the receipt of authentication request	
133098	Info	Hospitality User [name:%s] [role:%s] Successfully Authenticated	Authentication of hospitality user succeeded	
133104	Info	Hospitality User '[name:%s]' entry has expired, deleting from the database	Informational message upon deletion of hospitality user	
133105	Info	Internal User Database Server received Unknown Request Type [reqtype:%d]	To_be_filled_out	
133111	Info	Database sync started	Database sync started	
133115	Info	RAP allowlist upgraded successfully. Records upgraded=[num_rec:%d]	This shows that RAP allowlist was successfully upgraded.	
133126	Info	Ignore received localdb-sync message MsgCode:[mcode:%u] from [sip:%s]:[sport:%u] due to NOT in SYNC-STARTED state	Receiving localdb-sync message while it's not in sync-started state	
133500	Info	Initializing db_sync foreign parameters.	udbserver requesting db_sync parameter values from other processes	
133501	Info	Initializing db_sync internal parameters.	udbserver initializing db_sync internal parameters, starting timers and initiating db_sync registration if necessary	
133502	Info	Failed to initialize virtual-clock	Failed to initialize virtual-clock.	
133503	Info	Failed to initialize virtual-clock timer	Failed to initialize virtual-clock timer.	
133504	Info	Failed to initialize conductor-switch-list timer	Failed to initialize conductor-switch-list timer.	
133505	Info	Failed to initialize local-switch-list timer	Failed to initialize local-switch-list timer.	
133506	Info	Failed to initialize standalone timer	Failed to initialize standalone timer.	
133507	Info	Failed to initialize sync-state hash table	Failed to initialize sync-state hash table.	
133512	Info	Sending db_sync registration request to [ipaddr:%s] for db=[db_type:%s]	Sending db_sync registration request to remote switch	
133513	Info	Received db_sync registration request from [ipaddr:%pI4] mac [macaddr:%s]	Received db_sync registration request from remote switch	
133514	Info	Sending db_sync registration response to [ipaddr:%pI4]	Sending db_sync registration response to remote switch	
133515	Info	Received db_sync registration response from [ipaddr:%pI4] mac [macaddr:%s]	Received db_sync registration response from remote switch	
133523	Info	Cluster role changing from [old_cluster_role:%s] to [new_cluster_role: %s] time [timestamp: %f]	Cluster role change	
133524	Info	Received unknown cluster-role change request [new_cluster_role: %d]	Cluster role change	
133525	Info	Received reg-response error [error: %d] from [ipaddr:%s]	Cluster role change	
133527	Info	Ignoring retransmitted role change message [old_cluster_role:%s] to [new_cluster_role: %s] last ts [last_ts: %f] new ts [new_ts: %f]	Cluster role change	
133528	Info	Received invalid role change message magic header 0x[magic: %x]	Cluster role change	

133529	Info	Received cluster role change magic 0x[magic: %x] role [new_cluster_role: %s] time [timestamp: %f]	Cluster role change	
134100	Info	Off-Loader Server started	This indicated the Off-Loader server is started	
134108	Info	[func:%s](): Off-Loader process is initialized.	This indicates Off-Loader process is initialized.	
136000	Info	Auth-Survival Server started	This indicated the Survial server is started	
136017	Info	[func:%s](): Broadcast Survival-Server Status:[st:%s].	This indicates State Change for the Survival-Server is broadcasted.	
136020	Info	[func:%s](): survival process is initialized.	This indicates survival process is initialized.	
136023	Info	[func:%s](): Spawned the radiusd process(pid: [pid:%d]).	This indicates radiusd is spawned.	
136024	Info	[func:%s](): Change to use Server-Cert:[name:%s].	This indicates Server-certicate is changed.	
136025	Info	[func:%s](): Change Cache-Lifetime:[time:%d].	This indicates Cache-Lifetime is changed.	
136026	Info	[func:%s](): Re-Spawning radiusd process(pid:[pid:%d]).	This indicates respawning radiusd.	
136027	Info	[func:%s](): Terminate radiusd process(pid: [pid:%d]).	This indicates radiusd is stopped.	
137034	Info	RADIUS attribute not sent: [attribute:%s]	Controller has a reference to a RADIUS attribute that will be dropped.	
137035	Info	RADIUS type not sent: [type:%s]	Controller has a reference to a RADIUS type that will be dropped.	
142000	Info	Creating L2TP Tunnel from [outip:%s](innerip=[inip:%s])	An L2TP tunnel has been created.	
142001	Info	Deleting L2TP Tunnel from [outip:%s](innerip=[inip:%s])	An L2TP tunnel has been deleted.	
142002	Info	L2TP Tunnel from [outip:%s] timed out due to missed L2TP hellos)	L2TP tunnel timed out.	
142004	Info	[message:%s]	L2TP generic info.	
100105	Notice	FIPS Notice: [msg:%s]	This is a FIPS notice log in security module.	
103008	Notice	XAuth without IKE SA. Illegal message from client [IP:%s]	System received a illegal XAUTH message from a client. No security association was found	
103011	Notice	IPSEC AP is not licensed; dropping IKE request	System dropped IKE request from remote AP due to missing license	
103012	Notice	IPSEC VPN is not licensed; dropping IKE request	System dropped IKE request because of missing VPN license	
103064	Notice	Dropping IKE/IPSEC SA because we have exceeded the VPN license-limit of [sessions:%d]	Dropping VPN connection because we have reached the maximum limit of VPN licenses	
103072	Notice	VIA is not licensed; dropping IKE request	System dropped IKE request because of missing VIA license	
103074	Notice	Dropping IKE/IPSEC SA because we have exceeded the ACR license-limit	Dropping VPN connection because we have reached the maximum limit of ACR licenses	
104002	Notice	External DB Wired MAC check succeeded for BSS [bssid:%s] SSID [ssid:%s] MATCH [wired_mac:%s]	The shown AP was successfully found in the external database of valid MAC addresses	
106000	Notice	AM [bssid:%s]: Potentially rogue AP detected BSSID [bssid_str:%s] SSID [ssid:%s] MATCH MAC [mac:%s]	An AP has been detected with conditions that may cause it to be classified as a rogue (unsecure) or suspected rogue	
106001	Notice	AM [bssid:%s]: Potentially rogue AP detected BSSID [bssid_str:%s] SSID [ssid:%s]	An AP has been detected with conditions that may cause it to be classified as a rogue (unsecure) or suspected rogue	
106005	Notice	AM: Wireless containment: Sending type [subtype:%s] to AP [bssid:%s] from STA [mac:%s] channel [channel:%d]	To be filled out	
106006	Notice	AM: Wireless containment: Sending type [subtype:%s] from AP [bssid:%s] to STA [mac:%s] channel [channel:%d]	To be filled out	
106012	Notice	AM: Wireless tarpit containment: Sending Probe-Response with fake channel from AP [bssid:%m] to STA [mac:%m] on channel [channel:%d] with fake_channel [fc:%d]	To be filled out	
106013	Notice	AM: Wireless tarpit containment: Sending Probe-Response with fake BSSID for frame from AP [bssid:%m] to STA [mac:%m] on channel [channel:%d] with fake_bssid [fbssid:%m]	To be filled out	
106014	Notice	AM: Wireless tarpit containment: Sending Auth reply for frame from AP [bssid:%m] to STA [mac:%m] on channel [channel:%d] with algorithm [alg:%d] transaction [xn:%d] seq [seq:%d]	To be filled out	
106015	Notice	AM: Wireless tarpit containment: Sending Assoc-Response for frame from AP [bssid:%m] to STA [mac:%m] on channel [channel:%d] with aid [aid:%d] seq [seq:%d]	To be filled out	
106016	Notice	AM: Wireless tarpit containment: Client [mac:%m] is in tarpit for fake BSSID [bssid:%m] on channel [channel:%d]	To be filled out	

106017	Notice	AM: Wireless tarpit containment: Client [mac:%m] is in tarpit for fake channel [channel:%d] for BSSID [bssid:%m]	To be filled out	
109012	Notice	LDAP Server [name:%s]: Admin Bound successfully	System request to bind as admin user was successfull	
109021	Notice	LDAP: Truncated attribute '[name:%s]' to [len:%zu] bytes (original [olen:%d])	System truncated length of an attribute returned by the search result to 253	
121015	Notice	Purge Request: [packet_id:%d], [srv_ipaddr:%s], [fd:%d], [timer_id:%lu]	A new config was received (write memory on master), hence purging all the pending radius requests	
121017	Notice	Unknown vendor or attribute ID [vendor:%d]/[attrid:%d] in [func:%s]	The RADIUS vendor or the attribute ID is not known	Please use "show aaa radius-attributes" command to check if the vendor or attribute ID is supported.
121032	Notice	Purge Request: [packet_id:%d], [srv_ipaddr:%s], [fd:%d], [timer_id:%lu]	Radius Client IP change, hence purging all the pending radius requests	
124008	Notice	Denylisting user MAC=[mac:%s] IP=[ip:%s], reason=[r:%s]	A user has been denylisted	
124009	Notice	Set max authentication failure count for method '[mthd:%s]' to '[count:%d]'	Set maximum authentication failure count for an authentication method. If unsuccessful authentication count exceeds this limit, user will be denylisted	
124014	Notice	Taking Server [s:%s] out of service for [m:%d] mins	A server was taken out of service temporarily. This typically happens after switch fails to reach the server after multiple retries	
124015	Notice	Bringing Server [s:%s] back in service.	A server was brought back in service.	
124021	Notice	Set web server security protocol to [protocol:%s]	Web server security protocol was changed to include one or more from SSLv2, SSLv3 and TLSv1	
124022	Notice	Set web server cipher suite to [cipher:%s]	Web server cipher suite was changed to low, medium or high.	
124023	Notice	Disabling automatic redirect for captive portal	Disabling automatic redirect for captive portal. This is prevent captive portal on a MUX client.	
124024	Notice	Set sygate remediation failure role to [name:%s]	CIM remediation failure was reset	
124025	Notice	Administrative user '[name:%s]' authenticated successfully (role=[role:%s], privileged=[priv:%d])	Administrative user authenticated successfully and was assigned specified role. A privileged state indicated that user is dropped into enable mode automatically	
124036	Notice	NAT pool '[name:%s]' deleted	A NAT pool was deleted	
124037	Notice	NAT pool '[name:%s]' created; SNAT=[sip:%s]-[eip:%s], DNAT=[dip:%s]	A NAT pool was created	
124049	Notice	TACACS accounting is [action:%s]	TACACS accounting is enabled or disabled due to configuration change	
124050	Notice	TACACS accounting for [type:%s] commands is disabled	TACACS accounting for configuration, action, show or all commands is disabled due to configuration change	
124057	Notice	Server [s:%s] is up.	A server has responded to an authentication request.	
124065	Notice	TACACS+ Accounting Failed: result=[rs:%s]([ri:%d]), method=[m:%s], username=[name:%s] source=[ip:%s] auth server=[sg:%s]	TACACS+ accounting failed while using the specified server	
124685	Notice	{CFG} Sending mgmt-auth [mgmtmode:%s] message to fpapps.	This shows an internal debug message	
125023	Notice	Authentication Succeeded for User [user_name:%s], connection type SERIAL	Management user authentication completed successfully	
125024	Notice	Authentication Succeeded for User [user_name:%s], Logged in from [srcIp:%s] port [srcPort:%d], Connecting to [dstIp:%s] port [dstPort:%d] connection type [conn_type:%s]	Management user authentication completed successfully	
125028	Notice	Radius Authentication is [mode:%s]	Debug Message indicating the state of radius authentication	
125032	Notice	Authentication Succeeded for User [user_name:%s], Logged in from [srcIp:%s] port [srcPort:%d], Connecting to [dstIp:%s] port [dstPort:%d] connection type SSH	Management user authentication completed successfully	
125056	Notice	Since user '[user_name:%s]' is assigned 'no-access' role by radius authentication, the user will not be given any access.	User is assigned 'no-access' role.	
125057	Notice	Since user '[user_name:%s]' is assigned unknown role '[role_name:%s]' by radius authentication, the user will not be given any access.	User is assigned 'no-access' role.	

125058	Notice	Since user '[user_name:%s]' is not defined in authentication server, the user will not be given any access.	User not defined in the server database.	
125059	Notice	Since user '[user_name:%s]' authentication is rejected by authentication server, the user will not be given any access.	User access is rejected by the server role.	
126004	Notice	AP([RADIO_MAC:%m]@[NAME:%s]): Interfering AP: An AP detected an interfering access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP detected an access point classified as Interfering. The access point is declared Interfering because it is neither authorized or classified as Rogue.	This alert indicates an event that may affect your wireless infrastructure.
127004	Notice	AP([RADIO_MAC:%m]): Interfering AP: An AP detected an interfering access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP detected an access point classified as Interfering. The access point is declared Interfering because it is neither authorized or classified as Rogue.	This alert indicates an event that may affect your wireless infrastructure.
137015	Notice	Purge Request: [packet_id:%d], [srv_ipaddr:%s], [fd:%d], [timer_id:%ld]	A new config was received (write memory on master), hence purging all the pending radius requests	
137017	Notice	Unknown vendor or attribute ID [vendor:%d]/[attrid:%d] in [func:%s]	The RADIUS vendor or the attribute ID is not known	Please use "show aaa radius-attributes" command to check if the vendor or attribute ID is supported.
137032	Notice	Purge Request: [packet_id:%d], [srv_ipaddr:%s], [fd:%d], [timer_id:%ld]	Radius Client IP change, hence purging all the pending radius requests	
142007	Notice	[message:%s]	L2TP generic notice.	
100000	Warning	Security association validation failed, HMAC-MD5 digest does not match	NA	
100104	Warning	FIPS Warning: [msg:%s]	This is a FIPS warning log in security module.	
103065	Warning	Certificate "[certname:%s]" has either expired or is not yet valid.	The certificate chosen has either expired or is not yet valid.	Check the controller time settings, and check that the chosen certificate is currently valid.
103093	Warning	[prefix:%s] [message:%s]	Crypto PowerON Self Test msgs at bootup	
103103	Warning	[prefix:%s] [message:%s]	General warnings in IKE module	
104000	Warning	FLAGGING AP with BSSID [bssid:%s] SSID [ssid:%s] as an Unsecure AP	The identified AP has been flagged as an unsecure AP	
104001	Warning	FLAGGING AP with BSSID [bssid:%s] SSID [ssid:%s] as an Unsecure AP Wired MAC [match_mac:%s] IP [match_ip:%s]	The identified AP has been flagged as an unsecure AP	
104003	Warning	FLAGGING AP with BSSID [bssid:%s] SSID [ssid:%s] as a Suspect Unsecure AP Wired MAC [match_mac:%s] Confidence Level [conf_level:%d]	An AP has been detected with conditions that may cause it to be classified as a rogue (unsecured) or suspected rogue; the confidence level is below the threshold for containment	
106010	Warning	AM [bssid:%s]: Containment enabled on Suspect Rogue AP: BSSID [ap_bssid_str:%s], SSID [ssid:%s], Conf-Level [conf_level:%d]	Containment has been enabled for a suspected rogue AP because the confidence level for that AP equals or exceeds the configured value for that setting	
109013	Warning	LDAP Server [name:%s]: Connectivity lost to the Server, trying to re-establish	System lost connection with LDAP server. Server will be marked out-of-service temporarily and requests will be sent to other servers in the server-group	
118009	Warning	[string:%s]	This shows a warning message in Cert Mgr.	
118010	Warning	OCSP Response's freshness check failed. Please check if clocks of OCSP responder and this device are in sync	This shows a warning message indicating there can be clock skew between Responder and the Controller or the Responder is not sending fresh responses	
118017	Warning	[string:%s]	This shows a warning message in Cert Mgr for EST.	
121004	Warning	RADIUS server [name:%s] server-group [group:%s] -[fqdn:%s]-[ipaddr:%s]-[sin_port:%u] timeout for client=[cbuf:%s] auth method [server:%s]	RADIUS Server is unreachable. The server could be down or there is connectivity problem	Check RADIUS server connectivity
121006	Warning	RADIUS (RFC 3576): Ignoring request from unknown client [srv_ipaddr:%s] port([srv_port:%d])	A request was received on RADIUS port 3799 (RFC 3576), but the RADIUS server is not configured.	If the request is expected, please configure RADIUS server using "aaa rfc-3576-server" command.

121007	Warning	RADIUS (RFC 3576): Ignoring request from client [srv_ipaddr:%s] port([srv_port:%d]) with unknown code [code:%d]	A request was received on RADIUS port 3799 (RFC 3576) with unknown code.	Please check RADIUS server and RFC 3799 client configuration
121027	Warning	Received RADIUS packet(code=[code:%u]) from [ip:%s] with invalid Message-Authenticator! Silently discard it.	Received RADIUS packet with INVALID Message-Authenticator	
122001	Warning	socket creation error for [addr:%s]	Internal Error occurred while initiating connection to TACACS server	
122002	Warning	connection to [addr:%s] failed	Communication error occurred while initiating connection to TACACS server	
122003	Warning	all possible TACACS+ servers failed	Connection attempt to all the configured TACACS server failed	
124006	Warning	[hit:%s]	A firewall rule with log option was hit	
124026	Warning	[string:%s]	This shows an internal warning message	
124031	Warning	Denylisting user [usr:%s] due to request from external XML agent [a:%s]	System denylisted a user because of request from an external XML API agent.	
124033	Warning	Invalid length [len:%d] in Radius response	System received attribute in radius response of length more than maximum allowed. The attribute was truncated.	
124034	Warning	Authentication request for admin user '[usr:%s]' ignored; reason='[r:%s]'	Authentication request for admin user as ignored because admin authentication is disabled or no authentication server is configured.	
124035	Warning	Invalid length [len:%d] in Radius request	An authentication request failed because system attempted to send attribute in radius request of length more than maximum allowed.	
124056	Warning	No server available for AAA client type [type:%s]		
124396	Warning	Validuser ACL Destination IP and Source/Destination Port values must be "any". Action should be permit or deny.	This shows an internal debug message.	
124409	Warning	[func:%s](): Dot1x-Auth-Server mismatch, original-server:[oserver:%s] current-server:[cserver:%s]. Failed the dot1x authentication.	This indicates auth-server mismatch under dot1x authentication	
124414	Warning	[func:%s](): Cannot delete non-exist IP:[ipaddr:%s] on Bridge-Mode client:[mac:%s], Ignore the operation.	This indicates try to delete non-exist IP-address on a Bridge-Mode client.	
124603	Warning	[func:%s]([proto:%s]): Failed to send Access credential([type:%s]) to Survival-Server for station:[st:%s] username:[uname:%s] survMethod:[smethod:%x].	This indicates an error while sending access credential to survival-server	
124605	Warning	[func:%s]([proto:%s]): Failed to send Deleting Access credential to Survival-Server for station:[st:%s] username:[uname:%s] survMethod:[smethod:%x].	This indicates an error while sending access credential to survival-server	
124658	Warning	[func:%s]([proto:%s]): Password Encryption failed for station:[st:%s] username:[uname:%s].	This shows a failure while encrypting password	
124827	Warning	XML command=[cmd:%s] ([cmdid:%d]) from agent [ag:%s] IP=[ip:%s] result=Error, error='[e:%s]'	XML command processing did not complete successfully.	
124867	Warning	Authentication type [type:%s] not supported for role download	CPPM role download feature is currently not supported for the authtype	
124925	Warning	Deleting all active users	Deleting all active users	
124926	Warning	Deleting all dormant users	Deleting all dormant users	
124927	Warning	Auth module overload, Dropping new station request [mac:%s] Total drops: [total_drops:%u] Drops in last [interval:%d] seconds: [interval_drops:%d]	Auth module overload, Dropping new station request	
125011	Warning	Created a New Role [role_name:%s]	New management user role created	
125012	Warning	A permit entry is added to the role [role_name:%s]	Information indicating a permit entry has been added to the specified role	
125021	Warning	Authentication failed for User [user_name:%s], connection type SERIAL	Management user authentication from the console port failed	
125022	Warning	Authentication failed for User [user_name:%s], Logged in from [srcIp:%s] port [srcPort:%d], Connecting to [dstIp:%s] port [dstPort:%d] connection type [conn_type:%s]	Management user authentication failed	
125031	Warning	Authentication failed for User [user_name:%s], connection type is SSH	Management user authentication from the console port failed	

125033	Warning	Authentication failed for User [user_name:%s], Logged in from [srcIp:%s] port [srcPort:%d], Connecting to [dstIp:%s] port [dstPort:%d] connection type SSH	Management user authentication failed	
125060	Warning	User [user_name:%s] locked out on SERIAL port	Management user authentication failure threshold on serial port crossed the threshold.	
125061	Warning	User [user_name:%s] locked out, exceeded authentication threshold, Logged in from [srcIp:%s] port [srcPort:%d], Connecting to [dstIp:%s] port [dstPort:%d] connection type [conn_type:%s]	Management user authentication failure (on TELNET/SSH/WebUI) crossed the threshold.	
125071	Warning	Authentication Failed for User [user_name:%s], connection type [conn_type:%s]	SSH Public Key user authentication Failed	
125072	Warning	User [user_name:%s] locked out, exceeded authentication threshold, connection type [conn_type:%s]	SSH Public Key user authentication failure crossed the threshold.	
126005	Warning	Interfering AP: The system classified an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as interfering. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an access point has been classified as Interfering by the system. The access point is declared Interfering because it is not authorized, nor has it been classified as a Rogue.	This alert indicates an event that may affect your wireless infrastructure.
126006	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Impersonation: An AP detected AP impersonation of (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]), based of the number of beacons seen. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected AP Impersonation because the number of beacons seen has exceeded the expected number by the configured percentage threshold. The expected number is calculated based on the Beacon Interval Field in the Beacon frame. Detection is enabled via the 'Detect AP Impersonation' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
126007	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Multi-tenancy SSID Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is violating Valid SSID configuration by using a protected SSID.	This event indicates that an AP has detected an access point is violating Valid SSID configuration by using an SSID that is reserved for use by a valid AP only. Detection is enabled via the 'Detect Valid SSID Misuse' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126008	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Valid Channel Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is misconfigured because it is using a channel that is not valid.	This event indicates that an AP detected an access point that has a channel misconfiguration because it is using a channel that is not valid. Detection is enabled via the 'Detect Misconfigured AP' setting and the 'Valid 802.11a channel for policy enforcement' setting and the 'Valid 802.11g channel for policy enforcement' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126009	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Valid OUI Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is misconfigured because it is using an OUI that is not valid.	This event indicates that an AP detected an access point that has an OUI misconfiguration because it is using an OUI that is not valid. Detection is enabled via the 'Detect Misconfigured AP' setting and the 'Valid MAC OUIs' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126010	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Valid SSID Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is misconfigured because it is using an SSID that is not valid.	This event indicates that an AP detected an access point that has an SSID misconfiguration because it is using an SSID that is not valid. Detection is enabled via the 'Detect Misconfigured AP' setting and the 'Valid and Protected SSIDs' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126011	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Privacy Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has bad WEP configuration.	This event indicates that an AP detected an access point that is misconfigured because it does not have Privacy enabled. Detection is enabled via the 'Privacy' setting and the 'Detect Misconfigured AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.

126012	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Adhoc Containment Enforced: An AP is containing a node [IDS_EV_SOURCE_MAC:%m] that is part of the adhoc network (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR value is [IDS_EV_SNR:%d].	This event indicates that containment is being enforced on an ad hoc wireless network identified by the SRC MAC, BSSID and SSID shown. Detection is enabled via the 'Protect from Adhoc Networks' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126013	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Valid Station Protection Enforced: An AP is enforcing protection because a valid station ([IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is violating valid station policy.	This event indicates that Protection was enforced because a valid station's association to a non-valid access point violated Valid Station policy. Detection is enabled via the 'Protect Valid Stations' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect one or more clients of your wireless network.
126014	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): WEP Key Repeated: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with a Repeat WEP-IV violation. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid access point is using the same WEP initialization vector in consecutive packets. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126015	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): WEP Key Repeated: An AP detected a Repeat WEP-IV violation from a station (MAC [IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid station is using the same WEP initialization vector in consecutive packets. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126016	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Weak WEP Key: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with a Weak WEP-IV violation. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid access point is using a Weak WEP initialization vector. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126017	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Weak WEP Key: An AP detected a Weak WEP-IV violation from a station (MAC [IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid station is using a Weak WEP initialization vector. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126018	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Interference Detected: An AP detected interference for an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP has detected interference for an access point. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
126019	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Cleared Interference Detected: An AP detected that interference has cleared for an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that the previously detected interference for an access point is no longer present. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.

126020	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Interference Detected: An AP detected interference for a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP has detected interference for a station. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
126021	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Cleared Interference Detected: An AP detected that interference has cleared for a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that the previously detected interference for a station is no longer present. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
126022	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Retry Rate Exceeded: An AP detected that an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame retry rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Retry Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126023	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Receive Error Rate Exceeded: An AP detected that an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame receive error rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Receive Error Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126024	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Fragmentation Rate Exceeded: An AP detected that an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame fragmentation rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that an access point exceeded the configured upper threshold for Frame Fragmentation Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126025	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Bandwidth Rate Exceeded: An AP detected that a station or access point (MAC [IDS_EV_NODE_MAC:%m] with BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the allocated bandwidth rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a station or access point has exceeded the configured upper threshold for Bandwidth rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126026	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Low Speed Rate Exceeded: An AP detected that a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the low speed rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a station has exceeded the configured upper threshold for Low speed rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.

126027	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Non-unicast Rate Exceeded: An AP detected that a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the unicast traffic rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a station has exceeded the configured upper threshold for Non Unicast traffic rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126028	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): WPA Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has bad WPA configuration.	This event indicates that an AP detected an access point that is misconfigured because it is not using WPA. Detection is enabled via the 'Require WPA' setting and the 'Detect Misconfigured AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126029	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Invalid MAC OUI: An AP detected an invalid MAC OUI ([IDS_EV_TARGET_AP_BSSID:%m]) being used as the BSSID in a frame with SSID [IDS_EV_TARGET_AP_SSID:%s]. The Address Type in which the invalid MAC is used is [IDS_EV_ADDRESS_TYPE:%s], and SNR value is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an invalid MAC OUI in the BSSID of a frame. An invalid MAC OUI suggests that the frame may be spoofed. Detection is enabled via the 'Detect Devices with an Invalid MAC OUI' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126030	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Invalid MAC OUI: An AP detected an invalid MAC OUI ([IDS_EV_NODE_MAC:%m]) being used in a frame. The Address Type in which the invalid MAC is used is [IDS_EV_ADDRESS_TYPE:%s], and SNR value is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an invalid MAC OUI in the SRC or DST address of a frame. An invalid MAC OUI suggests that the frame may be spoofed. Detection is enabled via the 'Detect Devices with an Invalid MAC OUI' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126031	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: An AP detected a signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match in a frame. Detection is enabled via the 'IDS Signature' setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
126032	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): EAP Rate Anomaly: An AP received EAP handshake packets on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] at a rate which exceeds the configured IDS EAP handshake rate threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the rate of EAP Handshake packets received by an AP has exceeded the configured IDS EAP Handshake rate threshold. Detection is enabled via the 'Detect EAP Rate Anomaly' setting and the 'EAP Rate Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126033	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Adhoc Network: An AP detected an Adhoc network on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] where station [IDS_EV_SOURCE_MAC:%m] is connected to the Ad hoc AP (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]). SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network where a station is connected to an ad hoc access point. Detection is enabled via the 'Detect Adhoc Networks' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126034	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Flood Attack: An AP detected that the number of potential fake APs observed across all bands has exceeded the configured IDS threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the number of potential fake APs detected by an AP has exceeded the configured IDS threshold. This is the total number of fake APs observed across all bands. Detection is enabled via the 'Detect AP Flood Attack' setting and the 'AP Flood Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.

126035	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Disconnect Station Attack: An AP detected a disconnect attack of client [IDS_EV_SOURCE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has determined that a client is under Disconnect Attack because the rate of Assoc/Reassoc Response packets received by that client exceeds the configured threshold. Detection is enabled via the 'Detect Disconnect Station Attack' setting and the 'Disconnect STA Detection Theshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126036	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Wireless Bridge: An AP detected a wireless bridge between transmitter [IDS_EV_TRANSMITTER_MAC:%m] and receiver [IDS_EV_RECEIVER_MAC:%m]. SNR value is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a Wireless Bridge when a WDS frame was seen between the transmitter and receiver addresses. Detection is enabled via the 'Detect Wireless Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126037	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Station Associated to Rogue AP: An AP detected a client [IDS_EV_NODE_MAC:%m] associated to a rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AM detected a client associated with a Rogue access point. Detection is enabled via the 'Detect Station Association To Rogue AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
126038	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Cleared Station Associated to Rogue AP: An AP is no longer detecting a client [IDS_EV_NODE_MAC:%m] associated to a rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP that had previously detected a client association to a Rogue access point is no longer detecting that association. Detection is enabled via the 'Detect Station Association To Rogue AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
126039	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Adhoc Bridge: An AP detected an adhoc network bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]). SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network that is bridging to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126040	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Adhoc Bridge: An AP detected an adhoc network bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] between an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]) and a node [IDS_EV_SOURCE_MAC:%m]. SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network that is bridging to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126041	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Windows Bridge: An AP detected a bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m], SSID [IDS_EV_TARGET_AP_SSID:%s]).	This event indicates that an AP is detecting an access point that is bridging from a wireless network to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126042	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Windows Bridge: An AP detected a bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] between access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]) and a node [IDS_EV_SOURCE_MAC:%m].	This event indicates that an AP is detecting a station that is bridging from a wireless network to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.

126043	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: Netstumbler: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Netstumbler in a frame. Detection is enabled by referencing the predefined Netstumber signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
126044	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: ASLEAP: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for ASLEAP in a frame. Detection is enabled by referencing the predefined ASLEAP signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that affects one or more clients of your wireless network.
126045	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: Null Probe Response: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Null-Probe-Response in a frame. Detection is enabled by referencing the predefined Null-Probe-Response signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that affects one or more clients of your wireless network.
126046	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: AirJack: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Airjack in a frame. Detection is enabled by referencing the predefined AirJack signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that affects one or more clients of your wireless network.
126047	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: Deauth Broadcast: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Deauth-Broadcast in a frame. Detection is enabled by referencing the predefined Deauth-Broadcast signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
126048	Warning	Suspect Rogue AP: The system detected a suspected rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m], SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). The access point is suspected to be rogue with a confidence level of ([IDS_EV_CONF_LEVEL:%d]). Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an access point, classified as Suspected Rogue, is detected by the system. The AP is suspected to be rogue with the supplied confidence level.	This alert indicates an event that may affect your wireless infrastructure.

126049	Warning	Cleared Suspect Rogue AP: A previously classified suspected rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m], SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is no longer considered suspected rogue or it was removed from the network. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that a previously detected access point, classified as Suspected Rogue, is either no longer present in the network or has changed its state.	This alert indicates an event that may affect your wireless infrastructure.
126052	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): 802.11n 40MHZ Intolerance: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with HT 40MHz Intolerance Setting.	This event indicates that an AP is detecting an access point with the HT 40MHz intolerance setting. Detection is enabled via the 'Detect 802.11n 40MHz Intolerance' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126053	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): 802.11n 40MHZ Intolerance: An AP detected an HT 40MHZ Intolerance setting from a station ([IDS_EV_SOURCE_MAC:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. SNR is [IDS_EV_SNR:%d] and FrameType is [IDS_EV_FRAME_TYPE:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the system is detecting an HT 40MHz Intolerance setting from a Station. Detection is enabled via the 'Detect 802.11n 40MHz Intolerance' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126054	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): 802.11n Greenfield Mode AP: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with HT Greenfield support.	This event indicates that an AP detected an access point that supports HT Greenfield mode. Detection is enabled via the 'Detect Active 802.11n Greenfield Mode' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126055	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Retry Rate Exceeded: An AP detected that a station [IDS_EV_NODE_MAC:%m] associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame retry rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that a station exceeded the configured upper threshold for Frame Retry Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126056	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Retry Rate Exceeded on Channel: An AP detected that the configured threshold for frame retry rate was exceeded on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that the configured upper threshold for Frame Retry Rate was exceeded on a channel. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126057	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Receive Error Rate Exceeded: An AP detected that a station [IDS_EV_NODE_MAC:%m] associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_TARGET_AP_BAND:%s]) has exceeded the configured threshold for frame receive error rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that a station exceeded the configured upper threshold for Frame Receive Error Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126058	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Receive Error Rate Exceeded on Channel: An AP detected that the configured threshold for frame receive error rate was exceeded on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that the configured upper threshold for Frame Receive Error Rate was exceeded on a channel. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.

126059	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Fragmentation Rate Exceeded: An AP detected that a station [IDS_EV_NODE_MAC:%m] associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame fragmentation rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that a station exceeded the configured upper threshold for Frame Fragmentation Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126060	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Frame Fragmentation Rate Exceeded on Channel: An AP detected that the configured threshold for frame fragmentation rate was exceeded on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that the configured upper threshold for Frame Fragmentation Rate was exceeded on a channel. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
126061	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Channel Rate Anomaly: An AP detected frames of type [IDS_EV_FRAME_TYPE:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] which exceed the configured IDS rate Threshold for this frame type. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected frames on a channel which exceed the configured IDS rate threshold. Detection is enabled via the 'Detect Rate Anomalies' setting and the 'Rate Thresholds for [frame subtype]' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126062	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Node Rate Anomaly: An AP detected frames of type [IDS_EV_FRAME_TYPE:%s] transmitted or received by an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]), which exceed the configured IDS rate threshold for this frame type. SNR for AP is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected frames transmitted or received by an access point, which exceed the configured IDS rate threshold. Detection is enabled via the 'Detect Rate Anomalies' setting and the 'Rate Thresholds for [frame subtype]' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126063	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Node Rate Anomaly: An AP detected frames of type [IDS_EV_FRAME_TYPE:%s] transmitted or received by a station [IDS_EV_NODE_MAC:%m], which exceed the configured IDS rate threshold for this frame type. SNR for station is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected frames transmitted or received by a node, which exceed the configured IDS rate threshold. Detection is enabled via the 'Detect Rate Anomalies' setting and the 'Rate Thresholds for [frame subtype]' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126064	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Client Flood Attack: An AP detected that the number of potential fake clients observed across all bands has exceeded the configured IDS threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the number of potential fake clients detected by an AP has exceeded the configured IDS threshold. This is the total number of fake clients observed across all bands. Detection is enabled via the 'Detect Client Flood Attack' setting and the 'Client Flood Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126065	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Valid Client Not Using Encryption: An AP detected an unencrypted frame between a valid client ([IDS_EV_NODE_MAC:%m]) and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]), with source [IDS_EV_SOURCE_MAC:%m] and receiver [IDS_EV_RECEIVER_MAC:%m]. SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an unencrypted data frame between a valid client and an access point. Detection is enabled via the 'Detect Unencrypted Valid Clients' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
126066	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: Disassoc Broadcast: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Disassoc-Broadcast in a frame. Detection is enabled by referencing the predefined Disassoc-Broadcast signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.

126067	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Signature Match: Wellenreiter: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Wellenreiter in a frame. Detection is enabled by referencing the predefined Wellenreiter signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
126068	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Adhoc Network Using Valid SSID: An AP detected an adhoc node [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) using a valid/protected SSID. SNR is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network node using a valid/protected SSID. Detection is enabled via the 'Detect Adhoc Network Using Valid SSID' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126069	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Spoofing: An AP detected a frame that has a spoofed source address of [IDS_EV_SOURCE_MAC:%m], a BSSID of [IDS_EV_TARGET_AP_BSSID:%m], a destination address of [IDS_EV_RECEIVER_MAC:%m], and is on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. SNR is [IDS_EV_SNR:%d], and FrameType is [IDS_EV_SPOOFED_FRAME_TYPE:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that one of its virtual APs is being spoofed using MAC spoofing. Detection is enabled via the 'Detect AP Spoofing' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
126070	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Spoofing: An AP detected a frame from [IDS_EV_SOURCE_MAC:%m] addressed to one of its BSSIDs [IDS_EV_TARGET_AP_BSSID:%m] on the wrong CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Destination address is [IDS_EV_RECEIVER_MAC:%m], SNR is [IDS_EV_SNR:%d], and FrameType is [IDS_EV_SPOOFED_FRAME_TYPE:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a client trying to associate to one of its BSSIDs on the wrong channel. This can be a sign that the BSSID is being spoofed in order to fool the client into thinking the AP is operating on another channel. Detection is enabled via the 'Detect AP Spoofing' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
126071	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Omerta Attack: An AP detected an Omerta attack on client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an Omerta attack. Detection is enabled via the 'Detect Omerta Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126072	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): FATA-Jack Attack: An AP detected a FATA-Jack attack on client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of frame is [IDS_EV_SNR:%d].	This event indicates that an AP detected a FATA-Jack attack. Detection is enabled via the 'Detect FATA-Jack Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126073	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): CTS Rate Anomaly: An AP received CTS packets on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] at a rate which exceeds the configured IDS CTS rate threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the rate of CTS packets received by an AP exceeds the configured IDS threshold. Detection is enabled via the 'Detect CTS Rate Anomaly' setting and the 'CTS Rate Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.

126074	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): RTS Rate Anomaly: An AP received RTS packets on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] at a rate which exceeds the configured IDS RTS rate threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the rate of RTS packets received by an AP exceeds the configured IDS threshold. Detection is enabled via the 'Detect RTS Rate Anomaly' setting and the 'RTS Rate Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126075	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Valid Client Misassociation: An AP detected a misassociation between valid client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). Association type is ([IDS_EV_ASSOCIATION_TYPE:%s]), SNR of client is [IDS_EV_SNR:%d].	This event indicates that an AP detected a misassociation between a valid client and an unsafe AP. Detection is enabled via the 'Detect Valid Client Misassociation' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
126076	Warning	Neighbor AP: The system classified an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) as a neighbor. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an access point has been classified as a Neighbor by the system.	This alert indicates an event that may affect your wireless infrastructure.
126077	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): TKIP Replay Attack: An AP detected a possible TKIP replay against station [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] with SNR [IDS_EV_SNR:%d] and BAND [IDS_EV_AP_BAND:%s]). This may disrupt communication with [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a possible TKIP replay attack. If successful this could be the precursor to more advanced attacks. Detection is enabled via the 'Detect TKIP Replay Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126078	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): ChopChop Attack: An AP detected a ChopChop attack against station [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]). This could reveal the WEP key.	This event indicates that an AP detected a ChopChop attack. Detection is enabled via the 'Detect ChopChop Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126079	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Invalid Address Combination: An AP detected a frame with an invalid source address [IDS_EV_SOURCE_MAC:%m]. This could be an attempt to get the receiver [IDS_EV_RECEIVER_MAC:%m] to reply with a multicast or broadcast frame. Frame received on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with a SNR of [IDS_EV_SNR:%d].	This event indicates that an AP detected an invalid source and destination combination. Detection is enabled via the 'Detect Invalid Address Combination' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126080	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Malformed Frame - Assoc Request: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent an association request containing an empty SSID. If [IDS_EV_RECEIVER_MAC:%m] uses a vulnerable wireless driver this could cause it to crash.	This event indicates that an AP detected a malformed association request with a NULL SSID. Detection is enabled via the 'Detect Malformed Frame - Assoc Request' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.

126081	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Malformed Frame - HT IE: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a management frame containing one or more malformed HT Information Elements. This may disrupt communication with [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a malformed HT Information Element. This can be the result of a misbehaving wireless driver or it may be an indication of a new wireless attack. Detection is enabled via the 'Detect Malformed Frame - HT IE' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126082	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Overflow EAPOL Key: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a malformed EAPOL Key message with a declared length that is too large. This could disrupt or crash the device with address [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a key in an EAPOL Key message with a specified length greater than the length of the entire message. Detection is enabled via the 'Detect Overflow EAPOL Key' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126083	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Malformed Frame - Auth: An AP detected a malformed authentication frame from client [IDS_EV_NODE_MAC:%m] to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of frame is [IDS_EV_SNR:%d].	This event indicates that an AP detected an authentication frame with either a bad algorithm (similar to Fata-Jack) or a bad transaction. Detection is enabled via the 'Detect Malformed Frame - Auth' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126084	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Overflow IE: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a malformed information element with a declared length that is too large. This could disrupt or crash the device with address [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a management frame with a malformed information element. The declared length of the element is larger than the entire frame containing the element. This may be used to corrupt or crash wireless drivers. Detection is enabled via the 'Detect Overflow IE' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126085	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Malformed Frame - Large Duration: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a frame with an unusually large duration. This could be an attempt to deny service to all devices on this channel. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an unusually large duration in a wireless frame. This may be an attempt to block other devices from transmitting. Detection is enabled via the 'Detect Malformed Frame - Large Duration' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126086	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Beacon Frame with Incorrect Channel: An AP detected that the Access Point with MAC [IDS_EV_SOURCE_MAC:%m] and BSSID [IDS_EV_TARGET_AP_BSSID:%m] has sent a beacon for SSID [IDS_EV_TARGET_AP_SSID:%s]. This beacon advertizes CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] but was received on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_TARGET_AP_BAND:%s] with SNR [IDS_EV_SNR:%d].	This event indicates that an AP detected a beacon on one channel advertising another channel. This could be an attempt to lure clients away from a valid AP. Detection is enabled via the 'Detect Beacon on Wrong Channel' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.

126087	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Block ACK DoS Attack: An AP detected a data frame which indicates a possible Block ACK DoS Attack. The frame from [IDS_EV_SOURCE_MAC:%m] to [IDS_EV_RECEIVER_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) is outside the current sequence number window, and thus may be dropped. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an attempt has been made to deny service to the source address by spoofing a block ACK add request that sets a sequence number window outside the currently used window. Detection is enabled via the 'Detect Block ACK DoS' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126088	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Hotspotter Attack: An AP detected that the client with MAC address [IDS_EV_NODE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) may be under attack from the Hotspotter tool. The probe response was sent from AP [IDS_EV_SOURCE_MAC:%m] for SSID [IDS_EV_TARGET_AP_SSID:%s].	This event indicates that a new AP has appeared immediately following a client probe request. This is indicative of the Hotspotter tool or similar that attempts to event clients with a fake hotspot or other wireless network. Detection is enabled via the 'Detect Hotspotter Attack' setting in the IDS Impersonation profile.	This alert indicates an event that affects one or more clients of your wireless network.
126102	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Deauth Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disconnecting its client (MAC [IDS_EV_NODE_MAC:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s].	This event indicates that an AP has attempted to contain an access point by disconnecting its client. Detection is enabled via the 'Wireless Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126103	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Client Deauth Containment: An AP attempted to contain a client (MAC [IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s].	This event indicates that an AP has attempted to contain a client by disconnecting it from the AP that it is associated with. Detection is enabled via the 'Wireless Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126104	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Wired Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disconnecting client (MAC [IDS_EV_NODE_MAC:%m]) by disrupting device with IPv4 [IDS_EV_DEVICE_IP:%pI4] IPv6 [IDS_EV_DEVICE_IPV6:%s] and MAC [IDS_EV_DEVICE_MAC:%m].	This event indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126105	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Client Wired Containment: An AP attempted to contain a client (MAC [IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disrupting device with IPv4 [IDS_EV_DEVICE_IP:%pI4] and/or IPv6 [IDS_EV_DEVICE_IPV6:%s] and MAC [IDS_EV_DEVICE_MAC:%m].	This event indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126106	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): AP Tagged Wired Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disconnecting client (MAC [IDS_EV_NODE_MAC:%m]) by disrupting device with IPv4 [IDS_EV_DEVICE_IP:%pI4] and/or IPv6 [IDS_EV_DEVICE_IPV6:%s]and MAC [IDS_EV_DEVICE_MAC:%m] on VLAN [IDS_EV_VLAN_ID:%d].	This event indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126107	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Client Tagged Wired Containment: An AP attempted to contain a client (MAC [IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disrupting device with IP [IDS_EV_DEVICE_IP:%pI4] and/or IPv6 [IDS_EV_DEVICE_IPV6:%s] and MAC [IDS_EV_DEVICE_MAC:%m] on VLAN [IDS_EV_VLAN_ID:%d].	This event indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.

126108	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Tarpit Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] by tarpitting client (MAC [IDS_EV_NODE_MAC:%m]) by sending it tarpit on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] (BAND [IDS_EV_TARGET_AP_BAND:%s]) and fake BSSID [IDS_EV_SOURCE_MAC:%m].	This event indicates that an AP has attempted to contain an access point by moving a client that is attempting to associate to it to a tarpit. Detection is enabled via the 'Wireless Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126109	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Power Save DoS Attack: An AP detected a Power Save DoS attack on client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a Power Save DoS attack. Detection is enabled via the 'Detect Power Save DoS Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126110	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Wireless Hosted Network: An AP detected a wireless client [IDS_EV_NODE_MAC:%m] that is hosting an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]).Classification of client is [IDS_EV_TRAP_CLIENT_CLASS:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a wireless client that is hosting a softAP. The softAP could be used to share the hosting client's wired or wireless network connection with other wireless users. Detection is enabled via the 'Detect Wireless Hosted Network' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126111	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Client Associated To Hosted Network: An AP detected a client [IDS_EV_NODE_MAC:%m] associated to a hosted access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d].	This event indicates that an AP detected that a wireless client associated to an access point that is hosted by another wireless client. Detection is enabled via the 'Detect Wireless Hosted Network' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
126112	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Wireless Hosted Network Containment: An AP attempted to contain a client [IDS_EV_NODE_MAC:%m] that is associated to the hosted network (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d].	This event indicates that containment is being enforced on a client associated to a hosted network. Detection is enabled via the 'Protect from Wireless Hosted Networks' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126113	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Host of Wireless Network Containment: An AP attempted to contain a client [IDS_EV_NODE_MAC:%m] that is associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). The client is hosting the wireless hosted network [IDS_EV_TRAP_AP_BSSID:%m]. SNR of client is [IDS_EV_SNR:%d].	This event indicates that containment is being enforced on a client that is hosting a wireless hosted network. Detection is enabled via the 'Protect from Wireless Hosted Networks' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126114	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Enhanced Adhoc Containment: An AP attempted to contain an adhoc node [IDS_EV_NODE_MAC:%m] that is part of the adhoc network (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP has attempted to contain an adhoc node by disconnecting it from other members of the adhoc network. Detection is enabled via the 'Protect from Adhoc Networks - Enhanced' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.

126115	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Adhoc Network Using Valid SSID Containment: An AP attempted to contain an adhoc node [IDS_EV_NODE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d]) using a valid/protected SSID. SNR is [IDS_EV_SNR:%d]. BAND is [IDS_EV_AP_BAND:%s].	This event indicates that containment is being enforced on an ad hoc wireless network node using a valid/protected SSID. Detection is enabled via the 'Protect from Adhoc Networks Using Valid SSID' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
126116	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): WPA FT Attack: An AP detected a possible attack of the Fast BSS Transition for CLIENT [IDS_EV_NODE_MAC:%m] on BSSID [IDS_EV_TARGET_AP_BSSID:%m] and CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates there is a possible attack of the Fast BSS Transition causing a WPA key re-installation. This can be indicative of a security breach where an attacker can hijack a client's association and/or decrypt an otherwise secure connection. Detection is enabled via the 'Detect WPA FT Attack' setting and the 'WPA FT Attack Detection Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
126117	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Man in the Middle Attack: An AP detected a possible channel-based Man in the Middle attack. Spoofed beacon frame has source address of [IDS_EV_SOURCE_MAC:%m], a BSSID of [IDS_EV_TARGET_AP_BSSID:%m], announcing a channel switch to CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. SNR is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a possible channel-based Man in the Middle attack by someone using spoofed beacons with an invalid Channel Switch Announcement. Detection is enabled via the 'Detect Man in the Middle' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
126118	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): Phony BSSID Detection: An AP detected a phony BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] belonging to AP (NAME [IDS_EV_TARGET_AP_NAME:%s] and MAC [IDS_EV_TARGET_AP_MAC:%m]). Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a non-configured BSSID that should belong to one of our known valid APs. Detection is enabled via the 'Detect Phony BSSID' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
126119	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): GHOST TUNNEL Attack: An AP detected a possible attack of the Ghost Tunnel Server. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates there is a possible attack of the Ghost Tunnel. This can be airgap atttack only by beacon and probe request where an attacker can hijack a client. Detection is enabled via the 'Detect GHOST TUNNEL SERVER' setting and the 'GHOST TUNNEL Attack Detection Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
126120	Warning	AP([RADIO_MAC:%m]@[NAME:%s]): GHOST TUNNEL Attack: An AP detected a possible attack of the Ghost Tunnel CLIENT. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates there is a possible attack of the Ghost Tunnel. This can be airgap atttack only by beacon and probe request where an attacker can hijack a client. Detection is enabled via the 'Detect GHOST TUNNEL CLIENT' setting and the 'GHOST TUNNEL Attack Detection Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127006	Warning	AP([RADIO_MAC:%m]): AP Impersonation: An AP detected AP impersonation of (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]), based of the number of beacons seen. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected AP Impersonation because the number of beacons seen has exceeded the expected number by the configured percentage threshold. The expected number is calculated based on the Beacon Interval Field in the Beacon frame. Detection is enabled via the 'Detect AP Impersonation' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
127007	Warning	AP([RADIO_MAC:%m]): Multi-tenancy SSID Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is violating Valid SSID configuration by using a protected SSID.	This event indicates that an AP has detected an access point is violating Valid SSID configuration by using an SSID that is reserved for use by a valid AP only. Detection is enabled via the 'Detect Valid SSID Misuse' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.

127008	Warning	AP([RADIO_MAC:%m]): Valid Channel Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is misconfigured because it is using a channel that is not valid.	This event indicates that an AP detected an access point that has a channel misconfiguration because it is using a channel that is not valid. Detection is enabled via the 'Detect Misconfigured AP' setting and the 'Valid 802.11a channel for policy enforcement' setting and the 'Valid 802.11g channel for policy enforcement' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127009	Warning	AP([RADIO_MAC:%m]): Valid OUI Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is misconfigured because it is using an OUI that is not valid.	This event indicates that an AP detected an access point that has an OUI misconfiguration because it is using an OUI that is not valid. Detection is enabled via the 'Detect Misconfigured AP' setting and the 'Valid MAC OUIs' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127010	Warning	AP([RADIO_MAC:%m]): Valid SSID Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is misconfigured because it is using an SSID that is not valid.	This event indicates that an AP detected an access point that has an SSID misconfiguration because it is using an SSID that is not valid. Detection is enabled via the 'Detect Misconfigured AP' setting and the 'Valid and Protected SSIDs' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127011	Warning	AP([RADIO_MAC:%m]): Privacy Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has bad WEP configuration.	This event indicates that an AP detected an access point that is misconfigured because it does not have Privacy enabled. Detection is enabled via the 'Privacy' setting and the 'Detect Misconfigured AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127012	Warning	AP([RADIO_MAC:%m]): Adhoc Containment Enforced: An AP is containing a node [IDS_EV_SOURCE_MAC:%m] that is part of the adhoc network (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR value is [IDS_EV_SNR:%d].	This event indicates that containment is being enforced on an ad hoc wireless network identified by the SRC MAC, BSSID and SSID shown. Detection is enabled via the 'Protect from Adhoc Networks' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127013	Warning	AP([RADIO_MAC:%m]): Valid Station Protection Enforced: An AP is enforcing protection because a valid station ([IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) is violating valid station policy.	This event indicates that Protection was enforced because a valid station's association to a non-valid access point violated Valid Station policy. Detection is enabled via the 'Protect Valid Stations' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect one or more clients of your wireless network.
127014	Warning	AP([RADIO_MAC:%m]): WEP Key Repeated: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with a Repeat WEP-IV violation. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid access point is using the same WEP initialization vector in consecutive packets. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127015	Warning	AP([RADIO_MAC:%m]): WEP Key Repeated: An AP detected a Repeat WEP-IV violation from a station (MAC [IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid station is using the same WEP initialization vector in consecutive packets. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127016	Warning	AP([RADIO_MAC:%m]): Weak WEP Key: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with a Weak WEP-IV violation. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid access point is using a Weak WEP initialization vector. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.

127017	Warning	AP([RADIO_MAC:%m]): Weak WEP Key: An AP detected a Weak WEP-IV violation from a station (MAC [IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a valid station is using a Weak WEP initialization vector. Detection is enabled via the 'Detect Bad WEP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127018	Warning	AP([RADIO_MAC:%m]): Interference Detected: An AP detected interference for an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP has detected interference for an access point. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
127019	Warning	AP([RADIO_MAC:%m]): Cleared Interference Detected: An AP detected that interference has cleared for an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that the previously detected interference for an access point is no longer present. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
127020	Warning	AP([RADIO_MAC:%m]): Interference Detected: An AP detected interference for a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP has detected interference for a station. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
127021	Warning	AP([RADIO_MAC:%m]): Cleared Interference Detected: An AP detected that interference has cleared for a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that the previously detected interference for a station is no longer present. Detection is enabled via the 'Detect interference' setting in the RF Optimization profile.	This alert indicates an event that may affect your wireless infrastructure.
127022	Warning	AP([RADIO_MAC:%m]): Frame Retry Rate Exceeded: An AP detected that an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame retry rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Retry Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127023	Warning	AP([RADIO_MAC:%m]): Frame Receive Error Rate Exceeded: An AP detected that an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame receive error rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Receive Error Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127024	Warning	AP([RADIO_MAC:%m]): Frame Fragmentation Rate Exceeded: An AP detected that an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame fragmentation rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that an access point exceeded the configured upper threshold for Frame Fragmentation Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.

127025	Warning	AP([RADIO_MAC:%m]): Frame Bandwidth Rate Exceeded: An AP detected that a station or access point (MAC [IDS_EV_NODE_MAC:%m] with BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the allocated bandwidth rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a station or access point has exceeded the configured upper threshold for Bandwidth rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127026	Warning	AP([RADIO_MAC:%m]): Frame Low Speed Rate Exceeded: An AP detected that a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the low speed rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a station has exceeded the configured upper threshold for Low speed rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127027	Warning	AP([RADIO_MAC:%m]): Frame Non-unicast Rate Exceeded: An AP detected that a station ([IDS_EV_NODE_MAC:%m]) associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the unicast traffic rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that a station has exceeded the configured upper threshold for Non Unicast traffic rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127028	Warning	AP([RADIO_MAC:%m]): WPA Violation: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has bad WPA configuration.	This event indicates that an AP detected an access point that is misconfigured because it is not using WPA. Detection is enabled via the 'Require WPA' setting and the 'Detect Misconfigured AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127029	Warning	AP([RADIO_MAC:%m]): Invalid MAC OUI: An AP detected an invalid MAC OUI ([IDS_EV_TARGET_AP_BSSID:%m]) being used as the BSSID in a frame with SSID [IDS_EV_TARGET_AP_SSID:%s]. The Address Type in which the invalid MAC is used is [IDS_EV_ADDRESS_TYPE:%s], and SNR value is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an invalid MAC OUI in the BSSID of a frame. An invalid MAC OUI suggests that the frame may be spoofed. Detection is enabled via the 'Detect Devices with an Invalid MAC OUI' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127030	Warning	AP([RADIO_MAC:%m]): Invalid MAC OUI: An AP detected an invalid MAC OUI ([IDS_EV_NODE_MAC:%m]) being used in a frame. The Address Type in which the invalid MAC is used is [IDS_EV_ADDRESS_TYPE:%s], and SNR value is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an invalid MAC OUI in the SRC or DST address of a frame. An invalid MAC OUI suggests that the frame may be spoofed. Detection is enabled via the 'Detect Devices with an Invalid MAC OUI' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127031	Warning	AP([RADIO_MAC:%m]): Signature Match: An AP detected a signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match in a frame. Detection is enabled via the 'IDS Signature' setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
127032	Warning	AP([RADIO_MAC:%m]): EAP Rate Anomaly: An AP received EAP handshake packets on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] at a rate which exceeds the configured IDS EAP handshake rate threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the rate of EAP Handshake packets received by an AP has exceeded the configured IDS EAP Handshake rate threshold. Detection is enabled via the 'Detect EAP Rate Anomaly' setting and the 'EAP Rate Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.

127033	Warning	AP([RADIO_MAC:%m]): Adhoc Network: An AP detected an Adhoc network on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] where station [IDS_EV_SOURCE_MAC:%m] is connected to the Ad hoc AP (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]). SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network where a station is connected to an ad hoc access point. Detection is enabled via the 'Detect Adhoc Networks' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127034	Warning	AP([RADIO_MAC:%m]): AP Flood Attack: An AP detected that the number of potential fake APs observed across all bands has exceeded the configured IDS threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the number of potential fake APs detected by an AP has exceeded the configured IDS threshold. This is the total number of fake APs observed across all bands. Detection is enabled via the 'Detect AP Flood Attack' setting and the 'AP Flood Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127035	Warning	AP([RADIO_MAC:%m]): Disconnect Station Attack: An AP detected a disconnect attack of client [IDS_EV_SOURCE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has determined that a client is under Disconnect Attack because the rate of Assoc/Reassoc Response packets received by that client exceeds the configured threshold. Detection is enabled via the 'Detect Disconnect Station Attack' setting and the 'Disconnect STA Detection Theshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127036	Warning	AP([RADIO_MAC:%m]): Wireless Bridge: An AP detected a wireless bridge between transmitter [IDS_EV_TRANSMITTER_MAC:%m] and receiver [IDS_EV_RECEIVER_MAC:%m]. SNR value is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a Wireless Bridge when a WDS frame was seen between the transmitter and receiver addresses. Detection is enabled via the 'Detect Wireless Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127037	Warning	AP([RADIO_MAC:%m]): Station Associated to Rogue AP: An AP detected a client [IDS_EV_NODE_MAC:%m] associated to a rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AM detected a client associated with a Rogue access point. Detection is enabled via the 'Detect Station Association To Rogue AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
127038	Warning	AP([RADIO_MAC:%m]): Cleared Station Associated to Rogue AP: An AP is no longer detecting a client [IDS_EV_NODE_MAC:%m] associated to a rogue access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP that had previously detected a client association to a Rogue access point is no longer detecting that association. Detection is enabled via the 'Detect Station Association To Rogue AP' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
127039	Warning	AP([RADIO_MAC:%m]): Adhoc Bridge: An AP detected an adhoc network bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]). SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network that is bridging to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127040	Warning	AP([RADIO_MAC:%m]): Adhoc Bridge: An AP detected an adhoc network bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] between an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]) and a node [IDS_EV_SOURCE_MAC:%m]. SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network that is bridging to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127041	Warning	AP([RADIO_MAC:%m]): Windows Bridge: An AP detected a bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m], SSID [IDS_EV_TARGET_AP_SSID:%s]).	This event indicates that an AP is detecting an access point that is bridging from a wireless network to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.

127042	Warning	AP([RADIO_MAC:%m]): Windows Bridge: An AP detected a bridge on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] between access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]) and a node [IDS_EV_SOURCE_MAC:%m].	This event indicates that an AP is detecting a station that is bridging from a wireless network to a wired network. Detection is enabled via the 'Detect Windows Bridge' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127043	Warning	AP([RADIO_MAC:%m]): Signature Match: Netstumbler: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Netstumbler in a frame. Detection is enabled by referencing the predefined Netstumber signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
127044	Warning	AP([RADIO_MAC:%m]): Signature Match: ASLEAP: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for ASLEAP in a frame. Detection is enabled by referencing the predefined ASLEAP signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that affects one or more clients of your wireless network.
127045	Warning	AP([RADIO_MAC:%m]): Signature Match: Null Probe Response: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Null-Probe-Response in a frame. Detection is enabled by referencing the predefined Null-Probe-Response signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that affects one or more clients of your wireless network.
127046	Warning	AP([RADIO_MAC:%m]): Signature Match: AirJack: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Airjack in a frame. Detection is enabled by referencing the predefined AirJack signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that affects one or more clients of your wireless network.
127047	Warning	AP([RADIO_MAC:%m]): Signature Match: Deauth Broadcast: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Deauth-Broadcast in a frame. Detection is enabled by referencing the predefined Deauth-Broadcast signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
127052	Warning	AP([RADIO_MAC:%m]): 802.11n 40MHZ Intolerance: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with HT 40MHz Intolerance Setting.	This event indicates that an AP is detecting an access point with the HT 40MHz intolerance setting. Detection is enabled via the 'Detect 802.11n 40MHz Intolerance' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.

127053	Warning	AP([RADIO_MAC:%m]): 802.11n 40MHZ Intolerance: An AP detected an HT 40MHZ Intolerance setting from a station ([IDS_EV_SOURCE_MAC:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. SNR is [IDS_EV_SNR:%d] and FrameType is [IDS_EV_FRAME_TYPE:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the system is detecting an HT 40MHz Intolerance setting from a Station. Detection is enabled via the 'Detect 802.11n 40MHz Intolerance' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127054	Warning	AP([RADIO_MAC:%m]): 802.11n Greenfield Mode AP: An AP detected an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) with HT Greenfield support.	This event indicates that an AP detected an access point that supports HT Greenfield mode. Detection is enabled via the 'Detect Active 802.11n Greenfield Mode' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127055	Warning	AP([RADIO_MAC:%m]): Frame Retry Rate Exceeded: An AP detected that a station [IDS_EV_NODE_MAC:%m] associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame retry rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that a station exceeded the configured upper threshold for Frame Retry Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127056	Warning	AP([RADIO_MAC:%m]): Frame Retry Rate Exceeded on Channel: An AP detected that the configured threshold for frame retry rate was exceeded on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that the configured upper threshold for Frame Retry Rate was exceeded on a channel. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127057	Warning	AP([RADIO_MAC:%m]): Frame Receive Error Rate Exceeded: An AP detected that a station [IDS_EV_NODE_MAC:%m] associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_TARGET_AP_BAND:%s]) has exceeded the configured threshold for frame receive error rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that a station exceeded the configured upper threshold for Frame Receive Error Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127058	Warning	AP([RADIO_MAC:%m]): Frame Receive Error Rate Exceeded on Channel: An AP detected that the configured threshold for frame receive error rate was exceeded on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that the configured upper threshold for Frame Receive Error Rate was exceeded on a channel. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127059	Warning	AP([RADIO_MAC:%m]): Frame Fragmentation Rate Exceeded: An AP detected that a station [IDS_EV_NODE_MAC:%m] associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) has exceeded the configured threshold for frame fragmentation rate. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that a station exceeded the configured upper threshold for Frame Fragmentation Rate. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.
127060	Warning	AP([RADIO_MAC:%m]): Frame Fragmentation Rate Exceeded on Channel: An AP detected that the configured threshold for frame fragmentation rate was exceeded on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP has detected that the configured upper threshold for Frame Fragmentation Rate was exceeded on a channel. Detection is enabled via the 'Detect Frame Rate Anomalies' setting in the RF Event Thresholds profile.	This alert indicates an event that may affect your wireless infrastructure.

127061	Warning	AP([RADIO_MAC:%m]): Channel Rate Anomaly: An AP detected frames of type [IDS_EV_FRAME_TYPE:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] which exceed the configured IDS rate Threshold for this frame type. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected frames on a channel which exceed the configured IDS rate threshold. Detection is enabled via the 'Detect Rate Anomalies' setting and the 'Rate Thresholds for [frame subtype]' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127062	Warning	AP([RADIO_MAC:%m]): Node Rate Anomaly: An AP detected frames of type [IDS_EV_FRAME_TYPE:%s] transmitted or received by an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s]), which exceed the configured IDS rate threshold for this frame type. SNR for AP is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected frames transmitted or received by an access point, which exceed the configured IDS rate threshold. Detection is enabled via the 'Detect Rate Anomalies' setting and the 'Rate Thresholds for [frame subtype]' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127063	Warning	AP([RADIO_MAC:%m]): Node Rate Anomaly: An AP detected frames of type [IDS_EV_FRAME_TYPE:%s] transmitted or received by a station [IDS_EV_NODE_MAC:%m], which exceed the configured IDS rate threshold for this frame type. SNR for station is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected frames transmitted or received by a node, which exceed the configured IDS rate threshold. Detection is enabled via the 'Detect Rate Anomalies' setting and the 'Rate Thresholds for [frame subtype]' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127064	Warning	AP([RADIO_MAC:%m]): Client Flood Attack: An AP detected that the number of potential fake clients observed across all bands has exceeded the configured IDS threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the number of potential fake clients detected by an AP has exceeded the configured IDS threshold. This is the total number of fake clients observed across all bands. Detection is enabled via the 'Detect Client Flood Attack' setting and the 'Client Flood Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127065	Warning	AP([RADIO_MAC:%m]): Valid Client Not Using Encryption: An AP detected an unencrypted frame between a valid client ([IDS_EV_NODE_MAC:%m]) and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]), with source [IDS_EV_SOURCE_MAC:%m] and receiver [IDS_EV_RECEIVER_MAC:%m]. SNR value is [IDS_EV_SNR:%d].	This event indicates that an AP detected an unencrypted data frame between a valid client and an access point. Detection is enabled via the 'Detect Unencrypted Valid Clients' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
127066	Warning	AP([RADIO_MAC:%m]): Signature Match: Disassoc Broadcast: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Disassoc-Broadcast in a frame. Detection is enabled by referencing the predefined Disassoc-Broadcast signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
127067	Warning	AP([RADIO_MAC:%m]): Signature Match: Wellenreiter: An AP detected a factory default signature match ([IDS_EV_SIGNATURE_NAME:%s]) in a frame with BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] from transmitter [IDS_EV_TRANSMITTER_MAC:%m] to receiver [IDS_EV_RECEIVER_MAC:%m], with SNR [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a signature match for Wellenreiter in a frame. Detection is enabled by referencing the predefined Wellenreiter signature instance using the IDS Signature setting in the IDS Signature Matching profile.	This alert indicates an event that may affect your wireless infrastructure.
127068	Warning	AP([RADIO_MAC:%m]): Adhoc Network Using Valid SSID: An AP detected an adhoc node [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]) using a valid/protected SSID. SNR is [IDS_EV_SNR:%d].	This event indicates that an AP detected an ad hoc network node using a valid/protected SSID. Detection is enabled via the 'Detect Adhoc Network Using Valid SSID' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.

127069	Warning	AP([RADIO_MAC:%m]): AP Spoofing: An AP detected a frame that has a spoofed source address of [IDS_EV_SOURCE_MAC:%m], a BSSID of [IDS_EV_TARGET_AP_BSSID:%m], a destination address of [IDS_EV_RECEIVER_MAC:%m], and is on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. SNR is [IDS_EV_SNR:%d], and FrameType is [IDS_EV_SPOOFED_FRAME_TYPE:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected that one of its virtual APs is being spoofed using MAC spoofing. Detection is enabled via the 'Detect AP Spoofing' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
127070	Warning	AP([RADIO_MAC:%m]): AP Spoofing: An AP detected a frame from [IDS_EV_SOURCE_MAC:%m] addressed to one of its BSSIDs [IDS_EV_TARGET_AP_BSSID:%m] on the wrong CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Destination address is [IDS_EV_RECEIVER_MAC:%m], SNR is [IDS_EV_SNR:%d], and FrameType is [IDS_EV_SPOOFED_FRAME_TYPE:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a client trying to associate to one of its BSSIDs on the wrong channel. This can be a sign that the BSSID is being spoofed in order to fool the client into thinking the AP is operating on another channel. Detection is enabled via the 'Detect AP Spoofing' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
127071	Warning	AP([RADIO_MAC:%m]): Omerta Attack: An AP detected an Omerta attack on client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an Omerta attack. Detection is enabled via the 'Detect Omerta Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127072	Warning	AP([RADIO_MAC:%m]): FATA-Jack Attack: An AP detected a FATA-Jack attack on client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of frame is [IDS_EV_SNR:%d].	This event indicates that an AP detected a FATA-Jack attack. Detection is enabled via the 'Detect FATA-Jack Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127073	Warning	AP([RADIO_MAC:%m]): CTS Rate Anomaly: An AP received CTS packets on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] at a rate which exceeds the configured IDS CTS rate threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the rate of CTS packets received by an AP exceeds the configured IDS threshold. Detection is enabled via the 'Detect CTS Rate Anomaly' setting and the 'CTS Rate Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127074	Warning	AP([RADIO_MAC:%m]): RTS Rate Anomaly: An AP received RTS packets on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] at a rate which exceeds the configured IDS RTS rate threshold. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that the rate of RTS packets received by an AP exceeds the configured IDS threshold. Detection is enabled via the 'Detect RTS Rate Anomaly' setting and the 'RTS Rate Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127075	Warning	AP([RADIO_MAC:%m]): Valid Client Misassociation: An AP detected a misassociation between valid client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). Association type is ([IDS_EV_ASSOCIATION_TYPE:%s]), SNR of client is [IDS_EV_SNR:%d].	This event indicates that an AP detected a misassociation between a valid client and an unsafe AP. Detection is enabled via the 'Detect Valid Client Misassociation' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
127077	Warning	AP([RADIO_MAC:%m]): TKIP Replay Attack: An AP detected a possible TKIP replay against station [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] with SNR [IDS_EV_SNR:%d] and BAND [IDS_EV_AP_BAND:%s]). This may disrupt communication with [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a possible TKIP replay attack. If successful this could be the precursor to more advanced attacks. Detection is enabled via the 'Detect TKIP Replay Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.

127078	Warning	AP([RADIO_MAC:%m]): ChopChop Attack: An AP detected a ChopChop attack against station [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]). This could reveal the WEP key.	This event indicates that an AP detected a ChopChop attack. Detection is enabled via the 'Detect ChopChop Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127079	Warning	AP([RADIO_MAC:%m]): Invalid Address Combination: An AP detected a frame with an invalid source address [IDS_EV_SOURCE_MAC:%m]. This could be an attempt to get the receiver [IDS_EV_RECEIVER_MAC:%m] to reply with a multicast or broadcast frame. Frame received on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with a SNR of [IDS_EV_SNR:%d].	This event indicates that an AP detected an invalid source and destination combination. Detection is enabled via the 'Detect Invalid Address Combination' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127080	Warning	AP([RADIO_MAC:%m]): Malformed Frame - Assoc Request: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent an association request containing an empty SSID. If [IDS_EV_RECEIVER_MAC:%m] uses a vulnerable wireless driver this could cause it to crash.	This event indicates that an AP detected a malformed association request with a NULL SSID. Detection is enabled via the 'Detect Malformed Frame - Assoc Request' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127081	Warning	AP([RADIO_MAC:%m]): Malformed Frame - HT IE: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a management frame containing one or more malformed HT Information Elements. This may disrupt communication with [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a malformed HT Information Element. This can be the result of a misbehaving wireless driver or it may be an indication of a new wireless attack. Detection is enabled via the 'Detect Malformed Frame - HT IE' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127082	Warning	AP([RADIO_MAC:%m]): Overflow EAPOL Key: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a malformed EAPOL Key message with a declared length that is too large. This could disrupt or crash the device with address [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a key in an EAPOL Key message with a specified length greater than the length of the entire message. Detection is enabled via the 'Detect Overflow EAPOL Key' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127083	Warning	AP([RADIO_MAC:%m]): Malformed Frame - Auth: An AP detected a malformed authentication frame from client [IDS_EV_NODE_MAC:%m] to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of frame is [IDS_EV_SNR:%d].	This event indicates that an AP detected an authentication frame with either a bad algorithm (similar to Fata-Jack) or a bad transaction. Detection is enabled via the 'Detect Malformed Frame - Auth' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127084	Warning	AP([RADIO_MAC:%m]): Overflow IE: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a malformed information element with a declared length that is too large. This could disrupt or crash the device with address [IDS_EV_RECEIVER_MAC:%m].	This event indicates that an AP detected a management frame with a malformed information element. The declared length of the element is larger than the entire frame containing the element. This may be used to corrupt or crash wireless drivers. Detection is enabled via the 'Detect Overflow IE' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.

127085	Warning	AP([RADIO_MAC:%m]): Malformed Frame - Large Duration: An AP detected that the device with MAC address [IDS_EV_SOURCE_MAC:%m] (CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) has sent a frame with an unusually large duration. This could be an attempt to deny service to all devices on this channel. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected an unusually large duration in a wireless frame. This may be an attempt to block other devices from transmitting. Detection is enabled via the 'Detect Malformed Frame - Large Duration' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127086	Warning	AP([RADIO_MAC:%m]): Beacon Frame with Incorrect Channel: An AP detected that the Access Point with MAC [IDS_EV_SOURCE_MAC:%m] and BSSID [IDS_EV_TARGET_AP_BSSID:%m] has sent a beacon for SSID [IDS_EV_TARGET_AP_SSID:%s]. This beacon advertizes CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] but was received on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_TARGET_AP_BAND:%s] with SNR [IDS_EV_SNR:%d].	This event indicates that an AP detected a beacon on one channel advertising another channel. This could be an attempt to lure clients away from a valid AP. Detection is enabled via the 'Detect Beacon on Wrong Channel' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
127087	Warning	AP([RADIO_MAC:%m]): Block ACK DoS Attack: An AP detected a data frame which indicates a possible Block ACK DoS Attack. The frame from [IDS_EV_SOURCE_MAC:%m] to [IDS_EV_RECEIVER_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) is outside the current sequence number window, and thus may be dropped. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an attempt has been made to deny service to the source address by spoofing a block ACK add request that sets a sequence number window outside the currently used window. Detection is enabled via the 'Detect Block ACK DoS' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127088	Warning	AP([RADIO_MAC:%m]): Hotspotter Attack: An AP detected that the client with MAC address [IDS_EV_NODE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]) may be under attack from the Hotspotter tool. The probe response was sent from AP [IDS_EV_SOURCE_MAC:%m] for SSID [IDS_EV_TARGET_AP_SSID:%s].	This event indicates that a new AP has appeared immediately following a client probe request. This is indicative of the Hotspotter tool or similar that attempts to event clients with a fake hotspot or other wireless network. Detection is enabled via the 'Detect Hotspotter Attack' setting in the IDS Impersonation profile.	This alert indicates an event that affects one or more clients of your wireless network.
127102	Warning	AP([RADIO_MAC:%m]): AP Deauth Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disconnecting its client (MAC [IDS_EV_NODE_MAC:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s].	This event indicates that an AP has attempted to contain an access point by disconnecting its client. Detection is enabled via the 'Wireless Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127103	Warning	AP([RADIO_MAC:%m]): Client Deauth Containment: An AP attempted to contain a client (MAC [IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s].	This event indicates that an AP has attempted to contain a client by disconnecting it from the AP that it is associated with. Detection is enabled via the 'Wireless Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127104	Warning	AP([RADIO_MAC:%m]): AP Wired Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disconnecting client (MAC [IDS_EV_NODE_MAC:%m]) by disrupting device with IPv4 [IDS_EV_DEVICE_IP:%pI4] IPv6 [IDS_EV_DEVICE_IPV6:%s] and MAC [IDS_EV_DEVICE_MAC:%m].	This event indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127105	Warning	AP([RADIO_MAC:%m]): Client Wired Containment: An AP attempted to contain a client (MAC [IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disrupting device with IPv4 [IDS_EV_DEVICE_IP:%pI4] and/or IPv6 [IDS_EV_DEVICE_IPV6:%s] and MAC [IDS_EV_DEVICE_MAC:%m].	This event indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.

127106	Warning	AP([RADIO_MAC:%m]): AP Tagged Wired Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disconnecting client (MAC [IDS_EV_NODE_MAC:%m]) by disrupting device with IPv4 [IDS_EV_DEVICE_IP:%pI4] and/or IPv6 [IDS_EV_DEVICE_IPV6:%s]and MAC [IDS_EV_DEVICE_MAC:%m] on VLAN [IDS_EV_VLAN_ID:%d].	This event indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127107	Warning	AP([RADIO_MAC:%m]): Client Tagged Wired Containment: An AP attempted to contain a client (MAC [IDS_EV_NODE_MAC:%m]) that is associated to access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) by disrupting device with IP [IDS_EV_DEVICE_IP:%pI4] and/or IPv6 [IDS_EV_DEVICE_IPV6:%s] and MAC [IDS_EV_DEVICE_MAC:%m] on VLAN [IDS_EV_VLAN_ID:%d].	This event indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface. Detection is enabled via the 'Wired Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127108	Warning	AP([RADIO_MAC:%m]): Tarpit Containment: An AP attempted to contain an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m]) on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] by tarpitting client (MAC [IDS_EV_NODE_MAC:%m]) by sending it tarpit on CHANNEL [IDS_EV_TARGET_AP_CHANNEL:%d] (BAND [IDS_EV_TARGET_AP_BAND:%s]) and fake BSSID [IDS_EV_SOURCE_MAC:%m].	This event indicates that an AP has attempted to contain an access point by moving a client that is attempting to associate to it to a tarpit. Detection is enabled via the 'Wireless Containment' setting in the IDS General Profile profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127109	Warning	AP([RADIO_MAC:%m]): Power Save DoS Attack: An AP detected a Power Save DoS attack on client [IDS_EV_NODE_MAC:%m] and access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a Power Save DoS attack. Detection is enabled via the 'Detect Power Save DoS Attack' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127110	Warning	AP([RADIO_MAC:%m]): Wireless Hosted Network: An AP detected a wireless client [IDS_EV_NODE_MAC:%m] that is hosting an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s] with SNR [IDS_EV_SNR:%d]).Classification of client is [IDS_EV_TRAP_CLIENT_CLASS:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a wireless client that is hosting a softAP. The softAP could be used to share the hosting client's wired or wireless network connection with other wireless users. Detection is enabled via the 'Detect Wireless Hosted Network' setting in the IDS Unauthorized Device profile.	This alert indicates an event that may affect your wireless infrastructure.
127111	Warning	AP([RADIO_MAC:%m]): Client Associated To Hosted Network: An AP detected a client [IDS_EV_NODE_MAC:%m] associated to a hosted access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d].	This event indicates that an AP detected that a wireless client associated to an access point that is hosted by another wireless client. Detection is enabled via the 'Detect Wireless Hosted Network' setting in the IDS Unauthorized Device profile.	This alert indicates an event that affects one or more clients of your wireless network.
127112	Warning	AP([RADIO_MAC:%m]): Wireless Hosted Network Containment: An AP attempted to contain a client [IDS_EV_NODE_MAC:%m] that is associated to the hosted network (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). SNR of client is [IDS_EV_SNR:%d].	This event indicates that containment is being enforced on a client associated to a hosted network. Detection is enabled via the 'Protect from Wireless Hosted Networks' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.

127113	Warning	AP([RADIO_MAC:%m]): Host of Wireless Network Containment: An AP attempted to contain a client [IDS_EV_NODE_MAC:%m] that is associated to an access point (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]). The client is hosting the wireless hosted network [IDS_EV_TRAP_AP_BSSID:%m]. SNR of client is [IDS_EV_SNR:%d].	This event indicates that containment is being enforced on a client that is hosting a wireless hosted network. Detection is enabled via the 'Protect from Wireless Hosted Networks' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127114	Warning	AP([RADIO_MAC:%m]): Enhanced Adhoc Containment: An AP attempted to contain an adhoc node [IDS_EV_NODE_MAC:%m] that is part of the adhoc network (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]).	This event indicates that an AP has attempted to contain an adhoc node by disconnecting it from other members of the adhoc network. Detection is enabled via the 'Protect from Adhoc Networks - Enhanced' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127115	Warning	AP([RADIO_MAC:%m]): Adhoc Network Using Valid SSID Containment: An AP attempted to contain an adhoc node [IDS_EV_NODE_MAC:%m] (BSSID [IDS_EV_TARGET_AP_BSSID:%m] and SSID [IDS_EV_TARGET_AP_SSID:%s] on CHANNEL [IDS_EV_AP_CHANNEL:%d]) using a valid/protected SSID. SNR is [IDS_EV_SNR:%d]. BAND is [IDS_EV_AP_BAND:%s].	This event indicates that containment is being enforced on an ad hoc wireless network node using a valid/protected SSID. Detection is enabled via the 'Protect from Adhoc Networks Using Valid SSID' setting in the IDS Unauthorized Device profile.	This alert indicates that containment is being enforced to protect your wireless infrastructure.
127116	Warning	AP([RADIO_MAC:%m]): WPA FT Attack: An AP detected a possible attack of the Fast BSS Transition for CLIENT [IDS_EV_NODE_MAC:%m] on BSSID [IDS_EV_TARGET_AP_BSSID:%m] and CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates there is a possible attack of the Fast BSS Transition causing a WPA key re-installation. This can be indicative of a security breach where an attacker can hijack a client's association and/or decrypt an otherwise secure connection. Detection is enabled via the 'Detect WPA FT Attack' setting and the 'WPA FT Attack Detection Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
127117	Warning	AP([RADIO_MAC:%m]): Man in the Middle Attack: An AP detected a possible channel-based Man in the Middle attack. Spoofed beacon frame has source address of [IDS_EV_SOURCE_MAC:%m], a BSSID of [IDS_EV_TARGET_AP_BSSID:%m], announcing a channel switch to CHANNEL [IDS_EV_AP_CHANNEL:%d] and BAND [IDS_EV_AP_BAND:%s]. SNR is [IDS_EV_SNR:%d]. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates that an AP detected a possible channel-based Man in the Middle attack by someone using spoofed beacons with an invalid Channel Switch Announcement. Detection is enabled via the 'Detect Man in the Middle' setting in the IDS Impersonation profile.	This alert indicates an event that may affect your wireless infrastructure.
127119	Warning	AP([RADIO_MAC:%m]): GHOST TUNNEL Attack: An AP detected a possible attack of the Ghost Tunnel Server. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates there is a possible attack of the Ghost Tunnel. This can be airgap atttack only by beacon and probe request where an attacker can hijack a client. Detection is enabled via the 'Detect GHOST TUNNEL SERVER' setting and the 'GHOST TUNNEL Attack Detection Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that may affect your wireless infrastructure.
127120	Warning	AP([RADIO_MAC:%m]): GHOST TUNNEL Attack: An AP detected a possible attack of the Ghost Tunnel CLIENT. Additional Info: [IDS_EV_ADDITIONAL_INFO:%s].	This event indicates there is a possible attack of the Ghost Tunnel. This can be airgap atttack only by beacon and probe request where an attacker can hijack a client. Detection is enabled via the 'Detect GHOST TUNNEL CLIENT' setting and the 'GHOST TUNNEL Attack Detection Threshold' setting in the IDS Denial of Service profile.	This alert indicates an event that affects one or more clients of your wireless network.
132058	Warning	Vendor Id [vid:%d] not supported	Vendor ID in the radius response is not supported. Radius packet will be dropped.	
132094	Warning	MIC failed in [msg:%s] from Station [mac:%m] [bssid:%m] [apname:%s]	Station sent an WPA key message whose MIC verification failed	
133012	Warning	Retry to initialize Internal Database Server, Remaining retries=[retries:%d]	To_be_filled_out	
133038	Warning	Update user [name:%s] failed, user not present in the database	To_be_filled_out	
133109	Warning	User [name:%s] [role:%s] locked out, exceeded authentication threshold	Management user authentication failure (on SERIAL/TELNET/SSH/WebUI) crossed the threshold.	
133116	Warning	RAP allowlist upgrade failed partially. Records upgraded=[num_rec:%d] Records failed=[f_num_rec:%d]	This shows that RAP allowlist was partially upgraded.	

133117	Warning	Remote ip [name:%s] already configured with other MAC addresses	This shows that multiple MACs have the same remote-ip in rap allowlist-db	
133121	Warning	[func:%s]: Sending USERDB_REJ-msg to [dip:%s]:[dport:%u] with msgtype:[msgtype:%u] id:[id:%u] reqtype:[reqtype:%u] dbtype:[dbtype:%u]	This shows deatils about a REJECT response message is sent from udbserver at conductor	
133531	Warning	Putting [ap_macaddr:%s] in Unapproved State - Approved State Timer ([time:%d] mins) expired. Re-approval Needed.	Approved state timer puts APs from Approved to Unapproved state	
134101	Warning	[func:%s](): sapi_init() returned failed.	This indicates error while doing sapi_init().	
134102	Warning	[func:%s](): Failed in sapi_sync() on [lvl:%s].	This indicates error while doing sapi_sync().	
134104	Warning	[func:%s](): Failed in PAPI_Send() - err:[err:%d] arg:[arg:%p].	This indicates error in PAPI_Send().	
134105	Warning	[func:%s](): Received message with wrong length([len:%d]), Ignore it.	This indicates error in receiving PAPI message.	
134106	Warning	[func:%s](): Unable to create Dispatcher.	This indicates error in creating dispatcher.	
134107	Warning	[func:%s](): Unable to initialize PAPI.	This indicates error in initializing PAPI.	
134109	Warning	[func:%s](): Request Queue (size:[size:%lu]) is Full, Drop the request.	This indicates Request-queue in Off-Loader process is full.	
134110	Warning	[func:%s](): Unable to initialize SAPI.	This indicates SAPI cannot be initialized.	
134128	Warning	[func:%s](): Unable to process OWE data, L(STA-Pub):[ppl:%d], PrimeLength:[pl:%d], CrptoReady:[cr:%s].	This indicates Invalid Input data for OWE processing.	
134129	Warning	[func:%s](): Invalid inputs to SAE operations	This indicates Invalid Input data for SAE operations.	
136003	Warning	[func:%s](cmd=[cmd:%s]): Failed, Re-init DB Schema with '[schema:%s]'.	This indicated failure in finding DB Version.	
136004	Warning	[func:%s](): DB-Version Mis-Matched([curVer:%d]/[swVer:%d]), Re-init DB Schema with '[schema:%s]'.	This indicated DB Version mis-matched.	
136006	Warning	[func:%s](): Failed to insert attribute:'[attname:%s]' into [tblname:%s] for station:'[st:%s]' user:'[uname:%s]' survMethod:[smethod:%x], errno:[errno:%d], errmsg:[errmsg:%s].	This is indicates an failure while inserting access credential into survival database	
136009	Warning	[func:%s](): Current RAD-DB is FULL. Can not perform for station:'[st:%s]' user:'[uname:%s]'	This indicates the current RADDB is FULL and can not store the credential intoi RAD-DB.	
136012	Warning	[func:%s](): sapi_init() returned failed.	This indicates error while doing sapi_init().	
136013	Warning	[func:%s](): Failed in sapi_sync() on [lvl:%s].	This indicates error while doing sapi_sync().	
136015	Warning	[func:%s](): Failed in PAPI_Send() - err:[err:%d] arg:[arg:%p].	This indicates error in PAPI_Send().	
136016	Warning	[func:%s](): Received message with wrong length([len:%d]), Ignore it.	This indicates error in receiving PAPI message.	
136018	Warning	[func:%s](): Unable to create Dispatcher.	This indicates error in creating dispatcher.	
136019	Warning	[func:%s](): Unable to initialize PAPI.	This indicates error in initializing PAPI.	
136021	Warning	[func:%s](): Request Queue (size:[size:%lu]) is Full, Drop the request.	This indicates Request-queue in survival process is full.	
136022	Warning	[func:%s](): Unable to initialize SAPI.	This indicates SAPI cannot be initialized.	
136028	Warning	[func:%s](): Invalid Server-Cert name, size:[sz:%zu]).	This indicates server-cert-name is invalid.	
136029	Warning	[func:%s](): Invalid certificate message type in response message [type:%d].	This indicates msg type mismatch in response message.	
136030	Warning	[func:%s](): Certificate [cert:%s] was not found.	This indicates a certificate is not found.	
136031	Warning	[func:%s](): The service type for the certificate in the request [req:%d] and response [rsp:%d] does not match.	This indicates service type mismatch between certificate request and response.	
136033	Warning	[func:%s](): Capacity of RAD-DB is Full, Credential cannot be saved.	This indicates the RAD-DB is at its full capacity.	
136036	Warning	UPD-RadDB([req:%lu]@[worker:%s]): Failed to Update RAD-DB for station:'[st:%s]' user:'[user:%s]' survMethod:[smethod:%x], result:[res:%d].	This is an internal debugging message.	
136039	Warning	DEL-RadDB([req:%lu]@[worker:%s]): Failed to Delete station:'[st:%s]' user:'[user:%s]' survMethod:[smethod:%x] from RAD-DB, result:[res:%d].	This is an internal debugging message.	

136040	Warning	[func:%s](): Current RAD-DB capacity is:[percent:%d]%.	This indicates the current RAD-DB capacity reache warning level.	
136044	Warning	[func:%s](): Certificate '[cert:%s]' expired.	This indicates a certificate is expired.	
136047	Warning	[func:%s](): Failed to purge table [tblname:%s], errno:[errno:%d], errmsg:[errmsg:%s].	This is indicates an failure while purging access credential from survival database	
137004	Warning	RADIUS server [name:%s]-[fqdn:%s]-[ipaddr:%s]-[sin_port:%u] timeout	RADIUS Server is unreachable. The server could be down or there is connectivity problem	Check RADIUS server connectivity
137006	Warning	RADIUS (RFC 3576): Ignoring request from unknown client [srv_ipaddr:%s] port([srv_port:%d])	A request was received on RADIUS port 3799 (RFC 3576), but the RADIUS server is not configured.	If the request is expected, please configure RADIUS server using "aaa rfc-3576-server" command.
137007	Warning	RADIUS (RFC 3576): Ignoring request from client [srv_ipaddr:%s] port([srv_port:%d]) with unknown code [code:%d]	A request was received on RADIUS port 3799 (RFC 3576) with unknown code.	Please check RADIUS server and RFC 3799 client configuration
142006	Warning	[message:%s]	L2TP generic warning.	

ID	Type	Message	Description	Action
300109	Alert	Licenses will expire in [days:%u] days	Some evaluation licenses will expire in the stated number of days. For feature licenses, this will cause the controller to reload. At this level, fewer than 2 days remain until expiry.	Please make a list of licenses (from the "show license" command output) which are about to expire and contact support
300114	Alert	License manager initiating reload; unsaved configuration changes will be lost	Feature licenses have expired and the controller is reloading in order to deactivate the features.	Please make a list of expired licenses (from the "show license" command output) and contact support
300141	Alert	Licenses sent by the server will expire in [days:%u] days	Licenses sent by the server will expire in the stated number of days. At this level, fewer than 5 days remain until expiry.	Please resolve connectivity issues with the license server.
300146	Alert	Licenses contributed by the client with mac address [mac:%m] will expire in [days:%u] days	Licenses contributed by the client will expire in the stated number of days. At this level, fewer than 5 days remain until expiry.	Please resolve connectivity issues with the license client.
300162	Alert	Invalid licenses will be removed in [days:%u] days	Some invalid licenses will expire in the stated number of days. This will cause the controller to reload. At this level, fewer than 30 days remain until expiry.	Please make a list of licenses (from the "show license" command output) which are about to expire and contact support
300301	Alert	FIPS Alert: [msg:%s]	This is a FIPS alert log in system module.	
334529	Alert	Failed to add Lsa to AgingObj in LsaInstall		
341007	Alert	[msg:%s]		
341091	Alert	[func:%s]: [line:%d]: out of memory.	The AP is upgrading image from awc.	
341276	Alert	Could not program ACL = [acl:%d] to datapath.	Datapath ACL programming failed.	
341286	Alert	could not download the required file, reason [reason:%s]	could not download the required file.	
341287	Alert	managed mode: Could not apply the configuration fetched from server [reason:%s], error code [error_code:%d].	could not apply the configuration fetched from server.	
341342	Alert	Could not program ACL [name:%s]([acl:%d]) to datapath because the maximum ACE entries([number:%d]) has reached.	Datapath ACL programming failed.	
386001	Alert	[msg:%s]	UDMD system alert log	
300108	Critical	Licenses will expire in [days:%u] days	Some evaluation licenses will expire in the stated number of days. For feature licenses, this will cause the controller to reload. At this level, fewer than 15 days remain until expiry.	Please make a list of licenses (from the "show license" command output) which are about to expire and contact support
300117	Critical	Failed to create the license database: [error:%s]	At initialization time, the license database could not be created.	Please reload the controller. If the problem persists, contact support.
300144	Critical	Licenses sent by the server will expire in [days:%u] days	Licenses sent by the server will expire in the stated number of days. At this level, fewer than 15 days remain until expiry.	Please resolve connectivity issues with the license server.
300157	Critical	Licenses contributed by the client with mac address [mac:%m] will expire in [days:%u] days	Licenses contributed by the client will expire in the stated number of days. At this level, fewer than 15 days remain until expiry.	Please resolve connectivity issues with the license client.
300182	Critical	[function:%s]: Solid DB ERROR Message - [error:%s]	The license manager failed to query its database. This error is fatal and the process will restart	If the error persists, contact support
300183	Critical	[function:%s]: Asserting......	The license manager failed to query its database. This error is fatal and the process will restart	If the error persists, contact support
300187	Critical	[function:%s]: [error: %s]	An ODBC error has occurred when creating the License DB.	NA
300302	Critical	FIPS Critical: [msg:%s]	This is a FIPS critical log in system module.	
303048	Critical	Still do not have enough free flash space, nothing more to delete: free flash space is [free:%d] MB	This should not happen, contact technical support.	Contact technical support
303087	Critical	cannot open random dev	NA	
303088	Critical	Fatal error in reading the random dev	NA	
303089	Critical	Fatal Error : Key1 and Key 2 Stuck	NA	
303090	Critical	Fatal Error : FIPS Rand Seed Failed	NA	
303091	Critical	Failed SW FIPS KAT test, Fatal error	NA	
307087	Critical	BAD NETWORK CONFIGURATION.Configuration Snapshot is sent to the Conductor. A Local switch in the network has the same IP address as the conductor.	Network configuration is incorrect. A local switch in the network has the same IP address as the conductor.	Validate network configuration and addressing of local and conductor controller
309800	Critical	[func:%s](): [msg:%s]	This shows a critical error message in ExtIntfMgr.	
312403	Critical	[msg:%s]		
313109	Critical	[func_name:%s] Potentially Fatal Problem	To be filled out	
314806	Critical	POE over subscribed, Turning off [slot:%d]/[port:%d]	Turning off the port as the POE is oversubscribed	

315382	Critical	[cause:%s]	This syslog describes the reason the switch was rebooted	
325017	Critical	Maximum [string:%s] user capacity of [count:%d] reached.	System has reached maximum user capacity.	Limit of the system has been reached.
325026	Critical	Max xSec user capacity of [count:%d] reached	System has reached max xSec user capacity	
325028	Critical	Max ACR capacity of [count:%d] reached	System has reached max capacity of Advanced Crypto users	
334001	Critical	Unable to read regulatory domain data from hardware	The system reported an error while trying to read regulatory domain information from the system hardware. As a result, the country code may not be set correctly on the controller and the APs may not be able to come up without the appropriate country code.	Please contact Aruba tech-support if this problem persists.
334544	Critical	The number of OSPFv2 network routes exceeds the forwarding table limit of [num:%d] routes		
334545	Critical	Failed to add OSPFv2 route because routing table is full		
334546	Critical	Discarding LSA because LS database is full. LS database contains [num:%u] LSAs		
335002	Critical	An overtemperature condition has been detected: [desc:%s] [data:%f]	A card Tempertaure is too high. Assure that ambient temperture is not too high and that airflow is unrestricted around the chassis vents.	
335008	Critical	Communication with the Peer M3 in the Bottom slots is broken. Please check the Bottom slot to make sure it is operational	Top slot M3 is not able to talk to the bottom slot M3	
335020	Critical	Critical Alarm: [Critical: %s]	Critical system alarm log.	
335503	Critical	DHCP-RELAY exiting due to critical GSM errors.	GSM initialization failed, exiting dhcp-relay.	Contact Aruba tech-support.
341006	Critical	[msg:%s]		
341275	Critical	vpn tunnel switch to [tunnel:%s], reason:[reason:%s].	vpn tunnel switch.	
341279	Critical	managed mode: Could not download the configuration from the server.	Could not download the configuration from the server.	
341337	Critical	[msg:%s]	netlink critical message	
343501	Critical	[func:%s] [line:%d] [msg:%s]	System related critical messages logged in AirGroup	Contact tech-support
386002	Critical	[msg:%s]	UDMD system critical log	
394001	Critical	[msg:%s]	Generic Critical level system log	
398529	Critical	The system has reached its capacity of WAN policies.	The system has reached its WAN policy capacity.	Delete or consolidate the existing WAN policies to free up space for more policies.
399811	Critical	Unable to initialize [operation:%s] in [function:%s], [file:%s]:[line:%d].	This log indicates that the system was unable to initialize a system component. This could be a transient condition and the problem might go away	In case the problem persists, please contact the technical support.
300004	Debug	Received unexpected message type [ty:%d] from Station Management	NA	
300010	Debug	Mobile IP service is initializing...	Mobile IP service is starting to initialize. This message is always logged regardless if mobility is enabled or not with "router mobile" cli command	
300012	Debug	GSM: cha sta :[act:%s]: [mac:%s]		
300013	Debug	Mobile IP GSM thread started	Mobile IP GSM thread started	
300014	Debug	GSM: cha mip_proxy :[act:%s]: [mac:%s]		
300138	Debug	[function:%s]: attempting to instantiate config fragments for [feature:%s] [[id:%d]]	About to start instantiating config fragments for the feature.	
300140	Debug	[function:%s]: License Table already exists		
300149	Debug	[function:%s]: executing cmd [cmd:%s]	Executing the command.	
300150	Debug	[function:%s]: matched key: [key:%s], flags fl [fl:%x]/[kfl:%x], ft [ftctnt:%d]/[ft:%d], val [val:%u]/[kval:%u]	Matched the key.	
300151	Debug	[function:%s]: allowing 2nd temp key since tstamp is different limit [limit:%s] / [val:%u]	Allowing the second temp key since timestamp is different.	
300153	Debug	[function:%s]: constraining: max [max:%u], key [key:%u], cur [cur:%u]	Constraining the license limits to max. limits as the values configured through the license key are greater the allowed maximum limits.	
300159	Debug	[function:%s]: permanent/subscription keys can't be installed more than once	This key has already been installed once.	
300160	Debug	[function:%s]: allowing reinstall of [feature:%s] since icount is [icount:%s]	Allow reinstall since icount is less than the max. limit.	

300161	Debug	[function:%s]: disallowing reinstall of [feature:%s] since icount is [icount:%s]	Disallow reinstall since icount reached the max. limit.	
300167	Debug	[function:%s]: not deleting key [key:%s] since it is disabled	Not deleting the key as it is already disabled.	
300168	Debug	[function:%s]: t [t:%s], ct [ct:%s], et [et:%s], force [force:%d]	Display time expiry.	
300176	Debug	[function:%s]: Continuing show at [index:%d], totlics [totlics:%d]	Displaying the licenses.	
300177	Debug	[function:%s]: Stopping show at [index:%d]	Stopping the display of the licenses.	
300178	Debug	[function:%s]: Number of licenses: [num:%s]	Displaying the number of licenses.	
300184	Debug	[function:%s]: License DB existing version is [version:%d]	Displaying the License DB existing version.	
300185	Debug	[function:%s]: License DB already exists	License DB already exists.	
300188	Debug	[function:%s]: Command for creating the licensedb table is: [cmd:%s]	The command for creating the LicenseDB.	
300192	Debug	[function:%s]: setting activation status of all licenses to [status:%d]	Setting the activation status of all licenses.	
300193	Debug	[function:%s]: marking key [key:%s] as inactive	Marking the key as inactive.	
300194	Debug	[function:%s]: Mesh AP License Key [key:%s]	Displays the Mesh AP License Key.	
300197	Debug	[string:%s]	This shows an internal debug message.	
300204	Debug	CTS debug [msg:%s].	General debug log for CTS	
300307	Debug	FIPS Debug: [function:%s], [file:%s]:[line:%d]: [msg:%s]	This is a FIPS debugging log in system module.	
300501	Debug	[func:%s], [line:%d], [msg:%s]	System related debugging messages logged in the user visibility process	
300801	Debug	[msg:%s]	Central Agent Debug Message.	
300900	Debug	[name:%s]	This is an internal debug message	
301002	Debug	Traps are disabled. Cannot send traps.		
301248	Debug	Received a trap before initialization. Initializing the traps	To_be_filled_out	
301255	Debug	Inform Timer expired for record ([serial_num:%d]) going to [tst:%s]	To_be_filled_out	
301256	Debug	Removing the Notification Record ([serial_num:%d]), Retry count is met, trapnum [trapnum:%d]	To_be_filled_out	
301257	Debug	Got response/report to InformRequest from [clientip:%s]	To_be_filled_out	
301266	Debug	Removing the Notification Record ([serial_num:%d]), Received the Response	To_be_filled_out	
301281	Debug	Receive Name [name:%s], ip [ip_addr:%s], version [ver:%d], port [prt:%d], isInform [notify:%d] round trip time [rtt:%d], retrycount [retcnt:%d], isMms [ismms:%d]	To_be_filled_out	
301282	Debug	Error: Creating the receiver [rcvName:%s] table	To_be_filled_out	
301283	Debug	Receive Name [rcvName:%s], ip [ipStr:%s], version [version:%d], port [port:%d]	To_be_filled_out	
301284	Debug	Error, Adding the Data to the RespBuf in trap queue	To_be_filled_out	
301285	Debug	Inform Entry is already present.	To_be_filled_out	
301286	Debug	Trap Entry already present	To_be_filled_out	
301293	Debug	Modifying the V2C Host Receiver ([communityName:%s])	To_be_filled_out	
301295	Debug	[__LINE:%d]: Modifying the V2C Host Parameters ([communityName:%s])	To_be_filled_out	
301313	Debug	This is a New Trap([trapNum:%d]), Send it the switch	To_be_filled_out	
301315	Debug	Trap [trapNumber:%d] is Disabled	To_be_filled_out	
301321	Debug	too many active faults for trap '[descr:%s]'	To_be_filled_out	
301322	Debug	can't create uptime info for '[descr:%s]'	To_be_filled_out	
301323	Debug	can't clone OID info for '[descr:%s]'	To_be_filled_out	
301324	Debug	can't make trap OID info for '[descr:%s]'	To_be_filled_out	
301325	Debug	can't make trap time info for '[descr:%s]'	To_be_filled_out	
301326	Debug	can't clone notification OID info for '[descr:%s]'	To_be_filled_out	
301327	Debug	can't make date/time info for '[descr:%s]'	To_be_filled_out	
301331	Debug	Illegal CID in the request [oid_ptr:%d] from [ipaddr:%s]	To_be_filled_out	
301334	Debug	Processing Switch Ip Address Change Message	To_be_filled_out	
301336	Debug	[line:%d] Cannot send traps, Traps are disabled	To_be_filled_out	
301342	Debug	Could Not Retrieve the Network Processor CPU Utilization	To_be_filled_out	
301343	Debug	NP CPU Processor Load is [sysXProcessorLoad:%d]	To_be_filled_out	
301407	Debug	Sent classification server [ipaddr:%pI4] optype [type:%d] to WMS	SNMP agent debug message for when we notify WMS of new active MMS server.	

301419	Debug	[func:%s] Stats Collection done for req [req:%d] category [cat:%d]	not filled up	
301420	Debug	[func:%s] Stats Collection done for req [req:%d]	not filled up	
301421	Debug	[func:%s] [line:%d] Stats req being sent for [req:%d] cat [ct:%d] tbl [tbl:%d] appId [modId:%d] curfilelen [lnt:%d]	not filled up	
301427	Debug	[func:%s] Generating https response for the stats file [name:%s]	not filled up	
301435	Debug	[func:%s] [line:%d] Snmp Stats Req Timer is removed	not filled up	
301438	Debug	Processing Switch IPv6 Address Change Message	This syslog indicates IPv6 Address Change.	
303006	Debug	Failed to write faultmgr info: [error:%s]	NA	
303007	Debug	Failed to write faultmgr info: [error:%s]	NA	
303010	Debug	Registering applications dependency: node [src:%pI4]:[port:%d]: is dependent on port [local:%d]	NA	
303011	Debug	Sending applications dependency notification to node [src:%pI4]:[port:%d], local port [local:%d] is up	NA	
303012	Debug	Applications dependency: local port [local:%d] is up	NA	
303060	Debug	New Original Cached memory [cached:%d] ([cachedmb:%d] MB)	NA	
303078	Debug	Process [process:%s] [pid [pid:%d]] exited with [ecode:%d]	NA	
304003	Debug	[msg:%s]	System related debugging messages logged in the station manager (stm).	
304008	Debug	[msg:%s]		
304021	Debug	[func:%s]:[line:%d] Flow [flow_id:%d] not found		
304030	Debug	License key - [f:%s] - [mode:%s]	This message indicates whether the specified licensed feature is enabled or disabled	
304034	Debug	handle_enet_message_response: MAC [mac:%m] nothing outstanding		
304036	Debug	handle_enet_message_response: IP [ip:%P] not found		
304051	Debug	In-memory client denylist table cleared.	This log indicates that the in-memory client denylist was cleared.	
304052	Debug	Client denylist database table cleared.	This log indicates that the client denylist database table was cleared.	
304053	Debug	Client denylist repopulated from database.	This log indicates that the in-memory client denylist was repopulated from the database.	
304059	Debug	[func:%s], [line:%d]: sap_ip: [sapip:%s], tunnel_ip: [tunnelip:%s], tunnel id: [tunnelid:%x]	This debugging log indicates the tunnel id returned from datapath.	
304061	Debug	[func:%s], [line:%d]: add [add:%d] mcast_group [group:%x] dest_idx: [dest:%x]	This debugging log indicates the multicast group and destination index.	
304066	Debug	[func:%s]: [line:%d]: vlan [id:%d] has [user:%d] users	Count user number from a specified vlan.	
304069	Debug	Sending msg from STM to AMP mgmt-server [ip:%P] radios:[nradios:%d] vaps:[nvaps:%d] stas:[stas:%d] unassoc_stas:[unassoc_stas:%d] ap_info:[ap_info:%d] radio_info:[radio_info:%d] vap_info:[vap_info:%d] ap_sys_info:[ap_sys_info:%d] radios_ext:[nradios_ext:%d] vaps_ext:[nvaps_ext:%d] stas_ext:[stats_ext:%d] ap_eth_stats[ap_eth_stats:%d] ap_usb_stats[ap_usb_stats:%d] ap_lldp_nbr[ap_lldp_nbr:%d] ap_pcapdump_xfer[ap_pcapdump_xfer:%d]	This log displays a record of the transmission of the AMON message from STM to the amp management server. It includes statistics regarding the number of transmitted STM records.	
304070	Debug	Sending msg from STM to mgmt-server [ip:%P] radios:[nradios:%d] vaps:[nvaps:%d] stas:[stas:%d] unassoc_stas:[unassoc_stas:%d] ap_info:[ap_info:%d] radio_info:[radio_info:%d] vap_info:[vap_info:%d] ap_sys_info:[ap_sys_info:%d] radios_ext:[nradios_ext:%d] vaps_ext:[nvaps_ext:%d] stas_ext:[stats_ext:%d] ap_eth_stats[ap_eth_stats:%d] ap_usb_stats[ap_usb_stats:%d] ap_lldp_nbr[ap_lldp_nbr:%d] ap_pcapdump_xfer[ap_pcapdump_xfer:%d]	This log displays a record of the transmission of the AMON message from STM to the ale management server. It includes statistics regarding the number of transmitted STM records.	

304071	Debug	Sending msg STM to HTTP mgmt-server [protocol:%s] [hostname:%s] [port:%d] [identifier:%s] radios:[nradios:%d] vaps:[nvaps:%d] stas:[stas:%d] unassoc_stas:[unassoc_stas:%d] ap_info:[ap_info:%d] radio_info:[radio_info:%d] vap_info:[vap_info:%d] ap_sys_info:[ap_sys_info:%d] radios_ext:[nradios_ext:%d] vaps_ext:[nvaps_ext:%d] stas_ext:[stats_ext:%d] ap_eth_stats[ap_eth_stats:%d] ap_usb_stats[ap_usb_stats:%d]	This log displays a record of the transmission of the AMON message from STM to the http management server. It includes statistics regarding the number of transmitted STM records.	
304072	Debug	Adding AP_NEIGHBORS records, count [num_records:%d]	This log indicates the number of ap neighbors records added to the AMON message buffer.	
304073	Debug	Sent a total of [num_records:%d] AP_NEIGHBORS records	This log indicates the total number of ap neighbors records sent to the management server.	
304074	Debug	Adding RADIO_STATS records, count [num_records:%d]	This log indicates the number of radio stats records added to the AMON message buffer.	
304075	Debug	Sent a total of [num_records:%d] RADIO_STATS records	This log indicates the total number of radio stats records sent to the management server.	
304076	Debug	Adding VAP_STATS records, count [num_records:%d]	This log indicates the number of vap stats records added to the AMON message buffer.	
304077	Debug	Sent a total of [num_records:%d] VAP_STATS records	This log indicates the total number of vap stats records sent to the management server.	
304078	Debug	Adding UNASSOCIATED_STA records, count [num_records:%d]	This log indicates the number of unassociated station records added to the AMON message buffer.	
304079	Debug	Sent a total of [num_records:%d] UNASSOCIATED_STA records	This log indicates the total number of unassociated station records sent to the management server.	
304080	Debug	Adding STATION_STATS records, count [num_records:%d]	This log indicates the number of station stats records added to the AMON message buffer.	
304081	Debug	Sent a total of [num_records:%d] STATION_STATS records	This log indicates the total number of station stats records sent to the management server.	
304082	Debug	Adding AP_INFO records, count [num_records:%d]	This log indicates the number of ap info records to the AMON message buffer.	
304083	Debug	Sent a total of [num_records:%d] AP_INFO records	This log indicates the total number of ap info records sent to the management server.	
304084	Debug	Adding RADIO_INFO records, count [num_records:%d]	This log indicates the number of radio info records added to the AMON message buffer.	
304085	Debug	Sent a total of [num_records:%d] RADIO_INFO records	This log indicates the total number of radio info records sent to the management server.	
304086	Debug	Adding VAP_INFO records, count [num_records:%d]	This log indicates the number of vap info records added to the AMON message buffer.	
304087	Debug	Sent a total of [num_records:%d] VAP_INFO records	This log indicates the total number of vap info records sent to the management server.	
304088	Debug	Adding AP_SYS_STATS records, count [num_records:%d]	This log indicates the number of ap system stats records added to the AMON message buffer.	
304089	Debug	Sent a total of [num_records:%d] AP_SYS_STATS records	This log indicates the total number of ap system stats records sent to the management server.	
304090	Debug	handle_enet_message_response: IP [ip:%P] PORT [port:%d] not found		
304092	Debug	[APSTM_PASS_STA:%s]	This log used in different phases of APSTM_PASSIVE_STA AMON table population.	
304093	Debug	[CTRL_STM_PASS_STA:%s]	This log used in different phases of CTRL_STM_PASSIVE_STA AMON table population.	
304094	Debug	[APSTM_PASS_BSS_AGG:%s]	This log used in different phases of APSTM_PASSIVE_BSS_AGGR AMON table population.	
304097	Debug	In-memory client trail-info cleared.	This log indicates that the in-memory client trail-info cleared.	
304098	Debug	Adding RADIO_STATS_EXT records, count [num_records:%d]	This log indicates the number of radio stats ext records added to the AMON message buffer.	
304099	Debug	Sent a total of [num_records:%d] RADIO_STATS_EXT records	This log indicates the total number of radio stats ext records sent to the management server.	

304100	Debug	Adding VAP_STATS_EXT records, count [num_records:%d]	This log indicates the number of vap stats ext records added to the AMON message buffer.	
304101	Debug	Sent a total of [num_records:%d] VAP_STATS_EXT records	This log indicates the total number of vap stats ext records sent to the management server.	
304102	Debug	Adding STATION_STATS_EXT records, count [num_records:%d]	This log indicates the number of station stats ext records added to the AMON message buffer.	
304103	Debug	Sent a total of [num_records:%d] VAP_STATS_EXT records	This log indicates the total number of station stats ext records sent to the management server.	
304105	Debug	Adding AP_ETH_STATS records, count [num_records:%d]	This log indicates the number of ethernet stats records added to the AMON message buffer.	
304106	Debug	Sent a total of [num_records:%d] AP_ETH_STATS records	This log indicates the total number of ethernet stats records sent to the management server.	
304107	Debug	Adding AP_USB_STATS records, count [num_records:%d]	This log indicates the number of USB stats records added to the AMON message buffer.	
304108	Debug	Sent a total of [num_records:%d] AP_USB_STATS records	This log indicates the total number of USB stats records sent to the management server.	
304110	Debug	MM: [func:%s] mon client [name:%s] user info added, uuid = [uuid:%s], mac = [mac:%s]		
304111	Debug	MM: [func:%s] mon client's user info deleted for entry with uuid = [uuid:%s]		
304113	Debug	MM: [func:%s] mon client's [name:%s] user IP updated uuid = [uuid:%s], mac = [mac:%s], ip = [ip:%s], role = [role:%s]		
304114	Debug	[msg:%s]		
304115	Debug	MM: mon client [name:%s] deleted and recreated (l2 mobility)... last bssid = [last_bssid:%s], new bssid = [new_bssid:%s]		
304118	Debug	[APSTM_PASS_RADIO_AGG:%s]	This log used in different phases of APSTM_PASSIVE_RADIO_AGGR AMON table population.	
304120	Debug	Adding AP_LLDP_NBR records, count [num_records:%d]	This log indicates the number of ap lldp nbr records added to the AMON message buffer.	
304121	Debug	Sent a total of [num_records:%d] AP_LLDP_NBR records	This log indicates the total number of ap lldp nbr records sent to the management server.	
304122	Debug	Adding AP_PCAPDUMP_XFER records, count [num_records:%d]	This log indicates the number of ap pcapdump xfer records added to the AMON message buffer.	
304123	Debug	Sent a total of [num_records:%d] AP_PCAPDUMP_XFER records	This log indicates the total number of ap pcapdump xfer records sent to the management server.	
305016	Debug	Remote AP [name:%s]: LMS redirect suppressed.		
305025	Debug	[msg:%s]		
305026	Debug	[msg:%s]		
305055	Debug	[msg:%s]		
305060	Debug	[msg:%s]	Logs regarding downloadable regulatory table	
305062	Debug	[msg:%s]	Logs regarding AP configuration	
305063	Debug	[msg:%s]	Logs regarding configuration.	
305064	Debug	[msg:%s]	Logs regarding ap license debug	
305100	Debug	[msg:%s]		
305105	Debug	Analytics Engine Debug info: [msg:%s]	This is used for analytics debug	
306000	Debug	[msg:%s]	WCD debug log	
306408	Debug	Enabled TSGW Txn	Debug message that tsgw is enabled	
306409	Debug	Disabled TSGW Txn	Debug message that tsgw is disable	
306412	Debug	Requesting switch IP.	VPN module requesting for switch IP	
306414	Debug	[func:%s](): Entered, Caller:[caller:%s] pname:[pname:%s] prevaddr:[preaddr:%s]	Debugging message for entring get_addr from ip pools	
306415	Debug	[func:%s](): Caller:[caller:%s] pname:[pname:%s] prevaddr:[preaddr:%s]. Keep Previous IP address:[ip:%s]	Debugging message for keeping previous IP	
306416	Debug	[func:%s](): Caller:[caller:%s] pname:[pname:%s]. Allocated IP address:[ip:%s] from pool:[pool:%s]	Debugging message for allocating IP from pools	
306417	Debug	[func:%s](): Caller:[caller:%s]. Freeing IP address:[ip:%s] to pool:[pool:%s]	Debugging message for freeing IP to pools	

306418	Debug	[string:%s]	Internal Debugging message for VPNCLI	
306500	Debug	Register to subscribe service '[service:%s]'	Message to indicate a new module registering with the pub/sub service as subscriber	
306501	Debug	Register to publish service '[service:%s]'	Message to indicate a new module registering with the pub/sub service as publisher	
306502	Debug	Publish service '[service:%s]', object len [len:%d]	Message to indicate a new service being published, with the length of information published by this service. The object will be published to all the subscribers of the indicated service	
306503	Debug	Publish service '[service:%s]', object len [len:%d] to module [module:%d]	Message to indicate a new private service being published to the specified module, with the length of information published by this service	
306504	Debug	received subscription message from [sender:%d] for service '[service:%s]'	Message indicating reception of subscription message for a service	
306505	Debug	Module [[sender:%d]] will publish service '[service:%s]'	Publisher received a registration to publish a service	
306506	Debug	Module [[sender:%d]] will subscribe to service '[service:%s]'	Publisher received a registration to subscribe to a service	
306507	Debug	Forward subscribe request from [sender:%d] to [publisher:%d] (service '[service:%s]')	Message from Pub/Sub server about forwarding a subscription request to publisher	
306508	Debug	Module [[sender:%d]] will unsubscribe service '[service:%s]'	Message from Pub/Sub server about a module unsubscribing from a service	
306509	Debug	Module [[sender:%d]] will not publish service '[service:%s]'	Message from Pub/Sub server about a module stopping to publish a service	
306511	Debug	No subscriber exists for service '[service:%s]'; message from [sender:%d] dropped	Warning message from Pub/Sub server that no subscriber exists for the specified service for which a message was received from specified sender	
306512	Debug	Publish message from [sender:%d] to [subscriber:%d] (service '[service:%s]')	Message from Pub/Sub server that a message was published for the specified service to specified sender and receiver	
306513	Debug	Proxy subscribe request from [sender:%d] to [publisher:%d] (service '[service:%s]')	When a module begins to publish a service for which subscribers already exists, a proxy subscription request is sent to publisher on behalf of the subscriber	
306517	Debug	Resend pubsub message to register as publisher for service [service:%s] from Module [mod:%s]	Resent pubsub message to register as publisher	
306518	Debug	Resend pubsub message to register as subscriber for service [service:%s] from Module [mod:%s]	Resent pubsub message to register as subscriber	
306519	Debug	Unregister from subscribe service '[service:%s]'	Message to indicate a module unregistering with the pub/sub service as subscriber	
306603	Debug	Processing the Debug Information	NA	
306705	Debug	[msg:%s]		
306706	Debug	[func:%s], [msg:%s]		
307000	Debug	[__FUNCTION:%s]: sending trap with new role of [role_str:%s] [[nrole:%d]/[srole:%d]]		
307002	Debug	[mySwitchRole:%s]:Got a management message		
307004	Debug	Conductor DNS resolution is not allowed		
307005	Debug	Conductor DNS resolution is allowed		
307006	Debug	The switch conductor ip is set to [switchConductorIP:%s] and the switch ip is [ipStr:%s]		
307007	Debug	The switch conductor ip is the same as my ip		
307008	Debug	The switch conductor ip is the same as my ip(127.0.0.1)		
307009	Debug	The switch conductor ip is not the same as my ip		
307010	Debug	Resolving [conductor_switch:%s]		
307011	Debug	Got a conductor ip of [tempip:%s] through DNS. Discovering the Role again		
307012	Debug	Conductorip is not set and cannot be resolved. Switch becomes conductor		
307014	Debug	HEARTBEAT TIME INTERVAL IS [time:%d].....	NA	
307015	Debug	Sending a Message of type [messageType:%d] to [ip:%s]		
307017	Debug	LmsHeartBeatResultAction: name resolution for [switchConductorHostname:%s] failed		

307018	Debug	LmsHeartBeatResultAction: The new conductor is [conductorIp:%s]		
307020	Debug	Sending The Old heartbeat message...		
307023	Debug	Sending the [type:%s] heartbeat message with active config ID [ts:%d], state [st:%s] to [dip:%s]:[DestPortNum:%d]		
307025	Debug	[mySwitchRole:%s]:Sending heartbeat message to MMS		
307026	Debug	[mySwitchRole:%s]: Refreshing the lms list		
307027	Debug	Checking the LMS not responding flag for local [switchip:%s] flag value is [bNotResponding:%d], missedHB [fc:%d] socketID [sock:%d]		
307029	Debug	Updating LMS list due to switch going down		
307030	Debug	Starting the HeartBeat Engine [mySwitchRole:%s]		
307031	Debug	Cannot create the [timer_type:%s] timer for the switch		
307032	Debug	Stopping the HeartBeat Engine [mySwitchRole:%s]		
307033	Debug	In switchIpChangedCallback. Got a switch ip of [ipaddr:%s]		
307034	Debug	Got the switch ip for the first time		
307035	Debug	Discovering the switch role		
307036	Debug	The switch role is [mySwitchRole:%s]		
307037	Debug	Setting the cfg manager to sapi_state_up...		
307038	Debug	Starting the heartbeat engine		
307041	Debug	Stopping the heartbeat engine		
307043	Debug	Sending the Role Info to Cli		
307044	Debug	Conductor Request : Conductor ip [switchConductorIP:%s] local ip [str:%s]		
307045	Debug	Sending Conductor Ip to [appId:%d]		
307046	Debug	Cannot send Conductor Ip to application [appId:%d]		
307048	Debug	Got a message from [SrcPortNum:%d]:[MessageCode:%d]		
307049	Debug	Received a CFGM_PEER_AND_ROLE_REQ Message		
307050	Debug	Received a IPSEC CFG Message		
307051	Debug	Received the Role Change Message From FPAPPS		
307053	Debug	Invalid magic string in configuration request packet from [SrcPortNum:%d]		
307054	Debug	handleAckMessage:Heartbeat with conductor successful		
307055	Debug	handleAckMessage: we are MMS/SMMS, ignore ack		
307056	Debug	handleAckMessage:Heartbeat with conductor not successful		
307057	Debug	handleAckMessage:Heartbeat with conductor not successful([nConductorNotRespondingCounter:%d])		
307058	Debug	got sxdr_write failure on '[command:%s]'		
307060	Debug	Local switch ([switch_ip:%s]) is yet to make a connection request to the conductor.		
307061	Debug	Cannot Process Snapshot Request. Device [switch_ip: %s] has to retry the Snapshot Request		
307062	Debug	The active configuration file [szActiveConfigFileName:%s] is not valid		
307063	Debug	The active snapshot is [activesnapshot_ts:%d]		
307064	Debug	Reading the configuration for sending snapshot		
307065	Debug	The size of the config data to be transferred is [nSize:%d]		
307066	Debug	Cannot allocate packet for sending snapshot configuration		
307067	Debug	The snap shot message size is [nCount:%d]; computed size was [size:%zu]		
307071	Debug	Configuration sent successfully to the local [switchip:%s]		
307072	Debug	Current Version is [majorVer:%d].[minorVer:%d]		
307073	Debug	Activating the Snapshot		
307075	Debug	Activate sending [elem:%d] elements of configuration to Application [app_id:%d]		
307076	Debug	Large Papi Request Already in Progress, Application [app_id:%d] has to retry the Configuration Request		
307077	Debug	Sending Snap Shot to Application [appId:%d]:[elem:%d] Encrypt flag is [configEncrypt:%d]		
307078	Debug	Re initializing Configuration for APP [appId:%d]		
307079	Debug	PAPI Send Large Failed:Cannot send SnapShot to LOCAL:[app_id:%d]		

307082	Debug	Saving Snapshot Configuration to Config File		
307083	Debug	Preparing data for saving snapshot		
307084	Debug	Done Preparing data for saving snapshot		
307085	Debug	Cannot save configuration to default configuration file:[errno:%d]		
307086	Debug	Saved Snapshot configuration to default configuration file		
307088	Debug	Not saving snapshot configuration because there is no active configuration file		
307089	Debug	reading local configuration for saving snapshot		
307090	Debug	Done reading local configuration for saving snapshot		
307092	Debug	ERROR: Switch [switchip:%s] thinks we are the conductor and is sending a heartbeat message		
307093	Debug	[mySwitchRole:%s]: My active_ts [conductor_ts:%d], Received heartbeat message version [ver:%d] from a LMS [switchip:%s], pkt active_ts [pkt_ts:%d]		
307094	Debug	Creating switch status entry....		
307095	Debug	Setting switch entry not responding to false		
307097	Debug	Updating LMS list due to switch coming up		
307098	Debug	Local ([switchip:%s]) configState [cfg_state:%s], config ID [pkt_ts:%d] doesn't match with conductor config ID [ts:%d]		
307099	Debug	Timestamps are same, state is [cfgUpdateState:%s]		
307100	Debug	Sending heartbeat version [ver:%d] response over [transport:%s] to [dip:%s] config state [cfg_state:%s], my config ID [myts:%d] incoming packet cfgid [incomingts:%d]		
307101	Debug	Done sending a response to a new heartbeat ...		
307104	Debug	[role:%s] [state:%s] received a Heart Beat Response Msg, comparing my active config ID [activesnapshot_ts:%d] and incoming config ID [pkt_ts:%d]		
307105	Debug	requesting snapshot configuration..		
307106	Debug	Received the Role Change Message state [state:%d] conductor ip [conductor_ip:%s] peer ip [peer_ip:%s]		
307107	Debug	CFGM Sync with FPAPPS in progress... Ignoring		
307108	Debug	Cleaning up the Config List		
307109	Debug	Received the Role Change Message state=[state: %d] conductor ip [conductor_ip: %s] peer ip [peer_ip: %s], going active Conductor		
307110	Debug	Received the Role Change Message state=[state: %d] conductor ip [conductor_ip: %s] peer ip [peer_ip: %s], going backup Conductor		
307111	Debug	No Change in Role [state:%d] or Peer Ip [peerIp:%s]		
307112	Debug	Error sending Peer Response to DB Sync Task.		
307113	Debug	Got a message from [SrcPortNum:%d]:[MessageCode:%d] [SrcIpAddr:%s]		
307114	Debug	Received HeartBeat Response Message		
307115	Debug	Received the Role Change Message		
307117	Debug	[mySwitchRole:%s]:Got a heartbeat message from a LMS		
307121	Debug	Done sending a response to a heartbeat ...		
307122	Debug	Comparing [activesnapshot_ts:%ld] and [pkt_activesnapshot_ts:%ld]		
307125	Debug	[file:%s] [func:%s] [line:%d] [mySwitchRole:%s]:Got a snapshot request message from [switchip:%s]		
307126	Debug	Processing the snapshot message. Ignoring the new snapshot message		
307127	Debug	[mySwitchRole:%s]:Got a snapshot data message SnapShot ts [activesnapshot_ts:%d]		
307128	Debug	Locking the Configuration file		
307129	Debug	Error::Cannot Sync with CLI		
307130	Debug	Cannot save the snapshot configuration		
307131	Debug	Unlocking the Configuration file		
307132	Debug	Error: Cannot Release the Cli Semaphore		
307134	Debug	Not Activating the snap shot because the global configuration is not initialized yet		

307135	Debug	Setting the Sapi CFGM Level		
307138	Debug	Registering for switchip		
307140	Debug	Requesting VRRP Role		
307142	Debug	Configuration Manager Done syncing up with fpapps....		
307143	Debug	Configuration Manager Done syncing up with license manager....		
307144	Debug	Request for configuration for [appId:%d]		
307145	Debug	Configuration did not change, sending the previously parsed config data		
307146	Debug	Parsing the Configuration file to get Snapshot data		
307147	Debug	Done Parsing the Configuration file		
307148	Debug	Request for configuration for [appId:%d]		
307149	Debug	configuration for [appId:%d] has [configObjList:%d] entries		
307151	Debug	Reading config manager configuration...		
307152	Debug	The active configuration file name is [szActiveConfigFileName:%s]		
307153	Debug	Failed to read the configuration file [szActiveConfigFileName:%s]		
307154	Debug	Done reading config manager configuration		
307155	Debug	Backing up the configuration		
307156	Debug	Initialized config manager configuration		
307157	Debug	Initialized Snmp..		
307158	Debug	Cannot Initialize sapi		
307159	Debug	Initialized Sapi		
307160	Debug	Configuration Read Failed		
307161	Debug	Local Configuration Read Failed		
307162	Debug	Done reading local configuration...		
307163	Debug	Added message handlers ...		
307168	Debug	Setting CFGM to sapi state up SAPI_LEVEL_CFGMANAGER_LOCAL		
307169	Debug	Trying to sync with fpApps		
307170	Debug	Trying to sync with license manager		
307171	Debug	After the Sync State fpApps		
307172	Debug	The active snap shot is [activesnapshot_ts:%d]		
307173	Debug	Error Sending Data to Cli		
307174	Debug	Error sending LOGLEVEL_REQ to SYSLOGDWRAP task		
307175	Debug	Cannot Recv from CLI socket		
307177	Debug	Cannot Create CLI socket		
307178	Debug	Error Reading the Cli socket options		
307179	Debug	Error making the cli socket NON BLOCKING		
307181	Debug	Starting CFGM task..		
307182	Debug	Retrieve the Software Keys		
307183	Debug	Creating the config file semaphore		
307184	Debug	CFGM Cannot Initialize the CLI Sync Flag		
307185	Debug	Initialized cli semaphore		
307186	Debug	Building the command tree...		
307187	Debug	Done building the command tree...		
307188	Debug	Configuration Manager starting ...		
307189	Debug	Configuration Manager started with CFGMANAGER_LOCAL state		
307190	Debug	Request the Logging Level for CFGM from CLI.		
307191	Debug	Error:Conductor ip matches with an Interface address.		
307192	Debug	The new conductor is [conductorIp:%s]		
307194	Debug	The New Version is [majorVer:%d].[minorVer:%d]		
307195	Debug	In executeCommandObject() [objectType:%d]		
307196	Debug	App [appId:%d] already in list		
307197	Debug	Inserted App [appId:%d] into the list		
307198	Debug	Reading Complete Configuration		
307200	Debug	Getting Configuration from Hash for [appId:%d]		
307201	Debug	Large Papi Request Already in Progress, Adding Application [appid: %d] to the Retry List		

307202	Debug	Processing the Configuration request for application [appId:%d]		
307203	Debug	Generating Configuration Response for application [appid:%d]:[app_config:%d]		
307204	Debug	Sending Response for Configuration Request to [appid:%d] MessageCode is [code:%d]		
307205	Debug	PAPI Send Large Failed:Cannot send configuration to [sip:%s]:[appid:%d] - it will retry		
307206	Debug	Removing App [appId:%d] from the list - it will retry		
307207	Debug	Sending Logging Level Request to application [appId:%d]		
307208	Debug	Sending the Conductor ip to [SrcPortNum:%d]		
307209	Debug	Sending the Conductor ip to CLI		
307210	Debug	Removing App [appId:%d] from the list		
307211	Debug	Processing restricted Configuration request for application [appid:%d]		
307212	Debug	Sending Restricted configuration to app [appId:%d], Num Entries is [objConfig:%d]		
307213	Debug	Configuration Response for restricted request returned error		
307214	Debug	Cannot Allocate memory for the restricted configuration request		
307215	Debug	Error sending the Restricted response to the application [sz:%d]		
307217	Debug	Sending the State Change Information		
307219	Debug	Sending the IPSEC Configuration		
307220	Debug	Error sending IPSec config.		
307221	Debug	Switch ip is not configured yet, not opening the Configuration socket		
307223	Debug	[file:%s] [func:%s] [line:%d] Error, setting the [option_type:%s] option for socket [sock_id:%d] errno [err_str:%s]		
307224	Debug	Error Reading the Config server socket options		
307226	Debug	Error binding the Conductor Config socket: [err_str:%s]:Configuration distribution to the locals will not work properly	There was an error binding the Conductor Config socket. Configuration distribution to the locals will not work properly	
307227	Debug	Error Listening to the Conductor Config socket: [err_str:%s]:Configuration distribution to the locals will not work properly		
307229	Debug	Received a Connection request from [s_addr:%s], socket [lsock:%d]		
307230	Debug	Error, Local ([s_addr:%s]) switch requesting Connection with the conductor is not in the list. Ignoring the connection request		
307231	Debug	Error Setting the Socket Rcv timeout for the socket		
307233	Debug	Opening the Local CFGM socket, state [configSocketState:%d]		
307234	Debug	Switch ip is not configured, not opening the CFGM socket		
307235	Debug	Error opening the Local Config Socket. Configuration Requests to the Conductor will not work properly		
307237	Debug	Error binding the Local Config socket to [myip:%s]: [err_str:%s]:Configuration Requests to the Conductor will not work properly		
307239	Debug	Error Setting the Socket Send timeout for the socket		
307240	Debug	Connecting the Local CFGM socket, state [configSocketState:%d]		
307241	Debug	Error opening the local cfgm socket		
307243	Debug	Processing the snapshot message. Ignoring the new snapshot message		
307245	Debug	Transmission of the Config socket has bad magic number		
307248	Debug	[mySwitchRole:%s]:Got a snapshot data message SnapShot ts [activesnapshot_ts:%ld]		
307252	Debug	Activating the Snapshot		
307253	Debug	Peer ip matches with an Interface address.		
307258	Debug	dbsync process starting...		
307260	Debug	dbsync process ready		
307265	Debug	handle_cfg_message: role= [mySwitchRole:%d]		
307315	Debug	dbsync: failed to open database directory ([EXTRA_FILES_DIR:%s]) (errno= [err_msg:%s])		
307348	Debug	dbsync: Completed Database synchronization on the standby Conductor Switch		

307354	Debug	Error: terminating the local switch ([ip:%s]) connection, socket id is [sock:%d] at function [func:%s], line [line:%d].		
307355	Debug	Error: Deleting the local switch [ip:%s] from conductor switch list.		
307356	Debug	Error: Ageing out the local switch [ip:%s] from conductor switch list.		
307357	Debug	Error: Local switch [ip:%s] AirOS should be upgraded		
307372	Debug	Error occurred sending the configuration data to the local switch ([switchip:%s]): Error code is [code:%s]		
307373	Debug	Sent [size:%d] bytes of configuration, remaining configuration size [rsize:%d] for switch [ip:%s]		
307374	Debug	Size of configuration data is [size:%d]		
307375	Debug	Config socket has insufficient data [size:%d], error is [code:%s]		
307376	Debug	[file:%s] [func:%s] [line:%d] Error reading the config socket, ret value is [ret:%d]. Error code [code:%s]		
307378	Debug	Received an error [code:%s], retrieving the configuration.		
307379	Debug	Did not receive the complete configuration yet, received [size:%d] off total [full_config:%d] bytes		
307380	Debug	Received complete configuration [size:%d]		
307381	Debug	Received a configuration transmission termination message from the conductor.		
307382	Debug	module [module:%s] is busy.		
307383	Debug	Write memory Error, command List is NULL		
307384	Debug	Unable to get current software version.		
307387	Debug	[file:%s] [func:%s] [line:%d] Error, getting socket [option_type:%s] option, errno [error_str:%s]		
307388	Debug	Last Snapshot timer fired on switch [swip:%s], updatestate [upd_state:%s] role [rl:%s] GlobalConfigInit [bgl:%d] active config ID [ts:%d]		
307389	Debug	Last Snapshot timer Started on switch [swip:%s], updatestate [upd_state:%s] role [rl:%s] GlobalConfigInit [bgl:%d] active config ID [ts:%d], timerVal [timer:%d] minutes		
307390	Debug	Last Snapshot timer Stopped on switch [swip:%s], updatestate [upd_state:%s] role [rl:%s] GlobalConfigInit [bgl:%d] active Config ID [ts:%d], timerVal [timer:%d] minutes		
307391	Debug	dbsync: from [ip:%s] port [port:%d] code [msgcode:%d]	debug details of dbsync PAPI mismatch errors	
307392	Debug	[func:%s] [line:%d], Deferring AOS config activation as cfgm is busy pushing config to APP(s), largePapiInProgress [largepapi:%d] pending apply_aos_cfg [applyaoscfg:%d] apply_license_cfg [applyliccfg:%d]		
307393	Debug	[string:%s]	debug details on dbsync	
307402	Debug	Creating the upgrade semaphore flag		
307403	Debug	CFGM cannot initialize upgrade semaphore flag		
307404	Debug	Initialized upgrade flag semaphore		
307405	Debug	Cannot send data to profile manager		
307417	Debug	config sync message: (([__func:%s],[__line:%d],[msg:%s])		
307429	Debug	Registering for switchipv6		
309003	Debug	EndSession to IF-MAP server [[svr:%s]] successfully	This indicates successfully disconnect to an IF-MAP server.	
309006	Debug	Successfully Publish Request(req[id:%lu]) to IF-MAP server [[svr:%s]] using Conn:[conn:%lu]-[sid:%s]	This indicates a message is published to an IF-MAP server successfully.	
309009	Debug	Publish to IF-MAP server [[svr:%s]] Skipped - Session is Down	This indicates the skip of publishing to an IF-MAP server due to no session is established.	
309010	Debug	[func:%s](): Starting session to IF-MAP server [[svr:%s]]	This indicates MAPC is trying to establish a session to an IF-MAP server.	
309011	Debug	[func:%s](): Stopping session to IF-MAP server [[svr:%s]]	This indicates MAPC is trying to tear down a session to an IF-MAP server.	
309012	Debug	[func:%s](req[req:%lu]@[worker:%s]): Publishing user agent string for [type:%s]-MAC/IP=[mac:%s]/[ip:%s] UA-Str="[uastr:%s]..."	This indicates MAPC is trying to publish http-user-agent to IF-MAP server(s).	

309013	Debug	[func:%s](req[req:%lu]@[worker:%s]): No Publishing user agent string - CPPM is Down	This indicates publishing of http-user-agent to IF-MAP server(s) is skipped.	
309014	Debug	[func:%s](req[req:%lu]@[worker:%s]): Publishing mDNS info for mac:[mac:%s]	This indicates MAPC is trying to publish mDNS info to IF-MAP server(s).	
309015	Debug	[func:%s](req[req:%lu]@[worker:%s]): No Publishing mDNS info - CPPM is Down	This indicates publishing of mDNS info to IF-MAP server(s) is skipped.	
309016	Debug	[func:%s](): Renewing Session to IF-MAP server [[svr:%s]]	This indicates MAPC is renewing the current session to an IF-MAP server.	
309017	Debug	Renew Session to IF-MAP server [[svr:%s]] successfully with SessionId:[sid:%s]	This indicates successfully renew session to an IF-MAP server.	
309100	Debug	PAN-USER-CHANGED: IP=[ip:%s]	This indicates an IP is changed with enabled PAN-Integration.	
309101	Debug	PAN-USER-DELETED: IP=[ip:%s]	This indicates an IP is deleted with enabled PAN-Integration.	
309102	Debug	ACTIVE-PAN-PROF-CHG: Active PAN Profile Changed: from "[old:%s]" to "[new:%s]"	This indicates PAN Active Profile is changed.	
309104	Debug	PAN-PROF-CHG: pan-profile "[old:%s]" is changed"	This indicates PAN Profile is changed.	
309105	Debug	[func:%s](): Starting session to PAN server [[svr:%s]]	This indicates pan module is trying to establish a session to a PAN server.	
309106	Debug	[func:%s](): Stopping session to PAN server [[svr:%s]]	This indicates pan module is trying to tear down a session to a PAN server.	
309107	Debug	PAN-PROF-CHG: PAN Profile [[pname:%s]] is Changed	This indicates a PAN Profile configuration is changed.	
309110	Debug	EndSession to PAN server [[svr:%s]] successfully	This indicates successfully disconnect to a PAN server.	
309111	Debug	[func:%s](req[req:%s]@[worker:%s]): Posting UID:IP-USER for "type:[type:%s] IP:[ip:%s] name:[user:%s] device:[devid:%s]"	This indicates trying to post UID IP-USER mapping to PAN server(s).	
309112	Debug	Successfully Post User-ID Request(req[req:%s]) to PAN server [[svr:%s]] using Conn:[conn:%lu]	This indicates a success to post to a PAN server successfully.	
309114	Debug	[func:%s](): Renewing Session to PAN server [[svr:%s]]	This indicates current session to a PAN server is renewing.	
309115	Debug	Renew Session to PAN server [[svr:%s]] successfully	This indicates successfully renew session to a PAN server.	
309117	Debug	Request(req[req:%s]): Post to PAN server [[svr:%s]] Skipped - Session is Down	This indicates a failure to renew session to a PAN server.	
309118	Debug	Start UID-REFRESH: current-slot:[cslot:%d] refresh-slot:[rslot:%d] total-in-uid-cache:[tuid:%d] total-in-refresh:[tref:%d]	This is an internal debug message.	
309119	Debug	Summary UID-REFRESH: current-slot:[cslot:%d] refresh-slot:[rslot:%d] total-refresh-reqs:[requests:%d] total-refreshed-users:[users:%d] first-refresh-reqId:[fid:%ld] last-refresh-reqId:[eid:%ld]	This is an internal debug message.	
309121	Debug	[func:%s](req[req:%s]@[worker:%s]): Posting MULTIPLE-UID Mappings"	This indicates trying to post Multiple UID IP-USER mappings to PAN server(s).	
309122	Debug	Error([cause:%s]) on Posting User-ID Request(req[req:%s]) to PAN server [[svr:%s]] using Conn:[conn:%lu], tries:[tries:%d]/[max:%d], Retry again!	This indicates a timed out to post UID to a PAN server.	
309127	Debug	PAN-USER-DEACTIVATED: IP=[ip:%s]	This indicates an IP user is deactivated - switch over to other controller in the cluster.	
309128	Debug	PAN-UID-CACHE-UPDATED: IP=[ip:%s]	This indicates an UID-Cache entry is updated.	
309129	Debug	PAN-UID-CACHE-DELETED: IP=[ip:%s]	This indicates an UID-Cache entry is deleted.	
309130	Debug	PAN-UID-CACHE-CLEARED: UID-Cache Table is cleared	This indicates an UID-Cache table is cleared.	
309201	Debug	[func:%s](): Starting session to ClearPass-Insight server [[svr:%s]]	This indicates cpnw module is trying to establish a session to a ClearPass-Insight server.	
309202	Debug	[func:%s](): Stopping session to ClearPass-Insight server [[svr:%s]]	This indicates cpnw module is trying to tear down a session to a ClearPass-Insight server.	
309203	Debug	[func:%s](): Notify DataIsReady for WebSocket connection to server [[svr:%s]]	This indicates cpnw module has data raedy to be sent to a ClearPass-Insight server through WebSocket connection.	
309204	Debug	CPNW-WebSocket-Profile: [str:%s]	This is a cpnw module debugging message.	
309205	Debug	[func:%s](req[req:%s]@[worker:%s]): Subscribing Device-profiling for "mac:[mac:%s]"	This indicates trying to subscribe device-profiling at ClearPass-NetWatch.	
309206	Debug	[func:%s](req[req:%s]): Posting '[partial:%s]' on NwtWatch for [num:%u] Clients"	This indicates trying to subscribe/unsubscibe event at ClearPass-NetWatch.	

309207	Debug	Successfully Post '[partial:%s]' Request(req[req:%s]) with [num:%u] cliens to ClearPass-NetWatch"	This indicates a successful post at ClearPass-NetWatch.	
309208	Debug	Received '[partial:%s]' from ClearPass-NetWatch"	This indicates a message is received from ClearPass-NetWatch.	
309300	Debug	[func:%s](): [msg:%s]	This shows an internal debug message in GP	
309804	Debug	[func:%s](): [msg:%s]	This shows an internal debug message in ExtIntfMgr.	
309815	Debug	[func:%s](): group:"[grp:%s]" group_num:[g_num:%d] instance:"[inst:%s]" id:[id:%d] changed; refs:[refs:%d].	This is extifmgr internal debugging message.	
309816	Debug	[func:%s](): group:"[grp:%s]" instance:"[inst:%s]" deleted.	This is extifmgr internal debugging message.	
309817	Debug	[func:%s](): event:[ev:%d] result:[res:%d].	This is extifmgr internal debugging message.	
309819	Debug	[func:%s](): All config for CPPM IF-MAP profile are received - [[enstr:%s].	This is extifmgr internal debugging message.	
309825	Debug	extifmgr: GSM is initialized.	This is extifmgr internal debugging message.	
309826	Debug	[func:%s](): IP_USER GSM look up failed on IP=[ip:%s], Ignore received GSM-Event:[evtype:%s].	This is extifmgr internal debugging message.	
309827	Debug	[func:%s](): null ip_user. Skip processing	This is extifmgr internal debugging message.	
309828	Debug	[func:%s](): null notification data. Skip processing	This is extifmgr internal debugging message.	
309829	Debug	[func:%s](): Unknown action[act:%d]. Skip processing	This is extifmgr internal debugging message.	
309830	Debug	[func:%s](): PAN-Integration for IP=[ip:%s] is diabled. Skip processing	This is extifmgr internal debugging message.	
309831	Debug	[func:%s](): GSM ip-user channel: event-type=[type:%s]	This is extifmgr internal debugging message.	
309832	Debug	[func:%s](): null ip_key. Skip processing	This is extifmgr internal debugging message.	
309833	Debug	Request(req[req:%s]): No PAN server is configured. Skip processing.	This is extifmgr internal debugging message.	
309835	Debug	[func:%s](): GSM dev-id_cache channel: station=[mac:%s] event-type=[type:%s]	This is extifmgr internal debugging message.	
309836	Debug	[func:%s](): ClearPass-WebSocket Profile Changed: [en:%s] primary '[pi:%s]:[pp:%d]' secondary '[si:%s]:[sp:%d]'	This is extifmgr internal debugging message.	
309837	Debug	Connecting to WebSocket Server '[host:%s]:[port:%d]/[uri:%s]'	This is extifmgr internal debugging message.	
309841	Debug	[func:%s](): Successfully Sent [len:%lu] bytes to WebSocket Server '[host:%s]:[port:%d]/[uri:%s]'	This is extifmgr internal debugging message.	
309843	Debug	[func:%s](): GSM dev_id_cache lookup failed for mac [mac:%s], result:[res:%s]	This indicated failure in looking up dev_id_cache gsn channel.	
309847	Debug	Successfully Set Certificate CA-PATH '[capth:%s]' for WebSocket connection"	This indicates CA-PATH for a SecuredWebSocket Connection is set up successfully.	
309903	Debug	[func:%s](): [str:%s]	This indicates an internal debug message.	
310204	Debug	[msg:%s]	Generic DEBUG level system log	
310304	Debug	[msg:%s]	Generic DEBUG level system log	
310308	Debug	[msg:%s]	Generic DEBUG level system log	
310312	Debug	[msg:%s]	Generic DEBUG level system log	
310316	Debug	[msg:%s]	Generic DEBUG level system log	
310320	Debug	[msg:%s]	Generic DEBUG level system log	
310324	Debug	[msg:%s]	Generic DEBUG level system log	
310328	Debug	[msg:%s]	Generic DEBUG level system log	
310332	Debug	[msg:%s]	Generic DEBUG level system log	
311008	Debug	[msg:%s]		
311009	Debug	[msg:%s]		
311025	Debug	[msg:%s]		
312004	Debug	[str:%s]	Generic system debug message	
312106	Debug	Decoding ESI message [msg:%s]		
312303	Debug	[func:%s], [msg:%s]		
312400	Debug	[msg:%s]		
312503	Debug	[func:%s], [msg:%s]		
312601	Debug	[msg:%s]	CTB Agent Debug Message.	
313000	Debug	Processing Link State Change on [intIfNum:%d] event [event:%s]	To be filled out	
313005	Debug	Added Interface [intIfNum:%d] with vlanid [vlanid:%d] to STP instance [instanceID:%d]	To be filled out	
313006	Debug	Created STP instance [instanceID:%d]	To be filled out	
313007	Debug	Removed all VLANs from STP instance [instanceID:%d]	To be filled out	

313008	Debug	Added VLAN [id:%d] to STP instance [instanceID:%d]	To be filled out	
313009	Debug	Deleted VLAN [id:%d] from STP instance [instanceID:%d]	To be filled out	
313010	Debug	Interface [intIfNum:%d] moved from Vlan [oldvid:%d] Instance [oldInstance:%d] to new VLAN [newvid:%d] Instance [newinst:%d]	To be filled out	
313013	Debug	Configuring Vlan [vlanID:%d]	System is configuring a VLAN	
313018	Debug	Request to modify Vlan [vlanID:%d]	To be filled out	
313031	Debug	TunnelId [tunnelId:0x%x] is not Present in the Vlan Interface		
313040	Debug	Changing native vlan for port [prt:%d] oldVid is [oldVid:%d] New vid is [vId:%d]	To be filled out	
313046	Debug	Building Default Vlan Config Data		
313047	Debug	Initializing the dot1q structure		
313048	Debug	Initializing the Vlan Data Tree From Configuration Data		
313049	Debug	Deleting the Vlan [vlanID:%d] config entry [entry:%d]	To be filled out	
313050	Debug	Resetting the params for port [intfNum:%d]	To be filled out	
313058	Debug	Processing VLAN change Event [event:%s] for Vlan [vlanId:%d] Interface Number is [intIfNum:%d]	To be filled out	
313077	Debug	XSec Port is added to Vlan [vid:%d]	To be filled out	
313079	Debug	XSec Port is Removed From Vlan [vlanId:%d]	To be filled out	
313095	Debug	Interface [intIfNum:%d] is not a LAG member	To be filled out	
313112	Debug	Port-channel task starts successfully.		
313114	Debug	Invalid AMAP advertisement received, wrong length [wlen:%d], expected length [len:%zu]	To be filled out	
313117	Debug	Unable to get Interface id for vlan [vid:%d]	To be filled out	
313126	Debug	[func_name:%s]: Initialization successful		
313146	Debug	IPMAP Received the Event [event:%s] for Interface [if_num:%d]	To be filled out	
313158	Debug	Processing the Tunnel List for Vlan IP Add		
313160	Debug	Removing Ip [ipAddress:%s] address from Sibyte for interface [if_num:%d]		
313161	Debug	[func_name:%s]: Removed IP Address from OS		
313162	Debug	Processing the Tunnel List for IP Delete		
313163	Debug	Disabling the Routing mode for vlan Id [vlanId:%d]		
313166	Debug	Creating the Vlan in Kernel [vlanId:%d]	To be filled out	
313214	Debug	PPPoE: pppoed pid=[pi:%d] died		
313219	Debug	PPPoE: pppoed started: pid: [pppoed_pid:%d]		
313244	Debug	Could not find [ipAddr:%s] in IP lookup table after		
313247	Debug	Adding route for ip 0x[router:%x] intf 0x[intIfNum:%x]	System is inserting a route in the database	
313252	Debug	Adding a duplicate Route	System ignored request to add a duplicate route	
313254	Debug	Callback for RTO_ADD_ROUTE is being called		
313257	Debug	Resolved the Route to Interface number 0x[intIfNum:%x]		
313292	Debug	Adding IPv6 route for ip [router:%s] intf 0x[intIfNum:%x]	System is inserting a route in the database	
313297	Debug	Adding a duplicate Ipv6 route	System ignored request to add a duplicate route	
313299	Debug	Callback for RTO6_ADD_ROUTE is being called		
313302	Debug	Resolved the Ipv6 route to Interface number 0x[intIfNum:%x]		
313329	Debug	VRRP: Sending Advertisement for vrid [vrid:%d] at [sec:%x] second [ns:%x] nanosecond	System is sending VRRP advertisement for the specified VRID	
313333	Debug	VRRP: vrid "[vrid:%d]"(Master) - Received VRRP Advertisement with LOWER PRIORITY ([prio:%d]) from [ipaddr:%s], ignoring.	Warning indicating that the VRRP Master received Advertisement with lower priority which is ignored	
313334	Debug	VRRP: Received advertisement for vrid [vrid:%d] at [sec:%x] second [ns:%x] nanosecond	System is receiving VRRP advertisement for the specified VRID	
313335	Debug	VRRP ipv6: Received advertisement for vrid [vrid:%d] at [sec:%x] second [ns:%x] nanosecond	System is receiving VRRPV6 advertisement for the specified VRID	
313339	Debug	The card [slotNum:%d] is reinsertedn		
313348	Debug	DTL Sending Event [event:%s] for Interface [slot:%d]/[port:%d]n		
313353	Debug	Calling dtlCardInit function for slot [slotNum:%d]n		
313361	Debug	Received a card removed event - Purge the Interface tablen	A card has been removed	
313365	Debug	Creating the PHY Interface slot [slot:%d] port [port:%d]n		

313368	Debug	Nim Notifying Event [event:%d] for Interface [intIfNum:%d]n		
313369	Debug	Sending a Notification to the NIM Layer about Event [event:%s] for interface [interface:%d]		
313375	Debug	Retrieved interface Speed is [speedStatus:%d]n		
313394	Debug	Sending the Vlan [state:%s] for vlan Id [vlanId:%d]n		
313395	Debug	Sending the Physical Port [state:%s] trap for [port:%s]n		
313403	Debug	slot [slot:%d] port [port:%d], card is re-inserted, Ports are already created for this slot.		
313430	Debug	Initializing the slot [slot:%d] with cardID [cardId:%d] num of ports [numPorts:%d]		
313431	Debug	Card is Re-Inserted in the slot [slot:%d] ID [cardId:%d]n		
313432	Debug	Nim Layer is processing event [event:%s] for interface [slot:%d]/[port:%d]		
313433	Debug	Nim Received the event [event:%s] for interface [interface:%d]		
313435	Debug	Not changing the state of the VLAN. This is a switch ip vlan.		
313436	Debug	Error receiving PDU. Invalid usp [slot:%d]/[port:%d]		
313439	Debug	Port-Channel, State of the interface [iface:%d] changed to [state:%s]		
313442	Debug	Heartbeat sent on tunnel [tunId:%d] with srcip [srcIp:%s] dstip [dstIp:%s]	This message indicates that a heartbeat message has been sent on the tunnel	
313444	Debug	Heartbeat reply received on tunnel [tunId:%d] with srcip [srcIp:%s] dstip [dstIp:%s]	This message indicates that a heartbeat reply message has arrived	
313448	Debug	VRRP Tracking: vr [vid:%d] vlanid [vlanid:%d] trk value is [trkval:%d]		
313449	Debug	VRRP Tracking: vr [vid:%d] intfNumber [intfNum:%d] trk value is [trkval:%d]		
313450	Debug	VRRP Tracking: intfNumber [intfNum:%d] event is [event:%d]		
313456	Debug	PPP: pppd started for tty: [tty:%s]	PPP Daemon was successfully started	
313458	Debug	Route add failed on reload for [dst:%s] [gw:%s] with errno [errno:%d]		
313460	Debug	Fpapps config download still in progress, restarting route add retry timer		
313461	Debug	Attempting to add failed IPv4 routes on reload again to kernel		
313462	Debug	Attempting to add failed IPv6 routes on reload again to kernel		
313463	Debug	Error on removing IPv4 route object [route:%p] from [list:%p]		
313464	Debug	Error on removing IPv6 route object [route:%p] from [list:%p]		
313492	Debug	Route(s) add failed on reload: Retry timer started for [sec:%d] seconds		
313507	Debug	Uplink: [statusStr:%s]	This syslog is used for tracking the progress of uplink manager	
313508	Debug	Started the VRRP preempt delay timer for VRID [id:%d]	Started the VRRP preemption delay timer	
313509	Debug	VRRP Preempt delay timer expired for VRID [id:%d]	VRRP preemption delay timer expired	
313525	Debug	USB device [usb : %s] removed. Waiting for phytask to do the cleanup	PPP device removed	
313526	Debug	PPP process died [pid : %d]	PPP device died	
313609	Debug	VRRP ipv6: Sending Advertisement for vrid [vrid:%d] at [sec:%x] second [ns:%x] nanosecond	System is sending VRRP advertisement for the specified VRID	
313610	Debug	Started the VRRP IPv6 preempt delay timer for VRID [id:%d]	Started the VRRP preemption delay timer	
313611	Debug	VRRP IPv6 Preempt delay timer expired for VRID [id:%d]	VRRP preemption delay timer expired	
313620	Debug	VRRP ipv6: vrid "[vrid:%d]"(Master) - Received VRRP Advertisement with LOWER PRIORITY ([prio:%d]) from [ipaddr:%s], ignoring.	Warning indicating that the VRRP Master received Advertisement with lower priority which is ignored	
313621	Debug	VRRP IPv6 Tracking: vr [vid:%d] vlanid [vlanid:%d] trk value is [trkval:%d]		
313622	Debug	VRRP IPv6 Tracking: vr [vid:%d] intfNumber [intfNum:%d] trk value is [trkval:%d]		
313623	Debug	Function [function:%s] Line [line: %d]: [dbgmsg:%s]	Generic L2/L3 System debug message	
313633	Debug	VRRP IPv6 Tracking: intfNumber [intfNum:%d] event is [event:%d]		
313636	Debug	NAS COA VRRP IPv4: vrid [vrid:%d] Received [action:%s] message from cluster_mgr for vlanid [vlanid:%d] IP addr [ipaddr:%s] priority [prio:%d]	NAS COA VRRP debug information	
313637	Debug	NAS COA VRRP IPv6: vrid [vrid:%d] Received [action:%s] message from cluster_mgr for vlanid [vlanid:%d] IP addr [ipaddr:%s] priority [prio:%d]	NAS COA VRRP debug information	
313641	Debug	[func:%s]: [msg:%s]	Fpapps Amon debug information	
314814	Debug	POE for slot [slot:%d] in [state:%x]	NA	

315383	Debug	Acl Info message timed out for acl [name:%s]	Process Fpapps timed out trying to get the ACL information from Auth manager. This typically happens at initialization. Auth Manager, after its successful initialization will inform fpapps about the ACL.	
315386	Debug	[state:%s] Tunnel [tunnel:%d], I/f IP:[ip:%s], src:[srcIP:%s], dest:[dstIp:%s], type:[type:%x]n	Operation failed when trying to configure Tunnel source IPv6 with vlan i/f IPv6	
316008	Debug	Update Device-LC-List mapping for '[mac:%s]/[ip:%s] hostname:[name:%s] status:[st:%d]'	This indicates LC-Map needs be updated due to changes in device_lclist gsm channel	
316010	Debug	Delete Device-LC-List mapping for '[mac:%s]'	This indicates LC-Map entry needs be deleted due to deletion in device_lclist gsm channel	
316027	Debug	Sending message to Sysmapper of type=[type:%d]	To be filled out	
316028	Debug	Sending message to Probe: IP:[ip:%s] Msg-Type:[type:%s]	To be filled out	
316029	Debug	Sending message to Probe: IP:[ip:%s] Msg-Type:[msg_type:%s] AP [bssid:%m] Type:[type:%d]	To be filled out	
316030	Debug	Sending message to Probe: IP:[ip:%s] Msg-Type:[msg_type:%s] STA [mac:%m] RSTA Type:[type:%d] Valid-exempt:[ve:%s]	To be filled out	
316031	Debug	STA Probe: [op:%s] STA [mac:%m]	To be filled out	
316032	Debug	STA Probe: [op:%s] Probe [bssid:%m] for STA [mac:%m]	To be filled out	
316033	Debug	STA Probe: Removing Probe [bssid:%m]	To be filled out	
316034	Debug	Adding STA state tree node Monitor [mon_mac:%m] MAC [mac:%m] phy-num [phy_num:%d]	To be filled out	
316035	Debug	Deleting STA state tree node Monitor [mon_mac:%m] MAC [mac:%m] phy-num [phy_num:%d]	To be filled out	
316036	Debug	Received New STA Message: MAC [mac:%m] Status [status:%d]	To be filled out	
316037	Debug	AP not found for STA [mac:%s] AP [bssid:%s]	To be filled out	
316038	Debug	Config RSTA Type for STA [mac:%m] Rsta-type [rsta_type:%d] DB-Id [db_id:%d]	To be filled out	
316039	Debug	Setting RSTA Type for STA [mac:%m] from [old_rsta_type:%d] to [new_rsta_type:%d]	To be filled out	
316051	Debug	Sending probe-poll for Probe [mac:%m] IP [ip:%s]	To be filled out	
316052	Debug	Set Status for Probe [mac:%s] Old [old:%d] New [new:%d]	To be filled out	
316067	Debug	MAX Entries reached. Skipping node: [type:%s] MAC:[mac:%s] Monitor:[monitor_mac:%s]	To be filled out	
316071	Debug	Adding AP state tree node Monitor [mon_mac:%m] BSSID [bssid:%m] phy-num [phy_num:%d]	To be filled out	
316072	Debug	Deleting AP state tree node Monitor [mon_mac:%m] BSSID [bssid:%m] phy-num [phy_num:%d]	To be filled out	
316073	Debug	Received New AP Message: AP [bssid:%m] Status [status:%d] Num-WM [wm:%d]	To be filled out	
316074	Debug	SAP Register: Set Status for AP [bssid:%s] IP [ip:%s] Status [status:%d]	To be filled out	
316075	Debug	Set Status for AP [bssid:%s] Status [status:%d]	To be filled out	
316083	Debug	sql: [command:%s]	To be filled out	
316094	Debug	Could not create entry for station [mac:%m]	To be filled out	
316097	Debug	Sending notification to MMS to update RSSI for Monitor [monitor_mac:%m] [node_type:%s] [mac:%m] Old [old_val:%d] New [new_val:%d]	To be filled out	
316107	Debug	Dropping message [msg_name:%s] from Sysmapper	To be filled out	
316112	Debug	Handle SAP Down: Probe BSSID [bssid:%m]	To be filled out	
316200	Debug	Station [mac:%m] Phy [phy_type:%d] extracted from SNMP tree for Monitor [mon:%m] not found in table.	To be filled out	
316201	Debug	AP [bssid:%m] Phy [phy_type:%d] extracted from SNMP tree for Monitor [mon:%m] not found in table.	To be filled out	
316203	Debug	Set Configuration: Key=[key:%s] Value=[value:%s]	To be filled out	
316204	Debug	Get Configuration: Key=[key:%s]	To be filled out	
316205	Debug	Command: Name=[name:%s] Key=[key:%s] Value=[value:%s]	To be filled out	

316206	Debug	Show Command Received: Objtype=[type:%d]	To be filled out	
316207	Debug	Buf: [buf:%s]	To be filled out	
316210	Debug	SNMP Request [table:%s]: End of table condition	To be filled out	
316211	Debug	SNMP Request GET NEXT [table:%s]: Monitor [mon_mac:%m] AP [bssid:%m] Phy-num [phy_num:%d]	To be filled out	
316212	Debug	SNMP Request GET NEXT [table:%s]: Monitor [mon_mac:%m] STA [mac:%m] Phy-num [phy_num:%d]	To be filled out	
316213	Debug	SNMP Request GET NEXT EventTable: Event-ID [id:%d]	To be filled out	
316233	Debug	ct_fetch(): mac found [mac:%s] rows [row:%d]	To be filled out	
316235	Debug	Ageing AP Stats tree node Monitor [mon_mac:%m] BSSID [bssid:%m] Phy-num [phy_num:%d]	To be filled out	
316236	Debug	Ageing STA Stats tree node Monitor [mon_mac:%m] MAC [mac:%m] Phy-num [phy_num:%d]	To be filled out	
316237	Debug	Ageing Channel Stats tree node Monitor [mon_mac:%m] Channel [ch:%d]	To be filled out	
316238	Debug	Adding AP Stats tree node Monitor [mon_mac:%m] BSSID [bssid:%m] Phy-num [phy_num:%d]	To be filled out	
316239	Debug	Adding STA Stats tree node Monitor [mon_mac:%m] MAC [mac:%m] Phy-num [phy_num:%d]	To be filled out	
316240	Debug	Processing Stats-Update-Message from Probe [bssid:%m] Length [len:%zu]	To be filled out	
316246	Debug	test desc	To be filled out	
316268	Debug	Sending msg to mgmt-server [ip:%pI4] #wms_ap_info:[ap_info:%d] #wms_ap_stats:[ap_stats:%d] #wms_sta_info:[sta_info:%d] #wms_sta_stats:[sta_stats:%d]	This log displays a record of the transmission of the AMON message to the amp management server. It includes statistics regarding the number of transmitted WMS records.	
316269	Debug	Sending msg to HTTP mgmt-server [protocol:%s] [hostname:%s] [port:%d] [identifier:%s] #wms_ap_info:[ap_info:%d] #wms_ap_stats:[ap_stats:%d] #wms_sta_info:[sta_info:%d] #wms_sta_stats:[sta_stats:%d]	This log displays a record of the transmission of the AMON message to the http management server. It includes statistics regarding the number of transmitted WMS records.	
316270	Debug	Adding [type:%s] records, count [num_records:%d]	This log indicates the number of records of certain type added to the AMON message buffer.	
316271	Debug	Sent a total of [num_records:%d] [type:%s] records	This log indicates the total number of records of certain type sent to the management server.	
316272	Debug	MON_STA_INFO [func:%s]:[line:%d]: operation:[op:%d] sta_mac:[mac:%s] assoc_bssid:[bssid:%s] ht_type:[ht:%d] rsta_type:[rt:%d] phy_type:[pt:%d] is_ap:[ap:%d] status:[st:%d] channel:[ch:%d] ht_secondary_channel[ht_sec:%d] authenticated:[auth:%d]	WMS AMON generic debug message for MON_STA_INFO msg to be only used for debugging/private builds.	
316273	Debug	MON_AP_INFO [func:%s]:[line:%d]: operation:[op:%d] ap_bssid:[mac:%s] rap_type:[rt:%u] conf_lvl:[cl:%d] chan:[ch:%d] essid:[ssid:%s] encryption:[encr:%d] ibss:[ibss:%d] phy_type:[pt:%d] ht_type:[ht:%d] pri/sec chan:[pc:%d]/[sc:%d] type:[type:%d] status:[stat:%d] dos_enabled:[dos:%d] monitor_mac:[mon:%s] phy_num:[phy_num:%d]	WMS AMON generic debug message for MON_AP_INFO msg to be only used for debugging/private builds.	
316275	Debug	WIDS_EVENT_INFO [func:%s]:[line:%d]: sta_mac:[mac:%s] event_type:[et:%d] event_info:[info:%s] trap_id:[trap:%d]	WMS AMON generic debug message for WIDS_EVENT_INFO msg to be only used for debugging/private builds.	
316276	Debug	MON_ROGUE_AP_INFO [func:%s]:[line:%d]: rogue_ap_bssid:[mac:%s] rap_type:[rt:%d] conf_lvl:[cl:%d] match_mac:[mmac:%s] match_type:[mtype:%d] match_method:[mm:%d] match_ap_name:[name:%s] match_helper_ap_bssid:[hb:%s] match_time:[mt:%d]	WMS AMON generic debug message for MON_ROGUE_AP_INFO msg to be only used for debugging/private builds.	
316277	Debug	MON_AP_DEL [func:%s]:[line:%d]: ap_bssid:[mac:%s]	WMS AMON generic debug message for MON_AP_DEL msg to be only used for debugging/private builds.	
316278	Debug	MON_STA_DEL [func:%s]:[line:%d]: sta_mac:[mac:%s]	WMS AMON generic debug message for MON_STA_DEL msg to be only used for debugging/private builds.	

316280	Debug	STA [mac:%m] was [op:%s] the valid-exempt list.	Station was added to or removed from the valid-exempt list. Stations in the valid-exempt list are exempt from Valid Station Protection.	
316281	Debug	STA [mac:%m] was not added to the valid-exempt list. The list size has reached the limit: [max:%d].	Station was not added to the valid-exempt list due to the list reaching the max size.	
316288	Debug	Received New AP Message from LC [name:%s]-[ip:%s] : AP [bssid:%m] Status [status:%d]	Received New AP Message from LC	
316289	Debug	Received New STA Message from LC [name:%s]-[ip:%s] : MAC [mac:%m] Status [status:%d]	Received New STA Message from LC	
316306	Debug	SQL Command "[command:%s]" failed. Reason: [reason:%s]	To be filled out	
317000	Debug	ntpdwrap got signal [sig:%d] from pid [pid:%d], status [status:%d], errno [errno:%d]	ntpwrap received child exited signal signal, dumps error code	
317006	Debug	[str:%s]	NTP generic debug message	
319003	Debug	[msg:%s]	System related debugging messages logged in the station manager (arm).	
322001	Debug	[msg:%s]		
323002	Debug	[msg:%s]		
325029	Debug	Internal VLAN 4095 received	This shows an internal debug message	
325030	Debug	aaa_profile not found. aaa_prof = [authprofile:%s]	This shows an internal debug message	
326001	Debug	AM: [msg:%s]		
326076	Debug	AM: Sending Probe Poll Response V2: NumAPs=[num_aps:%d] NumSTAs=[num_sta:%d] Len=[bl:%d]	To be filled out	
326081	Debug	AM: Processing WMS_MODE message	To be filled out	
326086	Debug	AM: Sending Probe Register Message to : [ip:%s]	To be filled out	
326087	Debug	AM: Sending Probe UnRegister Message to : [ip:%s]	To be filled out	
326090	Debug	AM: message len [node_bl:%d]	To be filled out	
326092	Debug	AM: [line:%d]: Sending PROBE_STATS_UPDATE_MESSAGE for STAs of length [bl:%d]	To be filled out	
326093	Debug	AM: [line:%d]: Sending STM_AP_STATS_UPDATE for STAs of length [bl:%d]	To be filled out	
326094	Debug	AM:SM: Sending Spectrum Register Message for radio [r:%d] band [band:%s] to [ip:%s]	This log indicates that spectrum radio is registering with the controller.	
326095	Debug	AM:SM: Sending Spectrum Unregister Message for radio [r:%d] band [band:%s] to [ip:%s]	This log indicates that spectrum radio is un-registering with the controller.	
326099	Debug	AM:SM: Received Spectrum Unknown Radio Message for [bssid:%s]	This log indicates that AP not find spectrum radio, so sending unknown radio msg.	
326100	Debug	AM: Sending Probe Poll Response for unclassified devices: NumAPs=[num_aps:%d] NumSTAs=[num_sta:%d] Len=[bl:%d]	To be filled out	
326213	Debug	AM: MAC [mac:%s] matched with offset [match:%s]	To be filled out	
326216	Debug	AM: MAC [mac:%s] matched in [config_eth:%s] wired mac table	To be filled out	
326280	Debug	AM:SM: [msg:%s]		
326283	Debug	AM: [line:%d]: Sending STM_AP_ENET_STATS_UPDATE of length [bl:%d]	To be filled out	
330001	Debug	[msg:%s]		
330105	Debug	Error sending message to service [svc:%d]	An internal communication error occurred while sending a message	
330200	Debug	[msg:%s]	To_be_filled_out	
334000	Debug	[msg:%s]		
334008	Debug	[msg:%s]	Logs regarding downloadable regulatory table	
334009	Debug	Device add requested for MAC [mac:%s] model [model:%s] cfg path [path:%s]	Configuration device add request received with MAC address, device model and config-path	
334014	Debug	Profmgr GSM device remove requested for [mac:%s]	Profile Manager device config object remove requested.	
334025	Debug	Config file [filename:%s] created	Profile Manager generated config file following a "write mem" or "get full-config" request.	
334100	Debug	[msg:%s]		
334101	Debug	[msg:%s]		

334208	Debug	PhoneHome Transaction type [tt:%s] report type [rt:%s] finite state machine event [event:%s]: current: [curstate:%s], next: [nextstate:%s]	PhoneHome state machine debugging	
334213	Debug	PhoneHome successfully transported transaction type [tt:%s] report type [rt:%s], ID [tid:%s]	PhoneHome is deleting successfully uploaded transaction	
334216	Debug	PhoneHome Child thread handling post of transaction type [tt:%s] report type [rt:%s], previous state [ps:%s] current state [cs:%s], status [st:%d]	PhoneHome spwaning child process to deal with transaction posting	
334217	Debug	PhoneHome parent thread waiting for completion of transaction type [tt:%s] report type [rt:%s], previous state [ps:%s] current state [cs:%s], waitstatus [st:%d]	PhoneHome parent process waiting for completion of transaction posting by child	
334218	Debug	PhoneHome creating thread to deal with transaction type [tt:%s] report type [rt:%s], previous state [ps:%s] current state [cs:%s] posting, thread creation status [st:%d]		
334219	Debug	PhoneHome skipping auto-report due to invalid config filename		
334220	Debug	PhoneHome skipping auto-report due to invalid config size		
334222	Debug	PhoneHome debug info [fn:%s] [ln:%d] message [rs:%s]		
334223	Debug	PhoneHome skipping auto-report due to invalid SMTP or HTTPS configuration		
334224	Debug	PhoneHome skipping manual-report due to invalid SMTP or HTTPS configuration		
334225	Debug	PhoneHome DNS resolution Error. Please check the DNS settings.		
334226	Debug	PhoneHome failed signing the challenge string. Returning error for transaction with transaction type [tt:%s] report type [rt:%s] ID [tid:%s].		
334227	Debug	Error Converting the device certificate to PEM format in [file:%s] at [func:%s], [line:%d] . PhoneHome with abort communication with activate server.		
334228	Debug	Error posting command to Activate using CURL in transaction ID [tid:%s] at [file:%s] at [func:%s], [line:%d]. PhoneHome with abort communication with activate server.		
334229	Debug	PhoneHome starting file chunks upload for transaction type [tt:%s] report type [rt:%s], ID [tid:%s]		
334231	Debug	Sending chunk number [ctr:%d] in transaction ID [tid:%s] [msg:%s]		
334232	Debug	Received challenge string [chal:%s] from Activate for transaction ID [tid:%s]. Signing and sending for authentication...		
334233	Debug	Authentication with Activate for transaction ID [tid:%s] [msg:%s]		
334234	Debug	Transaction ID [tid:%s], type [posttype: %s] received error from activate with response code [rcode:%d] and status message [scode:%s]		
334235	Debug	Transaction ID [tid:%s], type [posttype: %s] was successful with response code [rcode:%d] and status message [scode:%s]		
334236	Debug	Initiating transaction type [posttype: %s] with Transaction ID [tid:%s]		
334237	Debug	phm-lite Webcc report interval was set to [interval: %d]		
334305	Debug	[msg:%s]		
334306	Debug	[func:%s]: [msg:%s]		
334501	Debug	PAPI_Send() failed for opcode [opcode:0x%x] [__FUNCTION:%s]		
334553	Debug	[__FUNCTION:%s]: TnlIntf is not there		
334554	Debug	[__FUNCTION:%s]: vlanIntf is not there for vlan [vlan_id:%d]		
334557	Debug	[__FUNCTION:%s]: Intf is not there for src IP [src_ip:%s]		
334558	Debug	[__FUNCTION:%s]: recvfrom len is invalid		
334559	Debug	[__FUNCTION:%s]: recvfrom failed with err [err:%d]		
335006	Debug	Received Heart beat Response from Peer M3 slot [slot:%d], Total number of received HB [rcv:%d], total number of sent HB [sent:%d], outstanding HB [out:%d]	Heartbeat stats when we received the HB	
335007	Debug	Received a Backplane Heartbeat Message from [slot:%d]	Received a HB message	
335014	Debug	ECC write error,could not open file [file : %s].	ECC write error.	
335105	Debug	[msg:%s]		
335106	Debug	[func:%s], [msg:%s]		

335304	Debug	[__FUNCTION:%s]: vlanIntf cannot be created for vlan [vlan_id:%d]		
335501	Debug	[str:%s]	DHCP generic debug message	
335502	Debug	DHCP-RELAY GSM initialization successful.	DHCP-RELAY GSM initialization successful.	
336005	Debug	[msg:%s]		
336006	Debug	[func:%s]: [msg:%s]		
337000	Debug	[msg:%s]		
338000	Debug	EV_LIB: [msg: %s]	Internal debugging message	
338100	Debug	EV_LIB: [msg: %s]	Internal debugging message	
338200	Debug	[str:%s]	RESOLVE generic debug message	
339305	Debug	[msg:%s]		
339306	Debug	[func:%s], [msg:%s]		
341001	Debug	[msg:%s]		
341022	Debug	AP can't retrieve data from datapath for session [ipaddr:%s] - [dipaddr:%s].	The AP is configuring ACL.	
341024	Debug	Setting global LED mode [mode:%d].	The AP is configuring LED mode.	
341025	Debug	Setting virtual controller key [key:%s].	The AP is configuring VC key.	
341124	Debug	[func:%s]: machine auth token client number-[num:%d].	Station update.	
341125	Debug	[func:%s]: add reauth ctx client-[num:%d].	Station update.	
341126	Debug	User: [user:%s] login by [type:%s] [result:%s].	User login.	
341127	Debug	[func:%s], [line:%d]: flushing ACL rule-[profile:%s].	AP is setting SSID.	
341133	Debug	Find AP-[ip:%s] fail, not in vc database.	AP is not in VC database.	
341137	Debug	Client [mac:%s] was removed.	AP remove client when timeout.	
341138	Debug	Conductor received alerts message from AP [ap_ip:%s].	AP receive user alert.	
341142	Debug	[func:%s], [line:%d]: html msg is [msg:%s].	AP receives HTML message from controller.	
341197	Debug	Send [msg:%s] to vc [ip:%s], length [len:%d].	Send register/heartbeat msg to vc.	
341198	Debug	[func:%s]: receive register/heartbeat from [mac:%m], [ip:%s].	Receive register/heartbeat msg from slave.	
341200	Debug	Check session id fail: client_ip [ip:%s], string [sid:%s].	Checking session id fail	
341234	Debug	Receive stats publish from [ip:%s].	Receive stats publish msg	
341236	Debug	Add [mac:%s] [status:%s] to subscription ap list.	Add ap to subscription ap list	
341237	Debug	Del [mac:%s] [status:%s] from subscription ap list.	Del ap from subscription ap list	
341238	Debug	Update [mac:%s] [status:%s] - [newstatus:%s] in subscription ap list.	Update ap status in subscription ap list	
341239	Debug	Del [mac:%s] [status:%s] from subscription ap list in timer.	Del ap from subscription ap list in timer	
341240	Debug	Del [mac:%s] from allowlist ap for not in subscription ap list.	Del ap from whitelist ap for not in subscription ap list	
341241	Debug	Del [mac:%s] from allowlist ap in case of [status:%s].	Del ap from whitelist ap in case of invalid status	
341242	Debug	Ap [mac:%s] has invalid subscription status [status:%d] in function[function:%s] [line:%d] .	ap has invalid subscription status	
341243	Debug	Reboot ap [mac:%s] for not in subscription ap list.	reboot ap for not in subscription ap list	
341244	Debug	Reboot ap [mac:%s] for invalid subscription status [status:%s] in function[function:%s] [line:%d] .	reboot ap for invalid subscription status	
341246	Debug	VC set delta configuration current_cfg_id [cid:%d] top_cfg_id [tid:%d].	new master set its own celta cfg id	
341247	Debug	VC need shrink delta configuration entrys. current_cfg_id [cid:%d] top_cfg_id [tid:%d] max [mid:%d]	VC need shrink delta configuration entrys	
341248	Debug	VC delta configuration entry list is empty.	VC delta configuration entry list is empty.	
341249	Debug	VC delete delta configuration cfg_id [cid:%d] in shrink operation. current_cfg_id [ccid:%d] top_cfg_id [tid:%d]	VC delete delta configuration entry in shrink operation	
341253	Debug	VC send delta configurations to ap. ap [ap_ip:%s] ap_cfg_id [acid:%d] delta_cfg_id [did:%d] current_cfg_id [cid:%d] top_cfg_id [tid:%d]	VC send delta configuration to ap.	
341255	Debug	VC need send delta configurations to ap [ap_ip:%s]. ap_cg_id [acid:%d] current_cfg_id [cid:%d] top_cfg_id [tid:%d].	VC need send delta configurations to ap.	
341256	Debug	AP receive delta configuration id [acid:%d] current_cfg_id [cid:%d] from msg [msg:%s] .	AP receive delta configuration id from msg.	
341257	Debug	VC delete delta configuration cfg_id [cid:%d] in timer operation. current_cfg_id [ccid:%d] top_cfg_id [tid:%d] timestamp [t:%u] current_time [ct:%u]	AP receive delta configuration id from msg.	
341259	Debug	Forming the Register Request message [Func:%s] - [Register:%s] .	Register Request Message	
341277	Debug	managed mode: Starts fetching configuration from the server.	Starts fetching configuration from the server.	

341278	Debug	managed mode: Configuration download done. File hash before [csum1:%s], after [csum2:%s]	Configuration file downloaded from the server.	
341280	Debug	managed mode: Configuration on AP and server matches.	Configuration on AP matches with the config on server.	
341281	Debug	managed mode: AP and server configuration differs.	AP and server configuration differs.	
341291	Debug	[msg:%s]	No per ap setting is present.	
341300	Debug	ale: access point op [op:%s], ap's mac [mac:%s], ap's name [name:%s], ap's model [model:%s], ap's deploy mode [depl_mode:%d], ap's ip [ip:%s].	access point op .	
341305	Debug	ale: report vap op [op:%s], bssid [bssid:%s], ssid [ssid:%s], radio [radio:%s].	report vap info.	
341306	Debug	Send MGMT CMD accounting user-[user:%s],line-[line:%s], cmd-[cmd:%s].	Send MGMT command accounting.	
341308	Debug	receive allowed ap check from asap, mac [mac:%m], allowed [allow:%d].	Receive allowed ap check from asap	
341309	Debug	ale: rssi: isap [isap:%d], raido_mac [radio_mac:%s], radio [radio:%d], mac [mac:%s], rssi [rssi:%d], associate [associate:%d] noise [noise:%d] receive time [receive_time:%d].	print rssi info.	
341310	Debug	ale: [op:%s] station: mac [mac:%s], bssid [bssid:%s].	print deleted station info.	
341311	Debug	ale: [op:%s] station: mac [mac:%s], username [username:%s], role [role:%s], bssid [bssid:%s], os [os:%s], ip [ip:%s].	print station info except delete.	
341312	Debug	ale: [op:%s] radio: mac [mac:%s].	print delete radio info.	
341313	Debug	ale: [op:%s] radio: mac [mac:%s], phy type [phy:%d], mode [mode:%d].	print radio info.	
341314	Debug	ale: [op:%s] vap: bssid [bssid:%s].	print delete vap info.	
341327	Debug	[func:%s]: recv am rssi report to central, msglen-[len:%d],	CLI receive rssi from AM.	
341332	Debug	[msg:%s]	netlink debug message	
342005	Debug	[msg:%s]		
342006	Debug	[func:%s], [msg:%s]		
343002	Debug	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related debugging messages logged in the mDNS proxy (mdns)	
343003	Debug	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related debugging parse messages logged in the mDNS proxy (mdns)	
343004	Debug	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related debugging configuration messages logged in the mDNS proxy (mdns)	
343008	Debug	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related debugging app validation messages logged in the mDNS proxy (mdns)	
343500	Debug	[func:%s] [line:%d] [msg:%s]	System related debug logged in AirGroup	
343506	Debug	[func:%s] [line:%d] [msg:%s]	System related debug messages logged in AirGroup	
343507	Debug	[func:%s] [line:%d] [msg:%s]	System related debug configuration messages logged in AirGroup	
343508	Debug	[func:%s] [line:%d] [msg:%s]	System related debugging app validation messages logged in AirGroup	
343509	Debug	[func:%s] [line:%d] [msg:%s]	System related debug OFC flow manager messages logged in AirGroup	
344002	Debug	([func:%s] [line:%d]) [msg:%s]	System related debugging messages logged in DDS	
345305	Debug	[msg:%s]		
345306	Debug	[func:%s], [msg:%s]		
346002	Debug	([func:%s] [line:%d]) [msg:%s]	System related debugging messages logged in HA_MGR	
346003	Debug	([func:%s] [line:%d]) [msg:%s]	System related debugging parse messages logged in HA_MGR	
346004	Debug	([func:%s] [line:%d]) [msg:%s]	System related debugging configuration messages logged in HA_MGR	
346008	Debug	[AP: %s] ([func:%s] [line:%d]) [msg:%s]	System related AP debugs logged in HA_MGR	
346009	Debug	([func:%s] [line:%d]) [msg:%s]	System related GSM debugs logged in HA_MGR	
347003	Debug	[msg:%s]	System related debugging messages logged in UCM.	
347009	Debug	[msg:%s]	System related debugging messages logged in the station manager (stm).	
348305	Debug	[msg:%s]		
348306	Debug	[func:%s], [msg:%s]		
350005	Debug	[[file:%s]:[line:%d]] [message:%s]	httpd wrap's module's debug message	
351017	Debug	Function: [function:%s] GSM port info event for port [port:%d]	NA	

351018	Debug	Function: [function:%s] GSM lldp info event for port [port:%d]	NA	
351019	Debug	Function: [function:%s] GSM chassis info event	NA	
351020	Debug	Function: [function:%s] LLDP link down event for port [id:%d]	NA	
351021	Debug	Function: [function:%s] LLDP link up event for port [id:%d]	NA	
351023	Debug	[str:%s]	LLDP generic debug message	
351024	Debug	Function: [function:%s] LLDP AMON log [str:%s]	NA	
354002	Debug	[message:%s][function:%s], [file:%s]:[line:%d], [threadID:%d]	WEB_CC module generic debug message	
354003	Debug	[threadid:%d]:[message:%s]	WEB_CC module generic log debug message	
354006	Debug	[__FUNCTION:%s]: SOS message invalid opcode [opcode : 0x%x] , expected [expectedopcode : 0x%x]		
354011	Debug	Success : GSM publish [_FUNCTION : %s] [retval : %d] [cat : %d] [rep : %d] [url : %s]		
354013	Debug	Success : GSM publish [_FUNCTION : %s] [retval : %d]		
354014	Debug	[__FUNCTION:%s]: LC SC message invalid opcode [opcode : 0x%x] , expected [expectedopcode : 0x%x]		
354022	Debug	[__FUNCTION:%s]: [url: %s]		
354024	Debug	[__FUNCTION:%s]: CACHE Lookup : [url: %s]		
354025	Debug	[__FUNCTION:%s] [url : %s] [flags: 0x%x] [rep : %d] [cat : %s]		
354026	Debug	[__FUNCTION:%s]: DB filename : [filename : %s] : [checksum: %s] : [Major: %d] : [Minor: %d]		
354027	Debug	[__FUNCTION:%s]: No DB update available.		
355002	Debug	[func:%s]: [msg: %s]	System related debugging messages logged in Cert Download Mgr	
356005	Debug	[msg:%s]	RNG mgr module debug message	
356303	Debug	[msg:%s]	Debug message about a condition in Mcell process	
356306	Debug	Initialized PAPI	Debug message about a condition in Mcell process	
356307	Debug	Protocol Buffer Initialized	Debug message about a condition in Mcell process	
356308	Debug	File Manager Initialized	Debug message about a condition in Mcell process	
356309	Debug	Record Snapshot started	Debug message about a condition in Mcell process	
356310	Debug	Record Snapshot ended	Debug message about a condition in Mcell process	
356312	Debug	Initializing [msg:%s]	Debug message about a condition in Mcell process	
356313	Debug	[msg:%s] is UP	Debug message about a condition in Mcell process	
356314	Debug	Waiting for [mod1:%s] [mod2:%s]	Debug message about a condition in Mcell process	
356315	Debug	AMON Notify: Empty mgmt_server_list	Debug message about a condition in Mcell process	
356316	Debug	To send AMP Payload	Debug message about a condition in Mcell process	
356317	Debug	Sent AMP Payload	Debug message about a condition in Mcell process	
356319	Debug	GSM replay ended with [retval:%d]	Debug message about a condition in Mcell process	
356320	Debug	[val1:%u] [tm1:%u] [dqtm:%u] [chan:%d] [type:%d] [ind:%d] [key:%d] [val2:%d]	Debug message about a condition in Mcell process	
356321	Debug	GSM Print: [field:%s] [val:%m]	Debug message about a condition in Mcell process	
356322	Debug	AP [ap:%s] Hardware Info Type [type:%d] NumRadios [val:%d] NumChanList [num:%d] FCC_ID [id:%s]	Debug message about a condition in Mcell process	
356323	Debug	AP Upsert (Name/Group/Type) = ([name:%s] [gr:%s] [sev:%d])	Debug message about a condition in Mcell process	
356324	Debug	AP Upsert Ant (2Ghz/5Ghz) = ([val1:%d] [val2:%d])	Debug message about a condition in Mcell process	
356329	Debug	GSM Radio Upsert radio base_mac [mac:%m]	Debug message about a condition in Mcell process	
356330	Debug	GSM Radio Upsert Trigger mcell_csm_handle_event for radio [rad:%m]	Debug message about a condition in Mcell process	
356333	Debug	Radio Delete Incoming key [radio:%m]. Found Radio	Debug message about a condition in Mcell process	
356334	Debug	BSS Upsert radio [mac1:%m] bssid [mac2:%m]	Debug message about a condition in Mcell process	
356335	Debug	BSS Delete: BSSID [mac1:%m] as key to delete	Debug message about a condition in Mcell process	
356336	Debug	BSS Delete radio [mac1:%m] bssid [mac2:%m]	Debug message about a condition in Mcell process	
356337	Debug	STA Upsert Update Client [client:%m] Old->New BSSID ([bss1:%m] -> [bss2:%m])	Debug message about a condition in Mcell process	
356338	Debug	STA Upsert Client ([client:%m]) to be added to MCELL_ASSOC_CLIENT_TBL	Debug message about a condition in Mcell process	
356339	Debug	Client [client:%m] to be deleted	Debug message about a condition in Mcell process	

356340	Debug	Radio Stats Update Radio [radio:%m] assoc_req/assoc_req_success/reassoc_req/reassoc_req_success = ([val1:%d]/[val2:%d]/[val3:%d]/[val4:%d])	Debug message about a condition in Mcell process	
356341	Debug	Recording [module:%s]	Debug message about a condition in Mcell process	
356342	Debug	Record Profile Profile type [type:%3d], InstName [inst:%s], Tail [tail:%s], from Key [key:%s]	Debug message about a condition in Mcell process	
356343	Debug	Record AP List ---------------- AP [mac:%m]	Debug message about a condition in Mcell process	
356344	Debug	action [str1:%m] seq [seq:%u] first 20mhz chan [c1:%u] [c2:%u] primary 20mhz chan [pc:%u] bw[bw:%d] intol40 [id:%d] tx_power[tx:%d] reason [reas:%d]	Debug message about a condition in Mcell process	
356345	Debug	[type:%s] Handler Type [evtype:%s] ([val:0x%X])	Debug message about a condition in Mcell process	
356346	Debug	Channel Assign mcell assign mode [asignmode:%u]	Debug message about a condition in Mcell process	
356347	Debug	Get Random Channel empty channel list	Debug message about a condition in Mcell process	
356348	Debug	Update Chan RF Profile	Debug message about a condition in Mcell process	
356349	Debug	Update Chan at Feasible Chanlists Update	Debug message about a condition in Mcell process	
356350	Debug	AP [ap:%s] updates channel lists	Debug message about a condition in Mcell process	
356351	Debug	Handle Radar Event Radar is detected on 2GHz band (radio [rad:%m] channel [chan:%u])	Debug message about a condition in Mcell process	
356352	Debug	action_init_recording	Debug message about a condition in Mcell process	
356353	Debug	Memory Init AP_HW_INFO Count [count:%d]	Debug message about a condition in Mcell process	
356354	Debug	Build Radio NBR Band [band:%u] Radio ([rad:%2u], [rad_str:%s]) has nbr ([nbr:%2u], [nbr_str:%s])	Debug message about a condition in Mcell process	
356355	Debug	Create Adj Matrix AP count [count:%u] Band [band:%u]	Debug message about a condition in Mcell process	
356356	Debug	Update Adj Matrix AP Index [ind:%u] ([str:%s])	Debug message about a condition in Mcell process	
356357	Debug	Row [row:%3u] [val:%s]	Debug message about a condition in Mcell process	
356358	Debug	Too long reg-domain channel list [l1:%d] > [l2:%d]	Debug message about a condition in Mcell process	
356362	Debug	Protobuf not initiated. Skip	Debug message about a condition in Mcell process	
356363	Debug	File Initialized	Debug message about a condition in Mcell process	
356364	Debug	File De-Initialized	Debug message about a condition in Mcell process	
356365	Debug	Export method is [msg:%s]	Debug message about a condition in Mcell process	
356366	Debug	Finalizing the file [fname:%s]	Debug message about a condition in Mcell process	
356367	Debug	Finalized the file [fname:%s]	Debug message about a condition in Mcell process	
356368	Debug	Prep File Configured file capacity [cap:%d] bytes	Debug message about a condition in Mcell process	
356369	Debug	Prep a new file [fname:%s]	Debug message about a condition in Mcell process	
356370	Debug	Flush to File [sz1:%zu] bytes (File [fname:%s]) (FileSize [sz2:%zu] bytes)	Debug message about a condition in Mcell process	
356371	Debug	mcell_file_manager_main exit	Debug message about a condition in Mcell process	
356372	Debug	NCFG Upsert Profile [name:%s] is added to profile table	Debug message about a condition in Mcell process	
356373	Debug	NCFG Group Name [name:%s] InstName [inst:%s] NumRefs [num:%u] ProfileType [type:%u]	Debug message about a condition in Mcell process	
356374	Debug	Ref_list [id:%d] RGroup [gr:%s] InstanceName [inst:%s]	Debug message about a condition in Mcell process	
356375	Debug	NCFG Group Delete Deleting profile [name:%s]	Debug message about a condition in Mcell process	
356376	Debug	NCFG Profile manager replay completed.	Debug message about a condition in Mcell process	
356377	Debug	NCFG Profile Manager Event [id:%d].	Debug message about a condition in Mcell process	
356378	Debug	NCFG Initialized [retval:%d]	Debug message about a condition in Mcell process	
356379	Debug	Searching radio [radio:%m] by BSSID [bss:%m]	Debug message about a condition in Mcell process	
356380	Debug	Clean BSS Table BSS [bssid:%m]	Debug message about a condition in Mcell process	
356381	Debug	Recvd PAPI message buflen [len:%d] msglen [mlen:%u]	Debug message about a condition in Mcell process	
356382	Debug	Received [type:%s] Message	Debug message about a condition in Mcell process	
356383	Debug	Rx PAPI message type [type:%d]	Debug message about a condition in Mcell process	
356384	Debug	Getting current configuration for the app	Debug message about a condition in Mcell process	
356385	Debug	Getting system info like switch ip, master, etc...	Debug message about a condition in Mcell process	
356386	Debug	Sending [req:%s] Request	Debug message about a condition in Mcell process	
356387	Debug	STA RSSI Report Radio [rad:%m] station RSSI reports (Total [tot:%d]) (Now [now:%ld])	Debug message about a condition in Mcell process	
356388	Debug	CSM SAPM Action Response received.	Debug message about a condition in Mcell process	

356389	Debug	Received SAPM Action Response message from [frm:%u] [id:%d] code[vc:%d] type MCELL_MESSAGE_CSM_SAPM_ACTION_RESP id ([ip:%u],[hx:%x],[val:%d]), length[len:%d]	Debug message about a condition in Mcell process	
356390	Debug	([val:%2d]) [mac:%m] [v2:%3d] [v3:%3d] [t:%u]	Debug message about a condition in Mcell process	
356391	Debug	Valid message code [num:%d] (type [type:%d]) received from [ip:%u]	Debug message about a condition in Mcell process	
356392	Debug	Proc SAPM Response is_ipv4 [is:%d] ipv4 [ip:%u] radio [rad:%d] ap_state [s1:%d]->[s2:%d] result [res:%d] chan [c:%d] secchan [s:%d] pwr [p:%d]	Debug message about a condition in Mcell process	
356393	Debug	Proc SAPM Response Radio key [m:%m] with action first 20mhz chan [c:%u] [c2:%u] prim 20mhz chan [c3:%u] bw [b:%d] intol40 [v1:%d] tx_power [p:%d] reason [r:%d] retries [n:%d] is removed after success	Debug message about a condition in Mcell process	
356394	Debug	radio_action for [r:%m] is different from action in resp first 20mhz chan [c1:%u],[c2:%u]/[c3:%u],[c4:%u] primary 20mhz chan [c5:%u]/[c6:%u] bw [c7:%d]/[c8:%d] tx_power [c9:%d]/[c10:%d]	Debug message about a condition in Mcell process	
356395	Debug	New Radio Key [k:%m] is inserted	Debug message about a condition in Mcell process	
356396	Debug	the same action first 20mhz chan [c1:%u]/[c2:%u] primary 20mhz chan [c3:%u],[c4:%u]/[c5:%u],[c6:%u] bw [c7:%d]/[c8:%d] intol40 [c9:%d]/[c10:%d] tx_power [c11:%d]/[c12:%d] reason [c13:%d]/[c14:%d] exists for radio key [k:%m]	Debug message about a condition in Mcell process	
356397	Debug	update action first 20mhz chan [c1:%u]/[c2:%u] primary 20mhz chan [c3:%u],[c4:%u]/[c5:%u],[c6:%u] bw [c7:%d]/[c8:%d] intol40 [c9:%d]/[c10:%d] tx_power [c11:%d]/[c12:%d] reason [c13:%d]/[c14:%d] for radio key [k:%m]	Debug message about a condition in Mcell process	
356398	Debug	the radio key [k:%m] with action first 20mhz chan [c1:%u] [c2:%u] primary 20mhz chan [c3:%u] bw [c4:%d] intol40 [c5:%d] tx_power [c6:%d] reason [c7:%d] num_retries [n:%d] is removed	Debug message about a condition in Mcell process	
356399	Debug	msg to SAPM wrt the radio key [k:%m] with action first 20mhz chan [c1:%u] [c2:%u] primary 20mhz chan [c3:%u] bw [c4:%d] intol40 [c5:%d] tx_power [c6:%d] reason [c7:%d] num_retries [c8:%d] is sent	Debug message about a condition in Mcell process	
356400	Debug	IP Response, Switch IP [k:%u]	Debug message about a condition in Mcell process	
356401	Debug	Master IP [ip:%u], Switch Role [r:%d]	Debug message about a condition in Mcell process	
356402	Debug	Got all configuration, Setting the process state to UP	Debug message about a condition in Mcell process	
356403	Debug	Register PUBSUB_SERVICE_MGMT_CONFIG	Debug message about a condition in Mcell process	
356404	Debug	[msg:%s]	Debug message about a condition during regulatory domain parsing in Mcell process	
356405	Debug	Event time [timestamp:%lu] seq [seq:%u] src [src:%m] type [eventtype:%u] [eventtypename:%s]	Debug message about event header	
357002	Debug	([func:%s] [line:%d]) [msg:%s]	System related debugging messages logged in Config Distributor	
358004	Debug	[msg:%s]		
358005	Debug	[func:%s]: [msg:%s]		
359001	Debug	[func:%s] [data: %s]	System related debugging messages logged in HCM	
360005	Debug	[msg:%s]		
360006	Debug	[func:%s]: [msg:%s]		
371001	Debug	Validating command:"[cmd:%s]" node:"[node:%s]"	Starting validation for command.	
371014	Debug	Validating command:"[cmd:%s]" - [msg:%s]	Debug NHLIST REF COUNT UPDATE ERROR.	
371015	Debug	Validating command:"[cmd:%s]" - [msg:%s]	Debug INTERFACE TUNNEL REF COUNT UPDATE ERROR.	
380000	Debug	logfwdwrap got signal [sig:%d] from pid [pid:%d], status [status:%d], errno [errno:%d]n	logfwdwrap received child exited signal signal, dumps error code	
381005	Debug	[msg:%s]		
381006	Debug	[func:%s], [msg:%s]		
386007	Debug	[msg:%s]	UDMD system debug log	
390005	Debug	[msg:%s]		
390006	Debug	[func:%s], [msg:%s]		
391002	Debug	[message:%s][function:%s], [file:%s]:[line:%d]	APPRF module generic debug message	
391006	Debug	[message:%s] [function:%s] [file:%s]:[line:%d]	APPRF module generic debug message	

392002	Debug	[msg:%s]		
392501	Debug	[msg:%s]		
393001	Debug	[func:%s] [line:%d] [msg:%s]	System related debugging parse messages logged in the DPI MGR	
393002	Debug	[func:%s] [line:%d] [msg:%s]	System related debugging configuration messages logged in by DPI MGR	
394006	Debug	[msg:%s]	Generic debug level system log	
397003	Debug	[msg:%s]	System related debugging messages logged by DDNS_CLIENT	
398501	Debug	[func:%s] [data: %s]	System related debugging messages logged in Policymgr	
398524	Debug	Add rule in policy [name:%s] with action [action:%d]	This shows an internal debug message	
398525	Debug	[func:%s] [data: %s]	This shows an internal debug message.	
398528	Debug	{Policy} [buf:%s].	This shows an internal debug message	
398531	Debug	invalid delete policy, matched: source [src:%d], dest [dest:%d], service [service:%d]	This shows an internal debug message	
398532	Debug	ICMP type [icmptype:%d], code [icmpfcode:%d]-[lcode:%d].	This shows an internal debug message	
398533	Debug	POLICYHIT: pcl([pcl:%s])=[pclnum:%d] (type [pcltype:%s]), index=[index:%d], TableId=[tableid:%d], index0=[index0:%d], hits=[hit:%d].	This shows an internal debug message	
398534	Debug	Add service: [name:%s] [proto:%d] [fport:%d] [lport:%d] [alg:%s]	This shows an internal debug message	
398536	Debug	[func:%s]: action [action:%s] for appname [appname:%s] id [appid:%d]	This shows an internal debug message	
398552	Debug	[func:%s] [data: %s]	System related debugging messages logged in Policy manager uplink.	Contact tech-support.
398570	Debug	Rx message [messageCode:%d]/[msgtype:%d], length [msglen:%d] from [SrcIpAddr:%s]:[SrcPortNum:%d]	This shows an internal debug message	
398580	Debug	Tx message to Sibyte, flag [flag:%d]. Opcode = [opcode:%d], msglen = [msglen:%d] [action_str:%s]	This shows an internal debug message	
398581	Debug	Tx message to Sibyte, blocking with ack, Opcode = [opcode:%d], msglen = [totlen:%d] [action_str:%s]	This shows an internal debug message	
398582	Debug	Tx message to Sibyte, blocking with reply, Opcode = [opcode:%d], msglen = [totlen:%d] [action_str:%s]	This shows an internal debug message	
398583	Debug	Rx Packet Length [bufferLen:%d] bytes Opcode [opcode:%d]	This shows an internal debug message	
398586	Debug	[func:%s]: [data:%s]	Policy Manager Amon debug information	
399001	Debug	[msg: %s] [lag: %d] [slot:%d] [port:%d]		
399003	Debug	[msg:%s] [Id:%d]		
399004	Debug	[msg:%s]		
399503	Debug	[module:%s] [msg:%s]	System related debugging messages logged by LHM	
399701	Debug	[msg:%s]		
399752	Debug	[msg:%s]		
399804	Debug	[function:%s], [file:%s]:[line:%d]: [error:%s]	This is an internal system debugging log.	
399806	Debug	Unable to open system file [sys_file:%s] in [function:%s], [file:%s]:[line:%d].	This log indicates that we were unable to open a system file for reading/editing. In some cases, the switch may be unaffected by the absence of non-critical files and continue to operate normally.	
399809	Debug	Config debug: [msg:%s] [errno:%d] in [function:%s], [file:%s]:[line:%d].	This log is used for debugging configuration changes	
399814	Debug	[error:%s]	This is an internal system debugging log.	
399819	Debug	Processing a Hidden command, on line#[line:%d]::[cmd:%s]	This log indicates a Hidden command on the line.	
399820	Debug	Processing a Global command, on the local, processing line#[line:%d]::[cmd:%s]	This log indicates a Global command is getting executed on the local.	
399821	Debug	Syntax error processing line#[line:%d]::[cmd:%s]	This log indicates that we saw a syntax error while parsing the config file.	
399823	Debug	[msg:%s]	This is an webserver system debugging log.	
399828	Debug	[msg:%s]	This is an webserver system debugging log.	
399835	Debug	Time taken for activation of configuration [sec:%ld] sec and [microseconds:%ld] microseconds.	This log defines time taken by application to active configuration once it has recieved all the configs from cfgm.	
399836	Debug	Command is not valid in this stacking mode, on line#[line:%d]::[cmd:%s]	An attempt was made to run a command that is not available in the current stacking mode.	

399837	Debug	Command not available on this platform, on line#[line:%d]::[cmd:%s]	An attempt was made to run a command that is not available due to the capabilities of the platform.	
399839	Debug	System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d]. Reason: [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
300300	Emergency	FIPS Emergency: [msg:%s]	This is a FIPS emergency log in system module.	
323001	Emergency	RFD process initialization failed	RFD process initialization failed	
330203	Emergency	MESHD process initialization failed.	MESHD process initialization failed, possibly because the mesh-node is not correctly provisioned.	Reprovision the AP. Please contact Aruba tech-support if this problem persists.
330204	Emergency	MESHD process exiting. No MESH role was specified.	MESHD process exiting. No MESH role was specified.	Reprovision the AP. Please contact Aruba tech-support if this problem persists.
330205	Emergency	MESHD process exiting. No MESH cluster profile was specified.	MESHD process exiting. No MESH cluster profile was specified.	Reprovision the AP. Please contact Aruba tech-support if this problem persists.
335021	Emergency	Emergency Alarm: [Emergency: %s]	Emergency system alarm log.	
341008	Emergency	[msg:%s]		
341338	Emergency	[msg:%s]	netlink emergency message	
386000	Emergency	[msg:%s]	UDMD system emergency log	
392001	Emergency	BLE DAEMON process initialization failed	BLE DAEMON process initialization failed	
399751	Emergency	BLE DAEMON process initialization failed	BLE DAEMON process initialization failed	
300000	Error	Unexpected fatal mobileip runtime error in [file:%s] at [func:%s], [line:%d]	Unexpected condition occurred in the mobility manager (mobileip)	Contact technical support
300005	Error	Unexpected mobileip runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the mobility manager (mobileip)	Contact technical support
300006	Error	Unexpected mobileip runtime error at [func:%s], [line:%d]: [errorstr:%s]	Unexpected condition occurred in the mobility manager (mobileip)	Contact technical support
300007	Error	Unexpected mobileip runtime error for station [mac:%m], [ip:%pI4] at [func:%s], [line:%d]	Unexpected condition occurred in the mobility manager (mobileip)	Contact technical support
300101	Error	Unable to initialize license manager	The license manager failed to initialize its database. This error is fatal and the process will restart.	If the error persists, please contact technical support
300102	Error	Sibyte: PAPI_Send() failed for opcode [opcode:%4x]	Backplane locking failed due to an inability to communicate with the datapath for the indicated opcode.	If the error persists, please contact technical support
300103	Error	Sibyte messaging failure: PAPI_Alloc() failed	Backplane locking failed due to an inability to allocate memory	If the error persists, please contact technical support
300110	Error	Serial number does not match: key [keyval:%s]; system [system:%s]; [key [key:%s]]; disabling	A serial number mismatch has been detected for the specified key, so the system disabled it. This is generally due to swapping flash modules or importing a license database from another controller.	If the error persists, please contact technical support
300111	Error	Model number does not match: key [keyval:%s]; system [system:%s]; [key [key:%s]]; disabling	A model number mismatch has been detected for the specified key, so the system disabled it. This is generally due to swapping flash modules or importing a license database from another controller.	If the error persists, please contact technical support
300112	Error	Limit not valid for [os:%s] [limit:%s][[id:%d]]; disabling	An invalid limit key has been detected, so the system disabled it. This is generally due to swapping flash modules or importing a license database from another controller.	If the error persists, please contact technical support
300113	Error	Feature not valid for [os:%s] [feature:%s][[id:%d]]; disabling	An invalid feature key has been detected, so the system disabled it. This is generally due to swapping flash modules or importing a license database from another controller.	If the error persists, please contact technical support
300116	Error	DB command '[cmd:%s]' failed with error [error:%s]	An SQL error occurred while executing the indicated command.	If the problem persists, please contact technical support
300119	Error	Failed to delete the license key [key:%s]	The indicated license key could not be deleted. The preceding message indicates the SQL error.	
300120	Error	Key creation failed [key:%s]	During an upgrade from an older release, creation of an evaluation key failed.	
300121	Error	Deletion of all licenses failed	Clearing all the licenses failed. The preceding error indicates the SQL failure.	

300123	Error	Activation status change failed	Changing the activation status of one or more keys failed. The preceding message indicated the SQL failure.	
300124	Error	feature table file open failed: [error:%s].	Internal communication between licensing and other applications has failed. Reload the controller.	If the problem persists, contact support.
300125	Error	feature table write failed: [error:%s].	Internal communication between licensing and other applications has failed. Reload the controller.	If the problem persists, contact support.
300127	Error	Error reading backplane serial number	The software was unable to obtain the system serial number. Licensed functions will not work	Please contact support.
300129	Error	[function:%s]: Encryption failed for '[time:%s]'	Encrypting the installation time for the key failed. If the problem persists, contact support.	
300130	Error	[function:%s]: failed to decrypt time [time:%s]	Decrypting the installation time for a key failed. If the problem persists, contact support.	
300131	Error	Failed to enable configuration fragment for feature [name:%s][[id:%d]] [fragment [fragment:%s]]: [error:%s]	After adding a license that requires a configuration file update, the update failed.	
300133	Error	[function:%s]: Serial number does not match: key [keyval:%s]; system [system:%s] key [[key:%s]]	A serial number mismatch has been detected for the specified key. This is generally due to swapping flash modules or importing a license database from another controller.	
300134	Error	[function:%s]: Model number does not match: key [keyval:%s]; system [system:%s] key [[key:%s]]	A model number mismatch has been detected for the specified key. This is generally due to swapping flash modules or importing a license database from another controller.	
300135	Error	[function:%s]: Serial number does not match: key [keyval:%s]; system [system:%s]	A serial number mismatch has been detected for the specified key. This is generally due to swapping flash modules or importing a license database from another controller.	
300136	Error	[function:%s]: Model number does not match: key [keyval:%s]; system [system:%s]	A model number mismatch has been detected for the specified key. This is generally due to swapping flash modules or importing a license database from another controller.	
300137	Error	[function:%s]: Error while retrieving the license record: [error:%s]	An SQL error occurred while looking up a license key.	
300142	Error	[function:%s]: Failed to export the License Database to file: [file:%s] [error:%s]	An SQL error occurred when exporting the database.	
300147	Error	[function:%s]: Failed to import the License Database from file: [file:%s] [status:%u] [error:%s]	An SQL error occurred when importing the database.	
300152	Error	[function:%s]: Platform upgrade from [fromplt:%s] to [toplt:%s] is not supported	Platform upgrade is not supported to the new platform from the existing platform.	
300154	Error	[function:%s]: Feature not valid for feature [feature:%s] id [id:%d]	This key contains a feature which is not allowed on this variant.	
300155	Error	[function:%s]: Evaluation key for feature [feature:%s] id [id:%d] is older than [days:%u] days; key cannot be added	The keys cannot be added as the Eval key for the feature is older.	
300156	Error	[function:%s]: Complete key already present, dropping the cmd	A complete key is already installed; only one is allowed.	
300163	Error	[function:%s]: Key already present, dropping the cmd	Dropping the cmd to add key as key is already present.	
300164	Error	[function:%s]: Key does not exist, dropping the cmd	Dropping the cmd to delete key as key is not present.	
300174	Error	License database creation failed	Failed to create a new License Database.	
300179	Error	[function:%s]: License report aborted; failed to set the stdout to file [file:%s]: [error:%s]	License report aborted due to a failure in file open.	
300180	Error	[function:%s]: License report generation failed [error:%s]	License report generation failed.	
300181	Error	[function:%s]: ODBC Init Failed [error:%s]	The license manager failed to initialize its database. This error is fatal and the process will restart	If the error persists, contact support
300189	Error	[function:%s]: Error while retrieving the license records, multiple License Entries	An error occurred while retrieving the license records as there are multiple License Entries.	
300190	Error	[function:%s]: No license entry found for key [key:%s]	There is no license entry matching the particular key.	
300195	Error	[function:%s]: No license entry found	No license entry found in the License DB.	
300199	Error	[function:%s]: Invalid license key	license keys installed are not valid for this controller.	
300201	Error	Config sync failed when trying to [updn:%s] configuration [tofrom:%s] [url:%s]	Operation failed when trying to sync the configuration with the MMS server. This could be due to the MMS server not properly configured, server unreachable, or an internal system error. Please retry after verifying the MMS connection. Contact Tech Support if problem persists.	

300303	Error	FIPS Error: [msg:%s]	This is a FIPS error log in system module.	
300500	Error	[func:%s], [line:%d], [msg:%s]	Unexpected condition occurred in user visibility process	
300800	Error	[msg:%s]	Central Agent encountered an Internal Error.	
300903	Error	[name:%s]	This is an internal error message	
301003	Error	Error, forwarding traps to the trap daemon.	The system reported an error while trying to send an internal PAPI message to the trap daemon for trap processing. As a result, a trap may not have been reported to a trap receiver.	
301011	Error	Can't open the Boot Filen	At startup, the SNMP process could not open a file containing the SNMP engine boots ID which is used for SNMPv3 user based security model. This is a fatal error and the SNMP process will be restarted.	
301012	Error	Can't open the Boot File for readingn	At startup, the SNMP process could not read a file containing the SNMP engine boots ID which is used for SNMPv3 user based security model. This is a fatal error and the SNMP process will be restarted.	
301014	Error	Invalid length. Encoding Failed: [file:%s]:[line:%d]	The SNMP server failed to create an SNMP PDU used for SNMP response due to an invalid data length. An SNMP response will not be generated.	
301016	Error	Error Building PDU [file:%s]:[line:%d]	The SNMP server failed to create an SNMP PDU used for an SNMP response. An SNMP response will not be generated.	
301025	Error	Error Adding [AddOID:%s] to the Varbind [file:%s]:[line:%d]	The SNMP server failed to create an SNMP PDU used for an SNMP response due to a failure in creating a var bind for the PDU response. An SNMP response will not be generated.	
301048	Error	[line:%d] Cannot Concatenate OID, [reason:%s]	The SNMP server reported an error while creating a new OID from 2 OIDs	
301050	Error	SNMP PDU from [srcIP:%s] action [act:%s]	The SNMP server reported an error while handling an SNMP PDU	
301067	Error	SNMP PDU from [srcIP:%s], parse VB failed, [reason:%s]	The SNMP server reported an error while handling SNMP varbinds	
301083	Error	SNMP PDU from [srcIP:%s], parse octet string failed, [reason:%s]	The SNMP server reported an error while handling an octet string varbind	
301084	Error	SNMP PDU from [srcIP:%s], Parse OID failed, [reason:%s]	The SNMP server reported an error while handling an OID	
301096	Error	SNMP PDU from [srcIp:%s], [func:%s] failed due to [reason:%s]	The SNMP server detected an invalid data type while parsing a PDU	
301126	Error	[file:%s] SNMP PDU from [srcIP:%s], [reason:%s]	The SNMP server reported an error while parsing an SNMP message	
301131	Error	Error creating snmp message packet	The SNMP server was unable to allocate memory for an octet string	
301132	Error	[line:%d] [msg:%s]	The SNMP server reported an invalid SNMP engine ID algorithm request	
301136	Error	message ID [mms:%d] is out of range	The SNMP server reported an invalid SNMP v3 message ID	If the error persists, please contact technical support
301138	Error	mms value [mms:%d] is out of range	The SNMP server received an SNMP v3 message that exceeds the maximum supported message size.	If the error persists, please contact technical support
301173	Error	[file:%s]:[line:%d] [msg_reason:%s]	The SNMP server received an invalid security level while creating an SNMPv3 message	If the error persists, please contact technical support
301178	Error	[line:%d] Row creation failed for table:[tbl_type:%s] [msg_reason:%s]	The SNMP server encountered an internal error while creating a new entry for an SNMP user or host	
301187	Error	Could not create vacmSecurityToGroupEntry for [SecurityName:%s]	The SNMP server encountered an internal error while creating a search string while adding or modifiying a host	
301202	Error	Unable to create OctetString for name [name:%s]	The SNMP server encountered an internal error while creating a search string while adding or modifiying a host	
301206	Error	[line:%d] Received bad value for security [type:%s]	The SNMP server encountered an invalid security level or model for SNMP v3 authentication	
301207	Error	[line:%d] Error Modifying the row. Row does not exist	The SNMP server encountered an internal error while modifying an internal host, community, or user entry	

301212	Error	[line:%d] Error Deleting the row. Row does not exist	The SNMP server encountered an internal error while deleting an internal host, community, or user entry	
301213	Error	Translate name to OID: hash table lookup failed: [text_str:%s]	The SNMP server encountered an internal error while converting dot notation name to its OID	If the error persists, please contact technical support
301214	Error	[line:%d] Make OID from Name: [msg_reason:%s]	The SNMP server encountered an internal error while creating an OID	If the error persists, please contact technical support
301216	Error	[line:%d] Converting to name from OID: [reason:%s]	The SNMP server encountered an internal error while converting an OID to a dot notation string	If the error persists, please contact technical support
301218	Error	Make Variable binding received a NULL object parameter	The SNMP server encountered an internal error while creating a varbind	If the error persists, please contact technical support
301219	Error	Make Variable binding received a NULL OID parameter	The SNMP server encountered an internal error while creating a varbind	If the error persists, please contact technical support
301220	Error	cannot make context SnmpEngineID	The SNMP server encountered an internal error while creating an SNMPv3 report PDU	If the error persists, please contact technical support
301221	Error	cannot make context Name	The SNMP server encountered an internal error while creating an SNMPv3 report PDU	If the error persists, please contact technical support
301222	Error	Could not parse reqid in encrypted message.You may have just got an error in ParseType, but this is normal behavior.	The SNMP server encountered an internal error while creating an SNMPv3 report PDU	
301223	Error	Initializing standard MIBS failed. Continuing anyway.	The SNMP server encountered an internal error while initializing the standard MIB	
301224	Error	Initializing enterprise MIBS failed. Continuing anyway.	The SNMP server encountered an internal error while initializing the enterprise MIB	
301227	Error	Received Zero-Length packet from [tst:%s]	The system reported an error when the SNMP process received a zero length packet	If the error persists, please contact technical support
301240	Error	Unknown Context received in the request	The SNMP process received a SNMP v3 request with an unknown context	Please verify that the credentials used for the SNMP v3 request is valid
301250	Error	Sendto failed, unable to send trap to manager [tst:%s].	The TRAPD process is unable to send a trap to a trap host	If the error persists, please contact technical support
301254	Error	[file:%s]:[line:%d] Error Destination Trap host is not found	The TRAPD process couldn't find the trap host receiving a generated trap	If the error persists, please contact technical support
301259	Error	Could not parse response/report to InformRequest	The TRAPD process is unable to parse an SNMP v3 inform response	If the error persists, please contact technical support
301261	Error	Processing Inform response, Cannot Parse PDU	The TRAPD process is unable to parse an SNMP v3 inform response	If the error persists, please contact technical support
301287	Error	[function:%s]: Error in setting the Security to Group	The TRAPD/SNMPD process is unable to edit an SNMPv3 security group entry	If the error persists, please contact technical support
301288	Error	[function:%s]: Error Setting the User	The TRAPD/SNMPD process is unable to add an SNMPv3 security user	Please verify that the SNMPv3 supplied credentials are correct. If the error persists, please contact technical support
301290	Error	Error Setting the Host Parameter ([communityName:%s])	The TRAPD process was unable to add an SNMP v1 host entry	Please verify that the supplied SNMP v1 trap host entry is valid. If the error persists, please contact technical support
301291	Error	Error Setting Host Receiver ([communityName:%s])	The TRAPD process was unable to add an SNMP v1 community target	Please verify that the supplied SNMP v1 trap host entry is valid. If the error persists, please contact technical support
301292	Error	Error: Cannot configure more than ([MAX_NUMBER_OF_INFORM_HOSTS:%d])	The TRAPD process has reached the maximum number of SNMP v3 inform hosts	Please remove an existing SNMP v3 inform hosts to add a new entry
301298	Error	User Entry is not present [uname:%s]	To_be_filled_out	
301299	Error	Error Setting V2C Host Receiver ([communityName:%s])	To_be_filled_out	
301300	Error	[line:%d] Error Setting the V2C Host Parameter ([communityName:%s])	To_be_filled_out	
301303	Error	Error Deleting the Trap params ([communityName:%s])	To_be_filled_out	
301304	Error	[line:%d] User should be defined, before adding to the Trap host	To_be_filled_out	
301305	Error	Error deleting the Manager User Entry	To_be_filled_out	
301306	Error	[line:%d] Error: deleting the Trap Host ([communityName:%s])	To_be_filled_out	
301307	Error	Error Deleting the V3 Host Parameter ([communityName:%s])	To_be_filled_out	
301308	Error	Cannot Create socket to send configuration to snmp agent	To_be_filled_out	
301309	Error	Error Sending Hostname change to CLI	To_be_filled_out	
301310	Error	Reached the Max Inform limit ([ARUBA_MAX_INFORM_PER_HOST:%d]) for a Host: Dropping the inform	To_be_filled_out	

301312	Error	Error: Deleting the Inform Host ([secName:%s])	To_be_filled_out	
301316	Error	[file:%s]:[line:%d] Trap not found in the trap list [trapNum:%d] source [source:%s]	To_be_filled_out	
301317	Error	Type is not supported [type:%d]	To_be_filled_out	
301318	Error	Error: Index Value is more than the index count [indx:%d] [cnt:%d]	To_be_filled_out	
301319	Error	Received an Invalid Packet type [MessageCode:%d], Expecting Snmp Resp	To_be_filled_out	
301320	Error	No OID for trap ID [id:%d]	To_be_filled_out	
301330	Error	OID Length in OID is not correct for Varbind [intg:%d]	To_be_filled_out	
301332	Error	Error: Finding the Varbind List length	To_be_filled_out	
301333	Error	AMP:Table not supported error	To_be_filled_out	
301344	Error	Error retrieving Number of Access Points	To_be_filled_out	
301345	Error	Error retrieving Number of Stations	To_be_filled_out	
301405	Error	SNMP agent unable to send notification response for trap [trap:%d] to the application [app:%s]	not filled up	
301409	Error	Received an Invalid SNMP Request type [type:%d] in the packet from [ip:%s]	not filled up	
301410	Error	[func:%s] Dropping this req - please enable stats collection first through CLI	not filled up	
301411	Error	[func:%s] Dropping this req - invalid request type	not filled up	
301412	Error	[func:%s] Dropping this req as a similar request is already in progress	not filled up	
301413	Error	[func:%s] Dropping this req as a similar request is already queued	not filled up	
301414	Error	[func:%s] Scheduling the Stats/Disc Request [index:%d]	not filled up	
301415	Error	[func:%s] Recvd rsp, when no req in progress	not filled up	
301416	Error	[func:%s] Recvd rsp, when req in progress is different	not filled up	
301417	Error	[func:%s] Recvd rsp, when req in progress is different	not filled up	
301418	Error	[func:%s] Dropping this req [req:%d] invalid category [cat:%d]	not filled up	
301422	Error	[func:%s] Dropping this req [req:%d] invalid tableid [table:%d]	not filled up	
301423	Error	[func:%s] [line:%d] Invalid req, Dropping the req [req:%d] catid [catid:%d] tableid [table:%d]	not filled up	
301424	Error	[func:%s] [line:%d] Stats/Disc File open error fname [filename:%s]	not filled up	
301425	Error	[func:%s] Cannot get the SwitchIp	not filled up	
301426	Error	[func:%s] [line:%d] Stats File seek error [filename:%s] offset [offset:%d]	not filled up	
301428	Error	[func:%s] Cannot open cookie file [name:%s]	not filled up	
301429	Error	[func:%s] No Active MMS IP, cannot send https response	not filled up	
301430	Error	[func:%s] Can't generate Cookie file, cannot send https response	not filled up	
301431	Error	[func:%s] Can't send https response	not filled up	
301432	Error	[func:%s] [line:%d]Can't create the symbolic link for the webui	not filled up	
301433	Error	[func:%s] [line:%d] Stats File write error [filename:%s]	not filled up	
301434	Error	[func:%s] [line:%d] Stats Req TimeOut error	not filled up	
301436	Error	[func:%s] [line:%d] MMS server [ipstr:%s] in sync request is different than the active MMS server	The controller only accepts config sync requests from the active MMS server. This syslog indicates the config sync was generated from a unrecognized IP address.	
303000	Error	Unexpected nanny runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the process manager (nanny)	Contact technical support
303001	Error	Unexpected nanny runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the process manager (nanny)	Contact technical support
303003	Error	Failed to open console starting [process:%s], error [err:%s] at line [line:%d]	Failed to open console while starting process	Contact technical support
303004	Error	Failed to exec starting [process:%s], error [err:%s] at line [line:%d]	Failed to exec process.	Contact technical support
303005	Error	Process [process:%s] [pid [pid:%d]]: wait4() returned -1, error [err:%s]	Internal Error	Contact technical support
303008	Error	Error Sending Data to Cli	NA	
303009	Error	Cannot Create CLI socket	NA	
303020	Error	Failed to fork while trying to reboot AP, error [err:%s]	Internal Error	Contact Technical Support
303021	Error	Machine should reboot but the no reboot flag is set in CPBOOT!	No Reboot flag is set in CPBOOT.	Contact Technical Support
303023	Error	nanny_list parse error: Line Number [line:%d] should start with RESTART, REBOOT, ONETIME, FOREVER or CONSOLE	This should not happen, contact technical support.	Contact Tecnical Support
303024	Error	Cannot open directory [dir:%s] retrieving core file, error [err:%s]	This should not happen, contact technical support.	Contact Tecnical Support
303025	Error	Found core file [fname:%s], [size:%d] bytes, compressing...	Compressing Core file.	Contact Technical Support
303026	Error	Compressing core file failed with code [errcode:%d]	Internal System error while compressing core file	Contact Technical Support

303027	Error	Core file can't be saved on flash, file size: [fsize:%ld]MB, available: [favail:%d]MB	Unable to save core file	Remove unused files from flash
303028	Error	No core file found for process [pname:%s] [pid [pid:%d]]	Process went down but no core file has been generated	If this issue is seen consistently contact Technical Support
303029	Error	Process [pname:%s] [pid [pid:%d]]: crash data saved in dir [dirname:%s]	Successfully generated Core file	Contact Technical Support
303030	Error	Attempting to transfer core of [process:%s] [pid [pid:%d]] to server [server:%s]	Transferring core file to server	Contact Technical Support
303041	Error	Free Flash space is [free:%d] MB, removing old crash dumps	Removing old crash dumps	Just an information message. No action required
303042	Error	After cleaning older crash data, free flash space is [free:%d] MB	Information mesage	Just an information message. No action required
303043	Error	After cleaning older crash data, free flash space is [free:%d] MB	Information mesage	Just an information message. No action required
303044	Error	Still not enough free flash space, cleaning more core files	System is trying to generate more free space. Cleaning more core files	Just an information message. No action required
303045	Error	After cleaning cores files, free flash space is [free:%d] MB	Information mesage	Just an information message. No action required
303046	Error	Still not enough free flash space, removing all crash data	Removing all crash data from flash	Just an information message. No action required
303047	Error	After cleaning ALL crash data, free flash space is [free:%d] MB	Information mesage	Just an information message. No action required
303050	Error	Low free space on RAM disk: [free:%d] MB, lower than [total:%d] MB, will clean up crash data	We are running low on memory. We will be removing old crash files to generate more free space	Just an information message. No action required
303051	Error	After cleaning cores free disk space is [free:%d] MB	Information mesage	Just an information message. No action required
303061	Error	Low freeMemory [free:%lu] ([freem:%lu] MB), total [total:%lu] ([totalm:%lu] MB), min [min:%d] MB	This message indicates system is running out of memory. System will reboot if the condition persists	Run "show processes" and "show memory" command to monitor usage
303063	Error	Total free memory ([free:%d] KB) too low, less than [min:%d] KB, will reboot AP	We are running very low on memory. AP will reboot	Contact Support
303070	Error	Critical process [proces:%s] [pid [pid:%d]] DIED, process marked as [restart:%s]	Critical process has gone done	Contact Technical Support
303071	Error	Critical Process died. Rebooting...	Critical process has died. Rebooting system	Contact Technical Support
303072	Error	[process:%s] old pid [opid:%d] new pid [npid:%d]	Process has been restarted	Information messgae. No action required
303073	Error	Process [process:%s] [pid [pid:%d]] died: got signal [signal:%s]	Process died because of signal mentioned above	Contact Technical Support
303074	Error	Process [process:%s] [pid [pid:%d]] died: exited with [ecode:%x]	NA	
303075	Error	Process [process:%s] [pid [pid:%d]] died: signal [signal:%s] stopped it	NA	
303076	Error	Non re-startable process [process:%s] [pid [pid:%d]] has terminated	One Time Process has terminated	Just an Information message. No action required
303079	Error	Restarted process [process:%s], new pid [npid:%d]	Restartable processes has been respawned	Information message no action required
303080	Error	Please tar and email the file crash.tar to [email:%s]	NA	
303081	Error	To tar type the following commands at the Command Line Interface: (1) tar crash (2) copy flash: crash.tar tftp: [serverip] [destn filename]	This message defines action to be taken once crash file has been generated	Follow instructions and contact Technical Support with crash.tar file
303082	Error	Please tar and email the crash information to [email:%s]	NA	
303083	Error	Process [process:%s] was restarted [ntimes:%d] time(s); no more restarts.	Process has been restarted with in defined limits. No more restarts for this process	Contact Technical Support
303084	Error	Failed to restart process [process:%s]	Internal system error, Unable to restart process	Contact technical Support
303085	Error	Process Manager (nanny) shutting down - Machine will reboot!	Nanny recieved SIGTERM, System will reboot	Contact Technical Support
303086	Error	Process Manager (nanny) shutting down - AP will reboot!	Nanny recieved SIGTERM, AP will reboot	Contact Technical Support
303093	Error	Out Of Memory handler killed process [process:%s]:[pid:%d] due to low memory. Set [set:%d]	NA	
303094	Error	Rebooting controller due to repeated low memory events	NA	
303096	Error	AP Hung, free memory ([free:%d] KB), less than [min:%d] KB, clients ([clients:%d]), leaked ([leaked:%d]), will reboot AP	We are running hung. AP will reboot	Contact Support
304000	Error	Unexpected stm (Station management) runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the station manager (stm).	Contact Aruba tech-support.
304001	Error	Unexpected stm (Station management) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the station manager (stm)	Contact Aruba tech-support.
304035	Error	PAPI_Send failed: [error:%d]; from [sport:%d] to [toaddr:%P]:[toport:%d] len [len:%d] type [type:%d]	Inter-process communication message failed to reach the target.	
304039	Error	VPOOL: Maximum capcity ([count:%d]) reached for Vlan Pool hash table	Please contact support	
304040	Error	VPOOL: Vlan Pool hash table ([vap:%s]) collision at [entry:%d]. Not handled!	Please contact support	
304041	Error	VPOOL: Error allocating VLAN from Virtual AP pool [name:%s]	Please contact support	
304045	Error	Connection to User DB failed	The application was not able to connect to the user database.	
304046	Error	Creation of Client Denylist tables in User DB failed	The application was not able to create the Client Denylist tables in the user database.	

304047	Error	SQL Command [command:%s] failed on User DB. Reason: [reason:%s]	This log indicates that an SQL command failed when it was executed on the user database.	
304049	Error	Update to client denylist database table failed.	This log indicates that an update to the client denylist database table failed.	
304054	Error	Client denylist is full and caused an entry to not be added. Limit: [limit: %d].	This log indicates that the client denylist table is full and an entry that would have been added could not be added.	
304055	Error	Unexpected stm (Station management) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the station manager (stm)	Contact Aruba tech-support.
304058	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s]; opcode [opcode:%d] action [action:%d]	Aruba inter-process communication message failed to reach datapath.	
304060	Error	[func:%s], [line:%d]: Sibyte reply truncated; opcode [opcode:%d] action [action:%d]	Datapath reply to PAPI message sent is truncated.	
304062	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s]	Aruba inter-process communication message failed to reach auth manager.	
304063	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s]	Aruba inter-process communication message failed to reach air monitor.	
304064	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s], dstport [dst:%d], msgcode [code:%d]	Aruba inter-process communication message failed to reach destination.	
304065	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s], dstport [dst:%d]	Aruba inter-process communication message failed to reach destination.	
304067	Error	PAPI_Send failed: [func:%s], [line:%d]: [error:%s]; from [sport:%d] to [toaddr:%P]:[toport:%d] len [len:%d] type [type:%d]	Inter-process communication message failed to reach the target.	
304095	Error	[AMON_ERROR:%s]	This log used to track errors in AMON message building.	
304112	Error	MM: [func:%s] received NULL gsm during mon user delete		
305004	Error	AP [name:%s]: [pcmd:%s] "[inst:%s]" is invalid.	The system tried to assign the specified profile to the specified AP, but the profile was invalid. This profile will not be used. Run "show profile-errors" to display profile problems.	
305027	Error	[owner:%s]: No valid instances of required profile "[prof:%s]"	The AP's configuration must contain at least one valid instance of the given profile type, but none were found. The AP will not be configured. Contact Aruba technical support and provide the output of "show profile-errors".	
305044	Error	AP [name:%s]: Unable to assign virtual AP "[vap:%s]": [pcmd:%s] "[inst:%s]" is invalid.		
305045	Error	AP [name:%s] at [ip:%P] is using the wrong key.		
305052	Error	AP [name:%s] has same value for native and uplink VLAN. AP will become unreachable		
305102	Error	[msg:%s]		
305103	Error	Total number of APs [cur:%u] has exceeded the recommended limit of [limit:%u]. Please reduce the number of APs connected.	Log applicable only to 7240, when total number of APs cross 2K.	
305106	Error	Analytics Engine Error info: [msg:%s]	This shows analytics error info	
306001	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d].	This log indicates that we encountered an internal system error	Contact your support provider
306002	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error	Contact your support provider
306400	Error	Unable to get license information	Application failed to get license information	
306402	Error	IKE Daemon can not HashCreate()...	IKE Daemon encounted an internal error during startup	
306403	Error	IKE Daemon received unknown data	IKE Daemon received information it can not process	This message can be ignored
306406	Error	IKE Daemon received unknown service type [service:%d]	IKE Daemon received internal message from unknown service	This message can be ignored
306407	Error	[function:%s]: Can not write sysctl(): [errno:%s]	Sysctl call failed	
306410	Error	IKE Daemon can not initSaveConfig()...	Ike Daemon could not initialize configuration data	
306413	Error	Requesting switch IP failed to send request.	VPN module requesting for switch IP failed.	
306419	Error	[func:%s](): Caller:[caller:%s]. Failed to get ip address from L2TP pool:[pname:%s].	Failed to get ip address from l2tp pool	
306514	Error	Pubsub send message code [mcd:%d] source port [sr_prt:%d] to destination port [dest_prt:%d] failed, errno [err_str:%s]	PubSub module encountered an internal error while sending a message to the specified module. The message will be resent	

306515	Error	Module [mod:%s] failed to register as publisher for service [service:%s]	Failed to send pubsub publisher message to pubsub module. The message will be resent	
306516	Error	Module [mod:%s] failed to register as subscriber for service [service:%s]	Failed to send pubsub subscriber message to pubsub module. The message will be resent	
306520	Error	Module [mod:%s] failed to unregister from subscribe service [service:%s]	Failed to unregister pubsub subscriber from pubsub module. The message will be resent	
306600	Error	Facility [facility:%d] Not found in the list	This is an internal system error	Please contact support
306701	Error	[msg:%s]	Unexpected condition occurred in the PDM process	
306702	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the PDM process	
307021	Error	[file:%s] [func:%s] [line:%d], MyRole [role:%s], Error sending [pkt_type:%s] to [sw_ip:%s] errno [errno_str:%s], socket ID [sock:%d]	Controller encountered error sending data over TCP socket between conductor-local	
307024	Error	[file:%s] [func:%s] [line:%d], MyRole [role:%s], Error receiving data on socket [sock:%d] errno [errno_str:%s], bytes received [byte_recv:%d]	Controller has encountered error receiving data over TCP socket between conductor-local	
307059	Error	Switch ([switchip:%s]) not in the Local Switch list	Conductor received communication from local from which it never heard (exchanged heart-beat).	
307069	Error	Send Large Failed:Cannot send snapshot configuration to [switchip:%s]:[CFGMANAGER:%d]	Configuration manager is unable to push config snapshot to Application due to failure of inter-process messaging	Contact technical support
307070	Error	Error occurred sending the configuration data to the local switch [switch_ip:%s]; error=[err_msg:%s]	Conductor failed to send configuration to Local over TCP connection	Contact technical support
307080	Error	sxdr_read failure on '[tbuf:%s]'		
307139	Error	Error sending request to L2/L3 module for switch ip registration	Configuration manager is unable to send switch ip request message to L2/L3 module	Contact technical support
307141	Error	Error sending request to L2/L3 module for VRRP Role Information	Configuration manager is unable to send VRRP role information message to L2/L3 module	Contact technical support
307164	Error	Cannot allocate packet for config messaging	Configuration manager is unable to allocate buffer, may be system is low on Memory	Contact technical support
307165	Error	Cannot allocate packet for heartbeat	Configuration manager is unable to allocate buffer, may be system is low on Memory	Contact technical support
307180	Error	Cannot Bind CLI socket	Bind socket system call failed. It will retried	If problem persists, contact technical support
307199	Error	Configuration file read error	Configuration manager is unable to read configuration file	Contact technical support
307222	Error	Error opening the Conductor Config Socket. Configuration distribution to the locals will not work properly	Error opening the Conductor Config Socket. Configuration distribution to the locals will not work properly	
307225	Error	Error making the Config server socket NON BLOCKING	There was an error in making the Config server socket NON BLOCKING	
307228	Error	Error Accepting a connection to the Conductor Config socket:[err_str:%s]	Error Accepting a connection to the Conductor Config socket	
307246	Error	Error allocating memory for configuration packet of size [len:%d]	Configuration manager is unable to allocate memory for config packet, may be system is low on Memory	Contact technical support
307247	Error	Received Configuration size ([ret:%d]) is less than expected value [len:%d] :: Error is [err_msg:%s]	Local received config less than what conductor conveyed in config header. This config download will be aborted and local will retry	If problem persists, contact technical support
307259	Error	dbsync: Unable to initialize dbsync module ([__func:%s])	DBSYNC was unable to initialize itself upon startup.	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support
307261	Error	dbsync: cannot initialize PAPI ([__func:%s])	DBSYNC was unable to initialize the internal messaging system upon startup.	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support
307262	Error	dbsync: PAPI length mismatch expected [msg_len:%d] received [bytes_read:%d]	DBSYNC encountered a length error with the internal messaging system	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support
307263	Error	dbsync: Received message from WMS in unexpected state ([state:%s]); Previous WMS database operation probably timed out	DBSYNC encountered a error when communicating with the wms process	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support
307264	Error	dbsync: Unhandled message received in ([__func:%s])	DBSYNC encountered an unrecognized message	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support
307266	Error	dbsync: Failed to receive ack for PAPI message ([__func:%s], error=[error:%d], current state is: "[state:%s]")	DBSYNC encountered an error when sending internal messages	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support
307267	Error	dbsync: PAPI_Alloc failed ([__func:%s])		
307268	Error	dbsync: PAPI_Send failed ([__func:%s])	DBSYNC encountered an error when sending internal messages	Try issuing a 'process restart dbsync' to reinitialize dbsync. If problem persists please contact Aruba support

307269	Error	dbsync: timed out, failed to complete in time (state= [state:%s], timeout= [sec:%d])		
307270	Error	dbsync: cleanup failure ([__func:%s])		
307271	Error	dbsync: cannot start l3 redundancy sync on primary conductor ([__func:%s])		
307272	Error	dbsync: cannot start l3 redundancy sync on secondary conductor ([__func:%s])		
307273	Error	dbsync: failed to start db sync on standby ([__func:%s])		
307274	Error	dbsync: Failed to backup the local user database on the active MC		
307275	Error	dbsync: rsync of database backup to secondary conductor failed ([__func:%s])		
307276	Error	dbsync: restoring of database backup on secondary conductor failed ([__func:%s])		
307277	Error	dbsync: Invalid sync state: [state:%d] ([__func :%s])		
307278	Error	dbsync: Failed to backup the WMS database on the active MC, status [status:%d]		
307279	Error	dbsync: failed to rename WMS database backup file ([filename:%s]) before sending to backup MC (errno= [err_msg:%s])		
307280	Error	dbsync: failed to open WMS database backup file ([filename:%s]) to send to backup MC (errno= [err_msg:%s])		
307281	Error	dbsync: failed to stat WMS database backup file ([filename:%s]) to send to backup MC (errno= [err_msg:%s])		
307282	Error	dbsync: failed to backup WMS database, backup file ([filename:%s]) size is 0, aborting		
307287	Error	dbsync: failed to receive wms db sync on standby ([__func:%s])		
307288	Error	dbsync: failed to open local users database backup file ([DBSYNC_UDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307289	Error	dbsync: failed to stat local users database backup file ([DBSYNC_UDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307294	Error	dbsync: failed to receive user db sync on standby ([__func:%s])		
307298	Error	dbsync: failed to receive db sync on standby ([__func:%s])		
307299	Error	dbsync: failed to open file ([filename:%s]) to send to backup MC (errno= [err_msg:%s])		
307300	Error	dbsync: failed to stat file ([filename:%s]) to send to backup MC (errno= [err_msg:%s])		
307314	Error	dbsync: failed to receive user db sync on standby ([__func:%s])		
307317	Error	dbsync: failed to stat file ([fName:%s]) (errno= [err_msg:%s])		
307319	Error	dbsync: Can not start db sync on backup Conductor Switch: ([state:%s])		
307322	Error	dbsync: Can not receive file on backup Conductor Switch: ([state:%s])		
307325	Error	dbsync: Can not receive db on backup Conductor Switch: ([state:%s])		
307326	Error	dbsync: Failed to create db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307327	Error	dbsync: Failed to write db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307330	Error	dbsync: Can not receive user db on backup Conductor Switch: ([state:%s])		
307331	Error	dbsync: Failed to create user db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307332	Error	dbsync: Failed to write user db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307335	Error	dbsync: Can not receive file on backup Conductor Switch: ([state:%s])		
307336	Error	dbsync: Failed to create file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307337	Error	dbsync: Failed to write file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		

307338	Error	dbsync: Failed to chmode file [filename:%s]. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307341	Error	dbsync: Can not restore db on backup Conductor Switch: ([__func:%s], [state:%s])		
307342	Error	dbsync: Failed to start database restore on the standby ([__func:%s])		
307347	Error	dbsync: Failed to restore the WMS database on the backup MC		
307351	Error	dbsync: Failed to restore the local user database on the backup MC		
307352	Error	dbsync: Can not restore local used db on backup Conductor Switch: ([__func:%s], [state:%d])		
307353	Error	dbsync: Failed to restore local user db on the standby ([__func:%s])		
307358	Error	dbsync: Failed to backup the global AP database on the active MC		
307359	Error	dbsync: failed to open global AP database backup file ([DBSYNC_UDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307360	Error	dbsync: failed to stat global AP database backup file ([DBSYNC_UDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307364	Error	dbsync: failed to receive global AP db sync on standby ([__func:%s])		
307365	Error	dbsync: failed to receive global AP db sync on standby ([__func:%s])		
307366	Error	dbsync: Can not receive global AP db on backup Conductor Switch: ([state:%d])		
307367	Error	dbsync: Failed to create global AP db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307368	Error	dbsync: Failed to write global AP db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307369	Error	dbsync: Failed to restore the global AP database on the backup MC		
307370	Error	dbsync: Can not restore local used db on backup Conductor Switch: ([__func:%s], [state:%d])		
307371	Error	dbsync: Failed to restore global AP db on the standby ([__func:%s])		
307386	Error	Unexpected fatal Configuration manager runtime error in [file:%s] at [func:%s], [line:%d]	An unexpected condition occurred in the configuration manager	Contact technical support
307394	Error	dbsync: failed to mmap [description:%s] ([filename:%s]) to send to backup MC (errno= [err_msg:%s])		
307395	Error	dbsync: failed to send [description:%s] ([filename:%s], size= [file_size:%d]) over to backup MC (errno= [err_msg:%s])		
307396	Error	dbsync: failed to munmap [description:%s] ([filename:%s]) to send to backup MC (errno= [err_msg:%s])		
307397	Error	dbsync: Did not receive a CPSEC database for synchronization. Return code [retcode:%d]		
307398	Error	dbsync: failed to receive CPSEC db sync on standby ([__func:%s])		
307399	Error	dbsync: failed to restore cpsec db on standby ([__func:%s])		
307400	Error	dbsync: Not enough space to receive [filename:%s] size [size:%zu] on standby ([free:%d]M free) ([__func:%s])		
307401	Error	dbsync: failed to notify userdb of userdb time change fixup event. ([__func:%s]:[__line:%d])		
307406	Error	dbsync: failed to open IAP database backup file ([DBSYNC_IAPDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307407	Error	dbsync: failed to stat IAP database backup file ([DBSYNC_IAPDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307408	Error	dbsync: failed to receive IAP db sync on standby ([__func:%s])		
307409	Error	dbsync: failed to receive IAP db sync on standby ([__func:%s])		
307410	Error	dbsync: Can not receive IAP db on backup Conductor Switch: ([state:%d])		

307411	Error	dbsync: Failed to create IAP db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307412	Error	dbsync: Failed to write IAP db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307413	Error	dbsync: Failed to restore the IAP database on the backup MC		
307414	Error	dbsync: Can not restore IAP db on backup Conductor Switch: ([__func:%s], [state:%d])		
307415	Error	dbsync: Failed to restore IAP db on the standby ([__func:%s])		
307416	Error	dbsync: Failed to backup the IAP database on the active MC		
307430	Error	Error sending request to L2/L3 module for switch ipv6 registration	Configuration manager is unable to send switch ipv6 request message to L2/L3 module	Contact technical support
307431	Error	dbsync: failed to open License database backup file ([DBSYNC_LICENSEDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307432	Error	dbsync: failed to stat License database backup file ([DBSYNC_LICENSEDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307433	Error	dbsync: failed to receive LICENSE db sync on standby ([__func:%s])		
307434	Error	dbsync: failed to receive LICENSE db sync on standby ([__func:%s])		
307435	Error	dbsync: Can not receive LICENSE db on backup Conductor Switch: ([state:%d])		
307436	Error	dbsync: Failed to create LICENSE db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307437	Error	dbsync: Failed to write LICENSE db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307438	Error	dbsync: Failed to restore the LICENSE database on the backup MC		
307439	Error	dbsync: Can not restore LICENSE db on backup Conductor Switch: ([__func:%s], [state:%d])		
307440	Error	dbsync: Failed to restore LICENSE db on the standby ([__func:%s])		
307441	Error	dbsync: Failed to backup the LICENSE database on the active MC		
307442	Error	dbsync: failed to rename license database backup file ([filename:%s]) before sending to backup MC (errno= [err_msg:%s])		
307443	Error	dbsync: Failed to write LICENSE db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307444	Error	dbsync: failed to open Bocmgr database backup file ([DBSYNC_BOCMGRDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307445	Error	dbsync: failed to stat Bocmgr database backup file ([DBSYNC_BOCMGRDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307446	Error	dbsync: failed to receive BOCMGR db sync on standby ([__func:%s])		
307447	Error	dbsync: failed to receive BOCMGR db sync on standby ([__func:%s])		
307448	Error	dbsync: Can not receive BOCMGR db on backup Conductor Switch: ([state:%d])		
307449	Error	dbsync: Failed to create BOCMGR db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307450	Error	dbsync: Failed to write BOCMGR db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307451	Error	dbsync: Failed to restore the BOCMGR database on the backup MC		
307452	Error	dbsync: Can not restore BOCMGR db on backup Conductor Switch: ([__func:%s], [state:%d])		
307453	Error	dbsync: Failed to restore BOCMGR db on the standby ([__func:%s])		
307454	Error	dbsync: Failed to backup the BOCMGR database on the active MC		
307455	Error	dbsync: failed to rename bocmgr database backup file ([filename:%s]) before sending to backup MC (errno= [err_msg:%s])		

307456	Error	dbsync: Failed to write BOCMGR db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307457	Error	[string:%s]	details on dbsync related errors	
307458	Error	dbsync: Failed to backup the upgrade manager database on the active MC		
307459	Error	dbsync: failed to rename upgrademgr backup file ([filename:%s]) before sending to backup MC (errno= [err_msg:%s])		
307460	Error	dbsync: failed to stat upgrade manager database backup file ([DBSYNC_UDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307461	Error	dbsync: failed to receive upgrade manager db sync on standby ([__func:%s])		
307462	Error	dbsync: failed to receive upgrade manager db sync on standby ([__func:%s])		
307463	Error	dbsync: Can not receive upgrade manager db on backup Conductor Switch: ([state:%s])		
307464	Error	dbsync: Failed to write upgrade manager db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307465	Error	dbsync: Failed to restore the upgrade manager database on the backup MC		
307466	Error	dbsync: Failed to restore upgrade manager db on the standby ([__func:%s])		
307467	Error	dbsync: Failed to backup the cluster upgrade manager database on the active MC		
307468	Error	dbsync: failed to rename cluster upgrade manager backup file ([filename:%s]) before sending to backup MC (errno= [err_msg:%s])		
307469	Error	dbsync: failed to stat cluster upgrade manager database backup file ([DBSYNC_UDB_BACKUP_FILE:%s]) to send to backup MC (errno= [err_msg:%s])		
307470	Error	dbsync: failed to receive cluster upgrade manager db sync on standby ([__func:%s])		
307471	Error	dbsync: failed to receive cluster upgrade manager db sync on standby ([__func:%s])		
307472	Error	dbsync: Can not receive cluster upgrade manager db on backup Conductor Switch: ([state:%s])		
307473	Error	dbsync: Failed to write cluster upgrade manager db backup file. Interrupting db sync ([__func:%s], errno=[err_msg:%s])		
307474	Error	dbsync: Failed to restore the cluster upgrade manager database on the backup MC		
307475	Error	dbsync: Failed to restore cluster upgrade manager db on the standby ([__func:%s])		
309301	Error	[func:%s](): [msg:%s]	This shows an error message in GP	
309801	Error	[func:%s](): [msg:%s]	This shows an error message in ExtIntfMgr.	
309812	Error	[func:%s](): Assert Failed ([expr:%s]).	This indicates an assert condition failed.	
309813	Error	[func:%s](): PAPI_Init() returned failed.	This indicates failure in calling PAPI_Init.	
309814	Error	[func:%s](): PAPI_AddLocking() returned failed.	This indicates failure in calling PAPI_AddLocking.	
309820	Error	[func:%s](): ncfg_init() returned failed.	This indicates failure in calling ncfg_init.	
309821	Error	[func:%s](): sapi_init() returned failed.	This indicates failure in calling sapi_init.	
309834	Error	[func:%s](): Invalid openSSL Crypto-Locking on type:[type:%d] mode:[mode:%x] from [file:%s]:[line:%d].	This is extifmgr internal ERROR message.	
309849	Error	[func:%s](): Failed to set openSSL to FIPS mode.	This indicates failure to set openSSL to FIPS mode.	
310202	Error	[msg:%s]	Generic ERROR level system log	
310302	Error	[msg:%s]	Generic ERROR level system log	
310306	Error	[msg:%s]	Generic ERROR level system log	
310310	Error	[msg:%s]	Generic ERROR level system log	
310314	Error	[msg:%s]	Generic ERROR level system log	
310318	Error	[msg:%s]	Generic ERROR level system log	
310322	Error	[msg:%s]	Generic ERROR level system log	
310326	Error	[msg:%s]	Generic ERROR level system log	
310330	Error	[msg:%s]	Generic ERROR level system log	

311013	Error	Image upgrade failed; details follow.	The AP was unable to upgrade its image. Message 311014 will follow with details about the error.	
311014	Error	[line:%s]	This message presents detailed information about an AP image upgrade error.	
311016	Error	Unable to create domain list file	Internal error occured while accessing domain lists file.	
311017	Error	Error occured while resolving IP's for domains	Internal error occured while resolving the domain names, contact support.	
311018	Error	Unable to read domain results file	Internal error occured while processing the domain results file, contact support.	
311019	Error	Unable to generate certificate signing request (CSR). AP will reboot.	The access point was unable to generate a certificate signing request (CSR). Contact technical support.	
311020	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
311021	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
311022	Error	Error allocating memory at file [file:%s] function [function:%s] line [line:%d]. Allocating [bytes:%d] bytes.	System failed to allocate memory at the specified location	Use "show memory" and "show process" commands to monitor memory usage. Contact customer support if problem persists.
311023	Error	Error allocating memory at file [file:%s] function [function:%s] line [line:%d]. Allocating [bytes:%d] bytes.	System failed to allocate memory at the specified location	Use "show memory" and "show process" commands to monitor memory usage. Contact customer support if problem persists.
311027	Error	[msg:%s]		
312000	Error	Received STOP signal, exiting	IP multicast process was terminated unexpectedly	
312002	Error	gsm_init failed. result [rval:%d] Line [line:%d]	GSM initilization failed	
312100	Error	Received STOP signal, exiting	ESI module has terminated unexpectedly. It will be restarted	
312206	Error	[func:%s](): PAPI_Init() returned failed.	This indicates error while doing PAPI_Init().	
312207	Error	[func:%s](): PAPI_AddLocking() returned failed.	This indicates error while doing PAPI_AddLocking().	
312208	Error	[func:%s]([line:%d]): Resource allocation failed	This indicates resource allocation failed.	
312209	Error	[func:%s]([line:%d]): Parsing of request message failed. Type:[type:%d]	This indicates problem in parsing of the telemetry request message.	
312301	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the Denylist Manager process (blmgr)	
312306	Error	Connection to User DB failed	The application was not able to connect to the user database.	
312307	Error	Creation of Client Denylist tables in User DB failed	The application was not able to create the Client Denylist tables in the user database.	
312308	Error	SQL Command [command:%s] failed on User DB. Reason: [reason:%s]	This log indicates that an SQL command failed when it was executed on the user database.	
312310	Error	Update to client denylist database table failed.	This log indicates that an update to the client denylist database table failed.	
312312	Error	Client denylist is full and caused entry [mac: %m] to not be added. Limit: [limit: %d].	This log indicates that the client denylist table is full and an entry that would have been added could not be added.	
312404	Error	[msg:%s]		
312501	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the Airslice Visibility process	
312600	Error	[msg:%s]	CTB Agent encountered an Internal Error.	
313003	Error	Spanning Tree instance exceeded maximum allowed member Vlan [maxvl:%d]"	STP instance exceeded maximum number of VLANs	
313015	Error	No available entries for VLAN ID [vlanID:%d]	VLAN creation failed as maximum capacity has been reached	
313016	Error	Attempt to create a vlan with an invalid vlan id [vlanID:%d]	VLAN creation failed due to invalid VLAN ID	
313017	Error	Creation of vlan [vlanID:%d] failed	VLAN creation failed	
313019	Error	Modification of vlan [vlanID:%d] attempted before bridge initialized	Cannot modify VLAN before bridge initialization is complete	
313020	Error	Problem updating data for VLAN [vlanID:%d]	VLAN update failed	
313024	Error	Tunnel [tunid:0x%x] add failed; cannot find Vlan Interface [vlanId:%d]	An error occured while adding tunnel to VLAN, specified VLAN does not exist	

313033	Error	Removing tunnel: could not determine Link Status for vlan [vlanId:%d]	An error occured while removing tunnel from VLAN, VLAN link status cannot be determined	
313041	Error	Vlan ([vId:%d]) is not created	An error occured while configuring native VLAN of port, specified VLAN does not exist	
313043	Error	[func_name:%s]: Error Trunk State bit cannot be active for vlan [vid:%d]	An error occured while creating VLAN, a trunk port is already member of this VLAN	
313094	Error	Unable to get ifType for interface [intIfNum:%d]	An error occured during interface event handling, failed to get the interface type	
313096	Error	Unsupported ifType [ifType:%d] for interface [intIfNum:%d]	To be filled out	
313097	Error	Could not find entry for LAG interface [intf:%d] line [ln:%d]	To be filled out	
313099	Error	Failed to add member [intIfNum:%d] to LAG [lg:%d] line [ln:%d]	To be filled out	
313102	Error	Can't find member [intIfNum:%d] in LAG [lagId:%d] line [ln:%d]	To be filled out	
313103	Error	Port-Channel Failed to set member [intIfNum:%d] STP state line [ln:%d]	To be filled out	
313104	Error	Port-Channel: Failed to enable member [intIfNum:%d] to LAG [lagId:%d]	To be filled out	
313107	Error	Port-Channel: Failed to disable member [intIfNum:%d] to LAG [lagId:%d]	To be filled out	
313108	Error	Port-Channel: unable to set STP state for LAG [lg:%d]	To be filled out	
313110	Error	Port-Channel: unable to set HW Soft Disable (1) for LAG [lg:%d] return code [rc:%d]	To be filled out	
313111	Error	Port-Channel: Unable to set HW Soft Disable (2) for LAG [lg:%d] return code [rc:%d]	To be filled out	
313124	Error	[func_name:%s]: Unable to initialize amapQ	To be filled out	
313125	Error	[func_name:%s]: Unable create task	To be filled out	
313137	Error	Static ARP add failure: null MAC address for ip [ip_addr:%s] is not allowed	To be filled out	
313138	Error	Static ARP add failure: broadcast/multicast address [bcmc:%s] for ip [ip_addr:%s] is not allowed	To be filled out	
313141	Error	Cannot Delete the Old Arp Entry for [ipAddress:%s]	To be filled out	
313147	Error	[func_name:%s]: hapiArpCommand ADD failed, ip [ip:%s]	To be filled out	
313164	Error	[func_name:%s] ERROR: opening the socket [vlanId:%d] error [errstr:%s]	System encountered an internal error while deleting a routing interface	
313165	Error	[func_name:%s]: ERROR: ioctl failed when deleting the Vlan [vlanId:%d] error [errstr:%s]	System encountered an internal error while deleting a routing interface	
313182	Error	IGMP already enabled for vlan [vlanId:%d]	Conflict in IGMP configuration	
313183	Error	IGMP Proxy already enabled for vlan [vlanId:%d]	Conflict in IGMP Proxy Configuration	
313184	Error	IGMP Proxy Config conflicts with IGMP for vlan [vlanId:%d]	Conflict in IGMP Snooping/Proxy Configuration	
313186	Error	Duplicate address detection failure for link local address [ipv6addr:%s] on vlan [vlanId:%d] interface	Configured IPv6 link local interface address is duplicate and is already in use in the network.	
313193	Error	Static NBR add failure: broadcast/multicast address [mac:%s] for ip [if_ip:%s] is not allowed	Interface IPv6 neigbor entry mac is broadcast/multicast address and hence invalid	
313194	Error	AMAP List Lock initialization failed	Error message to indicate that the AMAP list lock creation is failed	
313195	Error	NIM ports Lock initialization failed	Error message to indicate that NIM ports lock creation failed	
313196	Error	MLD Proxy config conflicts with MLD for vlan [vlanId:%d]	Conflict in MLD Snooping/Proxy Configuration	
313197	Error	MLD Proxy already enabled for vlan [vlanId:%d]	Conflict in MLD Proxy Configuration	
313215	Error	PPPoE: No response from PPPoE server. Giving up - pid [pid:%d]	The PPPoE session has exited unexpectedly. The connection will be re-established	
313218	Error	PPPoE: failed to execute pppoe command	The command to initiate a pppoe session has failed.	If this error persists and the controller is unable to establish an outside link, please contact support
313227	Error	PPPoE: VLAN [pppoe_client_vlan:%d] is invalid	The VLAN on which PPPoE has been configured for is no longer valid	Check if the PPPoE vlan has been deleted, or if pppoe is no longer configured on any vlans
313234	Error	PPPoE: Switch IP Address is Modified. Switch should be rebooted	The switch LOOP back address has been changed and switch rebooted to reflect this change	Save the current configuration and restart the controller
313235	Error	PPPoE: IP Address conflicts with another Interface	The PPPoE IP address conflicts with another interface IP on the controller	Check all the VLAN interfaces IPs configured on the controller for duplicates
313236	Error	PPPoE: Cannot Set IP Address: [ipaddr:%s]	An error occured when trying to set the PPPoE interface IP	If this error persists and the controller is unable to establish an outside link, please contact support

313237	Error	PPPoE: Failed to add ARP entry for server IP: [server_ip:%s]	An error occured when trying to add the PPPoE ARP entry	If this error persists and the controller is unable to establish an outside link, please contact support
313241	Error	Static ARP: too many entries ([__FUNCTION__:%s])	A static entry could not be added to ARP table because of internal resource limits	
313243	Error	Static ARP entry add error: [__FUNCTION__:%s] failed	A static entry could not be added to ARP table because of an internal error	
313248	Error	Exceeded the Max Static Routes([RtoMaxRoutes:%d])	A new route could not be added to the database because system exceeded the maximum route capacity	
313250	Error	Error: Inserting Route into internal Route Table	Systen encountered an internal error while inserting a route entry into the database	
313251	Error	Adding a Route returning error, database corruption	System detected database corruption while inserting a route entry into the database	
313253	Error	Adding a Bad Route	To be filled out	
313261	Error	Error adding the route ([ipaddr:%s] [gateway:%s]) Route Already existsn	System did not add a route because it already existed	
313262	Error	Error adding the route([ipaddr:%s] [gateway:%s]) errno [errno:%d]n	System encountered an internal error while adding a route	
313265	Error	Error deleting the route ([ipaddr:%s] [gateway:%s]) errno [errno:%d]n	System encountered an internal error while deleting a route	
313293	Error	Exceeded the max static Ipv6 routes([RtoMaxRoutes:%d])	A new route could not be added to the database because system exceeded the maximum route capacity	
313295	Error	Error: Inserting Ipv6 route into internal route table	Systen encountered an internal error while inserting a route entry into the database	
313296	Error	Adding a Ipv6 route returning error, database corruption	System detected database corruption while inserting a route entry into the database	
313298	Error	Adding a bad Ipv6 route	To be filled out	
313322	Error	Error trying to get the vlan [vlan:%d]'s ip address, trying to retrieve the switch ip ([__FUNCTION__:%s])	An error message indicating that VRRP could not get ipaddress assigned to the VLAN	
313323	Error	Failed to retrieve switch ip ([__FUNCTION__:%s])	An error message indicating that VRRP could not get the swtich IP address	
313349	Error	Hardware interface returned an error for Command DAPI_CMD_INTF_XSECn	An internal error occured while configuring MAC address of the interface	
313366	Error	Error Cannot convert USP into Interface number slot [slot:%d] port [port:%d]	System failed to get internal interface number from slot/port	
313374	Error	Error reading the Interface Speed Status [intIfNum:%d]n	System failed to get the interface speed	
313391	Error	Failed to Configure xSec tunnel in the hardware.	An internal error occured while configuring Xsec tunnel in the hardware	
313393	Error	Data Rate returned error for interface [intIfNum:%d]n	Failed to get the interface data rate	
313401	Error	Error: Retrieving the Statisticsn	An internal error occured while retrieving port statistics	
313404	Error	Error Setting the port speed for interface [interface:%d]	An internal error occured while configuring the port speed	
313405	Error	Error setting the auto negotiation status for interface [interface:%d]	An internal error occured while configuring the auto negotiation state of the port	
313406	Error	Error setting the admin status for interface [interface:%d]	An internal error occured while configuring the admin state of the interface	
313407	Error	Error setting the address type for interface [interface:%d]	An internal error occured while configuring the address type of the interface	
313408	Error	Error setting the MTU for interface [interface:%d]	An internal error occured while configuring the MTU of the interface	
313422	Error	Converting Slot/Port [slot:%d]/[port:%d] to interface number n	Failed to get internal interface number from slot/port	
313437	Error	Port-Channel, Failed to create LAG interface [id:%d]	This is an internal error indicating failure to create a LAG interface	
313438	Error	Port-Channel, creation notification failed [id:%d]	This is an internal error indicating failure in notification of LAG creation	
313440	Error	PoE: Major persistent PoE failure detected. Likely HW failure.	POE HW failure.	
313441	Error	Unable to send messages to VRRP	An internal error message indicating that system is unable to add messages in VRRP message queue, probably because VRRP queue is full.	
313446	Error	VRRP IP address of vrid [vrid:%d] conflicts with vrid [vrid2:%d]	This message indicates that the VRRP is disabled because of IP address conflict	

313452	Error	PPPD: pppd has died unexpectedly. pid: [pid:%d]	The PPPD child process for cellular/modem device have exited unexpectedly. It will be restarted as necessary	
313455	Error	PPP: execvp failed	The PPP operation failed when calling the service provider. The operation will be retried	
313503	Error	USB device error: [errStr:%s]	FPAPPS has encountered an error while processing USB device. The operation will be retried	
313599	Error	VRRP version 3 IPv6 address of vrid [vrid:%d] conflicts with vrid [vrid2:%d]	This message indicates that the VRRP is disabled because of IP address conflict	
313602	Error	Error trying to get the vlan [vlan:%d]'s ipv6 address, trying to retrieve the switch ipv6 ([__FUNCTION__:%s])	An error message indicating that VRRP could not get the ipv6 address assigned to the VLAN	
313603	Error	Failed to retrieve switch ipv6 add ([__FUNCTION__:%s])	An error message indicating that VRRP could not get the swtich IPv6 address	
313624	Error	VRRP [version:%s] [vrid:%d] failed to start: [dbgmsg:%s]	Generic L2/L3 System debug message	
313634	Error	Function [function:%s]: GSM Publish failed for port [port:%d] with error [rval:%d]	NA	
314800	Error	NVRAM checksum error detected	The NVRAM manufacturing information is not valid, please RMA the controller	
314808	Error	Restarting CXE QE on slot [slot:%d] (possible line card malfunction)	System is restarting stuck queue engine	Please contact support
314809	Error	Reconfiguring backplane SerDes IC for slot [slot:%d]	System has reconfigured SERDES configuration on the linecard	Please contact support if the message persists
314810	Error	Power Supply mismatch; no 200W supplies should be present, ignoring for POE	NA	
314811	Error	Power Supplies only support 200W, disabling POE	NA	
314812	Error	FPGA in slot [slot:%d] with id [id:%ld] is not supported	System is unable to detect the line card or the line card is not ready	If the message persists for more than 5 minutes, please reseat the line card. Later, replace the module/line card
315005	Error	ILLegal slot number [slot:%d] in confign	This log indicates that the slot index configured exceeds the number of slots supported.	
315013	Error	Interface error: unable to shutdown VLAN [vlan:%d] interface	Operation failed when attempting to shutdown the switch vlan interface	
315020	Error	Unable to decrypt string '[key:%s]'	An error was encountered while decrypting a key	
315073	Error	Error adding tunnel [tunnel:%d] to vlan [vlan:%d]n	Operation failed when trying to add tunnel membership to specified vlan	
315130	Error	IP address conflict detected while setting the [type:%s] Ip address [ipaddr:%pI4]n	An IP address conflict was detected while validating the ip address and netmask	
315131	Error	IP address conflict detected while setting the [type:%s] Ipv6 address [ipv6addr:%s]n	An IP address conflict was detected while validating the IPv6 address	
315153	Error	No free VLAN tracking entries leftn	Unable to find anymore available VLAN tracking slots to add the new entry	
315155	Error	Unable to update cfgm on peer master ip change	The switch was unable to determine the master vrid needed to update the peer masterip info	
315259	Error	Unable to find attribute [object:%s] value in SNMP packet	SNMP agent was unable to find the attribute value when processing the information request	
315381	Error	Error reading the system temperaturen	The switch was unable to determine the current temperature	
315384	Error	Port Channel configuration retrieval encountered an internal error for channel id [id:%d]		
315385	Error	Tunnel [tunnel:%d], Error mapping vlan [vlan:%d] to IPv6 [ec:%d]n	Operation failed when trying to configure Tunnel source IPv6 with vlan i/f IPv6	
316002	Error	Unable to initialize module: [name:%s]	To be filled out	
316005	Error	Unable to initialize GSM module: [rval:%d]	Error in initializing GSM	
316019	Error	Unable to get license information	To be filled out	
316022	Error	PAPI_Send failed	To be filled out	
316023	Error	PAPI_Send failed to probe IP [ip:%s] from WMS	WMS was not able to send a message to the probe. There may be a connectivity issue.	
316062	Error	Unexpected Hash Table error. At [function:%s] line [line:%d] method [method:%s] node [node:%s] MAC [mac:%m] phy-type[phy_type:%d]	To be filled out	

316066	Error	Unexpected Mismatch in [type:%s] val1:[str1:%s]-val2:[str2:%s]	To be filled out	
316121	Error	WMS hash iteration utililty could not reposition to the last read item in the hash table. At [function:%s] line [line:%d] MAC [mac:%s]	To be filled out	
316122	Error	WMS Util Iteration Scheduler add failed. At [function:%s] line [line:%d] Iteration type: [itr_type:%d] Error msg [err_msg:%s]	To be filled out	
316287	Error	GSM iteration context could not be obtained.	There was an internal error during the creation of GSM iteration context.	
316293	Error	WMS Event Table Cleanup: [str: %s]	This log is generated when issues are detected during the periodic cleanup of the WMS Event Table.	
316295	Error	WMS failed to rename the migration data file after it was processed.	This log is generated when WMS fails to rename the migration data file after it was processed.	
316299	Error	DB query execution error in mysql_store_result for command [command:%s].	This log is generated when mysql_store_result fails to read the result of the SQL query.	
316305	Error	[log:%s] at [function:%s] line:[line:%d].	This log is generated when there is an error accessing the WMS TEST file.	
316307	Error	mysql WML server "[name:%s]" is no longer supported. Please contact support for further details.	To be filled out	
316309	Error	[function:%s]: fatal error: [reason:%s]	This log is generated when an internal error occurs within WMS.	
316311	Error	Failed to encode WMS WIDS protobuf for [event_type:%d] and [trap_id:%d]	This log indicates we failed to encode wids parameters protobuf because of that the wids message will not be adedd AMON message buffer.	
317003	Error	[str:%s]	NTP generic error message	
319000	Error	Unexpected arm (ARM) runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the ARM process.	Contact Aruba tech-support.
319001	Error	Unexpected (arm process) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the ARM process. Report to technical support.	
319065	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s], dstport [dst:%d]	Aruba inter-process communication message failed to reach destination.	
320000	Error	unknown attribute [attr:%d].	This shows an internal debug message	
322000	Error	System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
323000	Error	System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
325012	Error	Bad name length	This shows an internal error message	
325016	Error	Maximum number of NAT pools have been created.	System has the maximum allowable number of NAT pools.	Delete unused NAT pools to free up space for more pools.
325020	Error	bad attribute length ([len:%d])	This shows an internal error message	
325022	Error	Bogus VLAN ID:[vlan:%d] received.	The L2/L3 module sent a message referencing a bad VLAN ID.	Call Aruba Technical Support.
325023	Error	Internal error occurred while updating CNNAME of default factory certificate.	File system could be corrupted, reverting to default certificate failed	
325024	Error	Internal error occurred while reverting to default factory certificate.	Custom uploaded certificate could be corrupted, reverting to default certificate failed	
325031	Error	MAC auth profile not found. prof = [profile:%s]	This shows an internal debug message	
325032	Error	Error in sending message to RAP: [apip:%s]	This shows an internal debug message	
325033	Error	Send to DHCP failed	Sending message to DHCP Daemon failed	
325034	Error	[msg:%s]	Printing AUTH NVMGR Error Message	
325035	Error	PAPI_SetSendBufferSize failed[errno:%s]	PAPP Setting of Send Buffer Size failure Message	
325036	Error	unknown attribute [type:%d]	This shows an internal error message	
325037	Error	connection to devid_cache db failed	This shows an internal error message	
325038	Error	unable to create devid_cache db tables	This shows an internal error message	
325039	Error	mysql_store_result failed	This shows an internal error message	

325040	Error	Too many host names in firewall rules	This shows an internal error message	
325041	Error	value pair (0x[bptr:%p]) next ptr. (0x[bptrnext:%p]) not NULL.	This shows an internal error message	
325042	Error	Update from emweb of incorrect type [type:%d] (len [len:%d])	This shows an internal error message	
325043	Error	GSM initialization failed with error '[result:%s]'	Internal Error: gsm_initialize failed	
325044	Error	GSM publish failed for bss-auth object [bss:%s] with error '[result:%s]'	Internal Error: gsm_publish failed	
325045	Error	GSM publish failed for mac-user [sta:%s] with error '[result:%s]'	Internal Error: gsm_publish failed	
325046	Error	GSM publish failed for ip-user [ip:%s] with error '[result:%s]'	Internal Error: gsm publish failed	
325047	Error	GSM publish failed for user [uuid:%s] with error '[result:%s]'	Internal Error: gsm publish failed	
325048	Error	GSM delete failed for mac-user [sta:%s] with error '[result:%s]'	Internal Error: gsm_delete failed	
325049	Error	Memory allocation failed while allocating memory for usergroup info AMON record for mac [mac:%s]	Internal Error: malloc failed, while allocating memory for usergroup info AMON record	
326054	Error	AM: read error - [recvlen:%d]	To be filled out	
326055	Error	AM: Received frame of size 0 from driver: Is-RX=[rx:%d] BufLen= [buf_len:%d] Channel=[ch:%d]	To be filled out	
326063	Error	AM: INET not configured in this system	To be filled out	
326068	Error	AM: Cannot retrieve ARP info	To be filled out	
326071	Error	AM: System encountered an internal communication error. Error occurred when message was sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error when sending messages to each other. This could be a transient condition and the problem may go away.	If the problem persists, contact your support provider
326143	Error	AM: Received incorrect number of Rate Threshold Profile instances: [np:%d]	To be filled out	
326183	Error	AM: Can't get STA_INFO for [ifname:%s]:[rval:%d]	To be filled out	
326267	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d].	This log indicates that we encountered an internal system error	Contact your support provider
326268	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error	Contact your support provider
326269	Error	AM: System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d].	This log indicates that the application processes, in the system, encountered an error while sending messages to each other. This may be a transient condition and the problem might resolve itself.	If the problem persists, contact your support provider.
326270	Error	AM: Error allocating memory at file [file:%s] function [function:%s] line [line:%d]. Allocating [bytes:%d] bytes.	System failed to allocate memory at the specified location	Execute the show memory and show process commands to view and monitor memory usage. If the problem persists, contact your support provider.
326281	Error	AM:SM: An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error	Contact your support provider
326282	Error	AM: Received frame of size [len:%d] from driver: PktType=[type:%d] Expected len>=[buf_len:%d] Channel=[ch:%d]	This log indicates that the driver is sending packets with invalid length.	
330201	Error	System encountered an internal communication error. Error occured when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
330208	Error	[msg:%s]	This log indicates a general error other than internal/communications errors. e.g. might point to a configuration problem.	
330209	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d].	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
330210	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
330211	Error	Error allocating memory at file [file:%s] function [function:%s] line [line:%d]. Allocating [bytes:%d] bytes.	System failed to allocate memory at the specified location	Use "show memory" and "show process" commands to monitor memory usage. Contact customer support if problem persists.

330212	Error	System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
330400	Error	Unable to open [RADVD_CONF:%s] to configure RADV parameters.	Unable to write to /etc/radvd.conf. Possible reason being file system is full.	Contact Aruba tech-support.
330401	Error	Unexpected radvdwrap runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the radvdwrap	Contact technical support
334010	Error	GSM operation on device config not supported for platform	Platform does not support device config GSM operations.	
334011	Error	Profmgr GSM init failed ret: [ret:%d]	Platform initialization for device config GSM operations failed.	
334012	Error	Device config operation rejected: profmgr GSM not initialized	Platform can not support device config GSM operations before init is done.	
334015	Error	Profmgr GSM device move requested for MAC address [mac:%s], cfg path [path:%s]	Profile Manager device config object move requested.	
334016	Error	Profmgr GSM device lookup requested with MAC address [mac:%s]	Profile Manager device config GSM object look up.	
334017	Error	Device entry move/remove rejected: not provisioned from the same source. MAC address [mac:%s]	Profile Manager device move/remove request rejected because device is provisioned from a different source.	
334018	Error	Config node not found for config path [path:%s]	Profile Manager non-profile command update not able to find config node.	
334019	Error	Failed to allocate default buffers for config node [node:%s]	Profile Manager non-profile command update default buffer allocation failed.	
334020	Error	Failed to locate config buffer for config node [node:%s] appid [id:%d]	Profile Manager non-profile command update failed to locate configuration buffers.	
334023	Error	Config update for config node:[node:%s], cmd:[cmd:%s], error: [st:%s]	Profile Manager non-profile command update status.	
334024	Error	Config update failed MALLOC failure at [func:%s]	Profile Manager non-profile command update failed because of memory allocation failure.	
334026	Error	File operation failed for file [filename:%s]	Profile Manager encountered a file operation failure with config file open or update.	
334028	Error	Found unsupported command APPID[id:%d] OBJTYPE[type:%d]	Profile Manager encountered a command with APPID or OBJTYPE ID not in table.	
334029	Error	No config change detected for config commit request, current global cfg id is [id:%lld]	Profile Manager did not detect any config changes in between two commit requests.	
334200	Error	Unexpected fatal phonehome runtime error in [file:%s] at [func:%s], [line:%d]	Unexpected condition occurred in the PhoneHome manager (phonehome). Report to technical support.	
334204	Error	Received unexpected message type [ty:%d] from Station Management	NA	
334205	Error	Unexpected phonehome runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the phonehome. Report to technical support.	
334206	Error	Unexpected phonehome runtime error at [func:%s], [line:%d]: [errorstr:%s]	Unexpected condition occurred in the PhoneHome manager (phonehome). Report to technical support.	
334209	Error	PhoneHome Transaction type [tt:%s] report type [rt:%s] received unexpected event [evt:%s], previous state [ps:%s] current state [cs:%s]	PhoneHome SM received unexpected Event. This should not happen, please report to TAC	
334221	Error	PhoneHome processing error at [fn:%s] [ln:%d] reason [rs:%s]	PhoneHome hitting processing error while preparing transaction. Please report to TAC	
334301	Error	[msg:%s]	Unexpected condition occurred in the fw_visibility process	
334302	Error	[func:%s]: [msg:%s]	Unexpected condition occurred in the fw_visibility process	
334400	Error	[error:%s]	Failed to initialize SAPI	
334402	Error	[error:%s]	Failed to initialize NCFG	
334403	Error	time() failed [error:%s]	Dispatcher timer failed to get time	
334404	Error	Failed to send PAPI msg [error:%d]	Failed to send PAPI message	
334406	Error	[error:%s]	Encountered failure sending mail to SMTP server	
334411	Error	[error:%s]	Util Proc general errors	
334500	Error	PAPI_Alloc() failed [__FUNCTION:%s]		
334502	Error	[__FUNCTION:%s]: Rcvd msg with opcode [opcode:0x%x]		
334503	Error	Error registering sibyte opcode [opcode:0x%x] [__FILE:%s] [__LINE:%d]		
334504	Error	[__FUNCTION:%s]: malloc failed		

334505	Error	Error registering OSPF callbacks [erc:%d]		
334506	Error	RTO Init failed [erc:%d]		
334507	Error	Management object set failed [erc:%d]		
334508	Error	Failed to create OSPF area [area:%s]		
334509	Error	Failed to create OSPF subnet [addr:%s] [mask:%s]		
334511	Error	[__FUNCTION:%s]: B_NewEx Failed		
334512	Error	[__FUNCTION:%s]: F_NewEx Failed		
334524	Error	[__FUNCTION:%s]: ARO_Id not yet set on Intf [intf:%s] Event [event:%s]		
334525	Error	OSPFv2 entering overload state. To restore OSPF to full operation, disable and re-enable OSPF		
334530	Error	FlushLsa called with NULL area for LSA without AS flooding scope		
334531	Error	Virtual link [link:%s] transit area not set		
334533	Error	[__FUNCTION:%s]: No area object		
334541	Error	[__FUNCTION:%s]: Failed to allocate memory		
334543	Error	NetLsaCheckPresense called with incorrect database entry. LS type is [type:%d]		
334547	Error	IFO_Init failed for intf [intf:%s] with err [err:%d]		
334548	Error	IFO_Config failed for intf [intf:%s] with err [err:%d]		
334549	Error	IFO_MetricConfig failed for intf [intf:%s] with err [err:%d]		
334550	Error	IFO_AuthKeyConfig failed for intf [intf:%s] with err [err:%d]		
334551	Error	[__FUNCTION:%s]: RTO_Config failed with err [err:%d]		
334552	Error	Unable to decrypt string '[key:%s]'		
334555	Error	Socket config failed for intf [intf:%s] with err [err:%d]		
335000	Error	Fan failure detected: [data:%d] [func:%s]	A possible chassis fan falure has been detected. Fan could need replacement.	
335001	Error	Voltage failure detected: [desc:%s] [data:%f]	A card voltage is out of tolerance. Card could need replacement.	
335003	Error	Single bit ECC error detected: [row:%x] [col:%x] [ba:%x]	A possible memory falure has been detected.	
335004	Error	Multi bit ECC error detected: [row:%x] [col:%x] [ba:%x]	A possible memory falure has been detected.	
335011	Error	Power Supply [PSid:%d] [Status : %s].	PS failure or missing.	
335013	Error	Power Supply [PSid:%d] Not Supported.	Non Supported PS.	
335015	Error	Fan Tray Removed.	Fan Tray Removed.	
335017	Error	Fan Absent detected: [data:%d] [func:%s]	A possible chassis fan absent has been detected.	
335101	Error	[msg:%s]	Unexpected condition occurred in the Misc process (misc-proc)	
335102	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the Misc process (misc-proc)	
335300	Error	PAPI_Alloc() failed [__FUNCTION:%s]		
335301	Error	PAPI_Send() failed for [__FUNCTION:%s]		
335303	Error	[__FUNCTION:%s]: Failed to allocate memory		
335500	Error	Unable to open [DHCPD_CONF:%s] to configure DHCP parameters.	Unable to write to /etc/dhcpd.conf. Possible reason being file system is full.	Contact Aruba tech-support.
335504	Error	Error: [error:%d] while initializing GSM for DHCP-RELAY.	DHCP-RELAY GSM initialization failure.	
335505	Error	Error: DHCP-OPTION82 XML parsed bytes NULL.	DHCP-OPTION82 XML parsing failure	
335506	Error	Error: DHCP-OPTION82 XML circuit ID bytes zero.	DHCP-OPTION82 XML Circuit ID parsing failure.	
335507	Error	Error: DHCP-OPTION82 XML remote ID bytes zero.	DHCP-OPTION82 XML Remote ID parsing failure.	
336001	Error	[msg:%s]	Unexpected condition occurred in Spectrum process	
336002	Error	[func:%s], [msg:%s]	Unexpected condition occurred in Spectrum process	
336008	Error	Spectrum process server socket is stuck. Recreating it.	Spectrum process server socket is stuck. Recreating it.	
339301	Error	[msg:%s]	Unexpected condition occurred in the rtpa process	
339302	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the rtpa process	
341005	Error	[msg:%s]		
341023	Error	Error setting global LED mode at [node:%s].	The AP is configuring LED mode.	
341026	Error	Fail to save configuration, error-[error:%s].	The AP is saving configuration .	
341027	Error	Fail to initial configuration, error-[error:%s].	The AP is initialing configuration .	
341028	Error	Image version format invalid: [version:%s].	The AP is upgrading image.	

341029	Error	Compare image version fail, old version-[old_version:%s], current version-[new_version:%s].	The AP is upgrading image.	
341030	Error	Upgrade version fail, from version [old_version:%s] to [new_version:%s].	The AP is upgrading image.	
341031	Error	Retrieve image fail, retry [time:%d].	The AP is loading configuration.	
341033	Error	Read configuration fail, error-[error:%s].	The AP is loading configuration.	
341034	Error	Save configuration fail, error-[error:%s].	The AP is saving configuration.	
341036	Error	[func:%s]: invalid image name.	The AP is upgrading image.	
341037	Error	Open image-[image:%s] fail.	The AP is upgrading image.	
341038	Error	Read image-[image:%s] header fail.	The AP is upgrading image.	
341039	Error	AP check image-[image:%s] version fail.	The AP is upgrading image.	
341040	Error	AP verify image-[image:%s] fail.	The AP is upgrading image.	
341041	Error	AP basic verify image-[image:%s] fail.	The AP is upgrading image.	
341042	Error	AP check image-[image:%s] version for mesh fail.	The AP is upgrading image.	
341044	Error	AP can't open MTD device-[device:%s].	The AP is setuping image.	
341047	Error	AP regulatory domains don't match Conductor-[id1:%d], member-[id2:%d], reason-[reason:%d].	The AP is upgrading image.	
341048	Error	Controller doesn't allow new AP-[mac:%s], reboot it.	The AP is upgrading image.	
341049	Error	[func:%s]: AP malloc sync list fail.	The AP is upgrading image.	
341050	Error	AP setup image fail, ret-[ret:%d].	The AP is setuping image.	
341051	Error	AP verdor name not match, Conductor-[name1:%s], Member-[name2:%s].	The AP is setuping image.	
341052	Error	[func:%s], [line:%d]: AP class not match, Conductor-[class:%d], Member-[class2:%d].	The AP is setuping image.	
341054	Error	[func:%s]: can't find right iurl for AP-[mac:%s], [ip:%s], class [class:%s].	The AP is upgrading image.	
341055	Error	[func:%s]: find right iurl for AP-[mac:%s], url [url:%s].	The AP is upgrading image.	
341056	Error	AP can't find image file-[file:%s].	The AP is upgrading image.	
341058	Error	AP download image state-[state:%d] error.	The AP is upgrading image.	
341063	Error	Could not open socket for [dip:%x]/[mask:%x].	The AP is setting kernal route.	
341064	Error	Could not add route for [dip:%x]/[mask:%x] [gw:%x].	The AP is setting kernal route.	
341067	Error	Open socket for corp fail [dip:%x]/[sip:%x]/[devname:%s].	The AP is creating tunnel.	
341068	Error	Get ifindex for corp fail [dip:%x]/[sip:%x]/[devname:%s].	The AP is creating tunnel.	
341070	Error	No space for corp tunnel [dip:%x]/[sip:%x]/[devname:%s].	The AP is creating tunnel.	
341072	Error	AP could not find post auth role [name:%s].	The AP is creating SSID.	
341074	Error	AP can't find essid-[name:%s].	The AP is creating SSID.	
341081	Error	No space for acl-[name:%s].	The AP is configuring ACL.	
341082	Error	ACL index-[index:%d] is invalid.	The AP is configuring ACL.	
341083	Error	ACL index-[index:%d] is inuse.	The AP is configuring ACL.	
341089	Error	[func:%s]: [line:%d]: AWC login error.	The AP is upgrading image from awc.	
341090	Error	[func:%s]: [line:%d]: could not save file.	The AP is upgrading image from awc.	
341092	Error	[func:%s]: [line:%d]: Parse error in payload.	The AP is upgrading image from awc.	
341093	Error	[func:%s]: [line:%d]: required class [class:%u] not found in payload.	The AP is upgrading image.	
341094	Error	[func:%s]: no class in url.	The AP is upgrading image.	
341095	Error	[func:%s]: url is NULL!.	The AP is upgrading image.	
341107	Error	[func:%s]: [line:%d] Cannot get essid from datapath for client-[ip:%s] port-[port:%s].	Handle papi message.	
341108	Error	[func:%s]: [line:%d] invalid session client-[ip:%s] sid-[sid:%s].	Handle papi message.	
341109	Error	[func:%s]: save certificate fail-[error:%s].	AP is setting cert.	
341110	Error	[func:%s]: delete certificate fail-[error:%s].	AP is setting cert.	
341111	Error	[func:%s]: save cert key fail-[error:%s].	AP is setting cert.	
341113	Error	[func:%s]: get gre host fail by [server:%s].	AP is setting gre name.	
341114	Error	[func:%s]: set gre name-[name:%s] fail.	AP is setting gre name.	
341116	Error	[func:%s]: clr gre name-[name:%s] fail.	AP is setting gre name.	
341118	Error	[func:%s]: create session fail for ip-[ipaddr:%s].	AP is creating session.	
341119	Error	[func:%s]: SID not match for IP-[ip:%s] sid-[sid:%s].	Handle papi message.	
341122	Error	[func:%s]: Malloc fail [num:%d].	Station sync.	
341123	Error	[func:%s]: [line:%d] parse token ret-[ret:%d].	Station sync.	

341130	Error	[func:%s], [line:%d]: ioctl fail ipaddr-[ip:%d] mac-[mac:%s] add-[add:%d].	AP is configuring arp entry.	
341141	Error	[func:%s], [line:%d]: bid is [bid:%d], max bid is [max_bid:%d].	Invalid branch ID.	
341143	Error	[func:%s],[line:%d]: could not get class-[class:%s] in payload.	AP receive upgrade message from airwave to update image.	
341144	Error	[func:%s],[line:%d]: could not find file-[file:%s].	AP is executing "show support-commands".	
341163	Error	Fail to add ids radio [mac:%m].	Fail to add ids radio.	
341210	Error	[func:%s]: ASAP to CLI socket open failed [errno:%d].	ASAP to CLI socket open failed.	
341211	Error	[func:%s]: ASAP to CLI socket ioctl failed [fd:%d] [errno:%d].	ASAP to CLI socket ioctl failed.	
341212	Error	[func:%s]: ASAP to CLI socket bind failed [fd:%d] [errno:%d].	ASAP to CLI socket bind failed.	
341213	Error	[func:%s]: ASAP to CLI socket recv failed [fd:%d] [errno:%d].	ASAP to CLI socket recv failed.	
341214	Error	[func:%s]: L2 Roam failed at home network [mac:%s] [ssid:%s].	L2 Roam failed at home network.	
341224	Error	[func: %s]: [nodename:%s], errno [errno:%s] info [info:%s].	sysctl fw from cli error.	
341230	Error	Controller denys new AP when upgrading-[mac:%s].	Controller denys new AP for upgrading image.	
341232	Error	Fail to retrieve ap config from flash after [retry:%d] retries.	fail to retrieve ap config from flash	
341235	Error	Add [mac:%s] to subscription ap list failed.	Add ap to subscription ap list failed	
341270	Error	set priority failed, failed to find type [type:%d], sub port [port:%d], priority [priority:%d].	set priority failed.	
341271	Error	ethernet [port_name:%s] link down.	ethernet link down.	
341272	Error	ethernet [port_name:%s] link up.	ethernet link up.	
341292	Error	ale: encode [msg_type:%s] message failed, err_msg:[err_msg:%s].	encode message failed.	
341293	Error	ale: encode [msg_type:%s] message tag for field failed, err_msg:[err_msg:%s].	encode message tag for field failed.	
341294	Error	ale: encode [msg_type:%s] message failed because of full buffer, bytes_written [bytes:%d], max size [max:%d]	encode message failed because of full buffer.	
341303	Error	ale: receive a wrongly reported rssi message from [ip:%s].	access point op.	
341315	Error	Failed to validate regulatory file, error=[err:%d].	Failed to validate regulatory file	
341316	Error	Failed to decrypt and decompress regulatory file, error=[err:%d].	Failed to decrypt and decompress regulatory file	
341336	Error	[msg:%s]	netlink error message	
341340	Error	uplink [uplink_name:%s] receive vlan down.	uplink vlan down.	
341341	Error	uplink [uplink_name:%s] receive vlan up.	uplink vlan up.	
342001	Error	[msg:%s]	Unexpected condition occurred in the Misc process (misc-proc)	
342002	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the Misc process (misc-proc)	
343000	Error	[thread:%u] Unexpected fatal mDNS proxy runtime error in [file:%s] at [func:%s] [line:%d]	Unexpected condition occurred in mDNS proxy	Contact tech-support.
343001	Error	[thread:%u] mDNS proxy runtime error at [func:%s] [line:%d] [data:%s]	Unexpected condition occurred in mDNS proxy (mdns)	Contact tech-support.
343502	Error	[func:%s] [line:%d] [msg:%s]	System related error messages logged in AirGroup	Contact tech-support
344000	Error	Unexpected fatal DDS runtime error at [func:%s] [line:%d] [data: %s]	Unexpected condition occurred in DDS	Contact tech-support.
345301	Error	[msg:%s]	Unexpected condition occurred in the GSM Manager process (gsmmgr)	
345302	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the GSM Manager process (gsmmgr)	
346000	Error	Unexpected fatal HA runtime error in [file:%s] at [func:%s] [line:%d]	Unexpected condition occurred in HA	Contact tech-support.
346001	Error	HA error at [func:%s] [line:%d] [data:%s]	Unexpected condition occurred in HA	Contact tech-support.
347000	Error	Unexpected UCC runtime error at [func:%s], [line:%d]	Unexpected condition occurred in UCM.	
347001	Error	Unexpected UCC runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in UCM.	
347004	Error	Unexpected stm (Station management) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the station manager (stm)	Contact Aruba tech-support.
347006	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s], dstport [dst:%d]	Aruba inter-process communication message failed to reach destination.	
347010	Error	PAPI_Send failed, [func:%s], [line:%d]: [error:%s]	Aruba inter-process communication message failed to reach auth manager.	
347011	Error	[msg:%s]	System related error messages logged in UCM.	
348301	Error	[msg:%s]	Unexpected condition occurred in the IPSTM process (ipstm)	
348302	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the IPSTM process (ipstm)	
350000	Error	Error configuring Apache with sygate failure URL	Failed to change the HTTPD sygate firewall rewrite configuration in the HTTPD configuration file	If error persists, please contact technical support

350007	Error	Error determining certificate Common Name	Failed to verify the HTTPD certificate	Please replace the HTTPD certificate with a valid one
350008	Error	SSL Library Error: [err:%s] [data:%s] [annotate:%s]	Error in SSL Library	
351000	Error	Received STOP signal, exiting	IP multicast process was terminated unexpectedly	
351002	Error	gsm_init failed. result [rval:%d]	GSM initilization failed	
351003	Error	gsm_replay failed. result [rval:%d]	GSM replay failed	
351004	Error	gsm_start_receiving_events failed. result [rval:%d]	GSM start recieving events failed	
351005	Error	DisplatcherCreate failed	NA	
351006	Error	PAPI_Init failed	PAPI initialization failed	
351007	Error	sapi_Init failed	SAPI initialization failed	
351011	Error	Invalid Physical Port [port:%d] passed at Function: [function:%s]	NA	
351012	Error	LLDP Timer Create failed for interval [sec:%d]	NA	
351013	Error	LLDP Timer Restart failed for interval [sec:%d]	NA	
351015	Error	LLDP PAPI_Alloc failed at Function: [function:%s] for port [port:%d]	NA	
354001	Error	[message:%s][function:%s], [file:%s]:[line:%d]	WEB_CC module generic SYSTEM error	
354005	Error	Error registering sibyte opcode [opcode:0x%x] [__FILE:%s] [__LINE:%d]	WEB_CC module generic SYSTEM error	
354007	Error	PAPI alloc failed : [__FUNCTION : %s]		
354008	Error	PAPI send failed : [opcode:0x%x] [__FUNCTION : %s] [errno : %d] [errStr : %s]		
354009	Error	[msg : %s] : [retval:%d] [gsmstr : %s] [_FUNCTION : %s]		
354010	Error	Failed GSM publish [_FUNCTION : %s] [retval : %d] [cat : %d] [rep : %d] [url : %s]		
354012	Error	Failed GSM delete [_FUNCTION : %s] [retval : %d]		
354021	Error	[__FUNCTION:%s]: bca_init failure : [__LINE : %d]		
354028	Error	[__FUNCTION:%s]: DB download failed . [rc : %d] [is_update : %d]		
355001	Error	[func:%s]: [msg:%s]	Unexpected condition occurred in cert download mgr.	Contact tech-support.
356001	Error	[msg:%s]	RNG mgr module system error	
356100	Error	[msg:%s] [func:%s] [line:%d]	Unexpected condition occurred in the dpagent process	
356301	Error	[msg:%s]	Unexpected condition occurred in Mcell process	
356311	Error	amon_init returned an error [error:%d]... exiting	Error message about a condition in Mcell process	
356318	Error	GSM [event:%s] failed [errcode:%d]	Error message about a condition in Mcell process	
356326	Error	AP Delete AP not found by key [id:%m]	Error message about a condition in Mcell process	
356327	Error	Radio Upsert Radio [rad:%m] is being added but no AP knows this radio. Skip	Error message about a condition in Mcell process	
356328	Error	Radio Upsert AP [ap:%s] ran out of radio_tbl slot while adding radio [rad:%m]	Error message about a condition in Mcell process	
356331	Error	Radio Delete Update Radio [radio:%m] being deleted but its parent AP does not exist.	Error message about a condition in Mcell process	
356332	Error	Radio Delete Radio [str:%s] being deleted but its parent AP [bss:%m] does not think the radio was a child	Error message about a condition in Mcell process	
356359	Error	Assert Failed	Error message about a condition in Mcell process	
356360	Error	Invalid to allocate 0 bytes in memory. Probably you did not handle the data type properly. Abort now.	Error message about a condition in Mcell process	
356361	Error	Memory allocation failed - Assert failed	Error message about a condition in Mcell process	
357000	Error	Unexpected fatal CFGDIST runtime error at [func:%s] [line:%d] [data: %s]	Unexpected condition occurred in Config Distributor	Contact tech-support.
358000	Error	[msg:%s]	Unexpected condition occurred in the dhcpdproxy process	
358001	Error	[func:%s]: [msg:%s]	Unexpected condition occurred in the dhcpdproxy process	
359000	Error	Unexpected HCM runtime error at [func:%s] [line:%d] [data: %s]	Unexpected condition occurred in HCM.	Contact tech-support.
360001	Error	[msg:%s]	Unexpected condition occurred in the ip_flow_export process	
360002	Error	[func:%s]: [msg:%s]	Unexpected condition occurred in the ip_flow_export process	
360008	Error	Unexpected (ip_flow_export process) runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the ip_flow_export process. Report to technical support.	
360009	Error	Unexpected (ip_flow_export process) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the ip_flow_export process. Report to technical support.	
362000	Error	[msg:%s]	Unexpected Initialization Error	
371000	Error	Validation failed command:"[cmd:%s]" error:"[err:%s]"	Validation for command has failed.	
371002	Error	Datastore error at node:"[node:%s]" appId:[app:%s] obj:[obj:%s] - [msg:%s]	Datastore error during validation.	

371003	Error	Invalid rfc-3576 udp-port	Validation for command has failed.	
371004	Error	Invalid args to validation function [name:%s]	Invalid arguments to function.	
371005	Error	Datastore lookup failed at function name: "[name:%s]" node:"[node:%s]" obj:"[obj:%s]" errcode:"[errcode:%d]"	Datastore lookup failure during Validation	
371006	Error	Failed to configure system cmd: "[cmd:%s]" node:"[node:%s]" flags:"[flags:%x]" ret:"[code:%d]"	Failure to configure internal system command during validation	
371007	Error	[function:%s](Role:[name:%s]): VLAN:[vlan:%s] is not configured	VLAN referred by role not found	
371008	Error	Failed to create node iterator in [func:%s] for node [node:%s]	Error creating node iterator	
371009	Error	Error while acquiring profile ref for [type:%s]:[prof: %s] by [np:%s] at node [node:%s]	Error acquiring profile reference	
371010	Error	Error while releasing profile ref for [type:%s]:[prof: %s] by [np:%s] at node [node:%s]	Error releasing profile reference	
371011	Error	Error while reading radius dictionary	Error while reading radius dictionary	
371012	Error	Unknown profile [type:%s]:[name:%s]	Unknown profile type	
371013	Error	Error while releasing np ref for [type:%s]:[obj: %s] by [np:%s] at node [node:%s]	Error releasing non-profile reference	
371016	Error	Max acls used: [count:%d] at node [node:%s]	Due to some configuration/function which includes ACL entries to be created/updated has miscalculated the ACL count. Probably, somewhere ACL count has been over counted, or MAX_ACLS limit check has been missed.	
380001	Error	[string:%s]	logfwdwrap encountered an Internal Error	
381001	Error	[msg:%s]		
381002	Error	[func:%s], [msg:%s]		
386003	Error	[msg:%s]	UDMD system error	
390001	Error	[msg:%s]	Unexpected condition occurred in the Misc process (misc-proc)	
390002	Error	[func:%s], [msg:%s]	Unexpected condition occurred in the Misc process (misc-proc)	
391001	Error	[message:%s][function:%s], [file:%s]:[line:%d]	APPRF module generic SYSTEM error	
391003	Error	Error registering sibyte opcode [opcode:0x%x] [__FILE:%s] [__LINE:%d]	APPRF module generic SYSTEM error	
391004	Error	Error allocating memory for PAPI msg [function:%s]	APPRF module generic SYSTEM error	
391005	Error	Error sending PAPI message of type [opcode:0x%x] [function: %s]	APPRF module generic SYSTEM error	
392000	Error	Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
392500	Error	System encountered an internal communication error. Source [src:%s] destination [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
393000	Error	DPIMGR: [func:%s] [line:%d] [msg:%s]	Unexpected condition occurred in DPI MGR	Contact tech-support.
394002	Error	[msg:%s]	Generic error level system log	
394101	Error	Received STOP signal, exiting	IP multicast process was terminated unexpectedly	
397000	Error	[msg:%s]	Unexpected condition occurred in DDNS_CLIENT	Contact tech-support.
398500	Error	Unexpected Policymgr runtime error at [func:%s] [line:%d] [data: %s]	Unexpected condition occurred in Policymgr.	Contact tech-support.
398508	Error	Bad name length	This shows an internal error message	
398527	Error	[msg: %s]	This shows an internal error message.	
398530	Error	Reached maximum entry count 128 in Policy [name:%s].	This shows an internal debug message.	
398535	Error	[function:%s]:[line:%d] Memory allocation failed.	This shows an internal debug message.	
398550	Error	Unexpected Policymgr runtime error at [func:%s] [line:%d] [data: %s]	Unexpected condition occurred in Policy manager uplink.	Contact tech-support.
398560	Error	register failed for id = [id:%d], name = [name:%s]	This shows an internal error message	
398561	Error	Message to [ip:%s]:[port:%d]([app_name:%s]) with MsgCode [msg_code:%d], Msglen [len:%d], and Msgtype [msg_type:%d] failed with Errno [errno:%d], Errstr [errstr:%s]		
398584	Error	PAPI_SetSendBufferSize failed[errno:%s]	PAPI Setting of Send Buffer Size failure Message	

398585	Error	GSM initialization failed with error '[result:%s]'	Internal Error: gsm_initialize failed	
399000	Error	[msg:%s]	Unexpected Initialization Error	
399002	Error	[msg:%s] [lagId: %d] [slot: %d] [port: %d]		
399006	Error	[msg:%s]		
399007	Error	papi send failed for lacp message on egress [intf:%x]		
399008	Error	[msg: %s] [intf:%x]		
399009	Error	[msg: %s]		
399500	Error	[module:%s] [msg:%s]	Unexpected condition occurred in LHM	Contact tech-support.
399600	Error	[msg:%s] [func:%s] [line:%d]	Unexpected condition occurred in the apimagemgr process	
399700	Error	System encountered an internal communication error. Source [src:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
399750	Error	Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d] error [error:%s].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
399800	Error	Error allocating memory at file [file:%s] function [function:%s] line [line:%d]. Allocating [bytes:%zu] bytes.	System failed to allocate memory at the specified location	Use "show memory" and "show process" commands to monitor memory usage. Contact customer support if problem persists.
399801	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d].	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
399802	Error	System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] destination application [dst:%s] at file [file:%s] function [func:%s] line [line:%d].	This log indicates that application processes in the system encountered an error sending messages to each other. This could be a transient condition and the problem might go away. In case the problem persists please contact the technical support.	
399803	Error	An internal system error has occurred at file [file:%s] function [function:%s] line [line:%d] error [error:%s].	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
399805	Error	Operation timed out [operation:%s] in [function:%s], [file:%s]:[line:%d].	This log indicates that the operation timed out while sending a data packet, or while waiting for a status acknowledgement from a peer. This may be the result of a remote host that is unreachable and the problem may be resolved once the remote host becomes available. In case the problem persists please contact the technical support.	
399807	Error	Configuration error: [msg:%s] [code:%d] in [function:%s], [file:%s]:[line:%d].	This log indicates that a configuration error has occurred.	
399810	Error	System socket error detected, errno [errno:%d] in [function:%s], [file:%s]:[line:%d].	This log indicates that the system encountered a problem while opening/communicating with a system socket	
399812	Error	Internal communication error while sending a message from application [src:%s] with opcode [op:%s] to datapath at file [file:%s], function [function:%s], line [line:%d]	Application processes in the system encountered an error sending message to the datapath. This could be a transient condition and the problem might go away	In case the problem persists, please contact the technical support
399813	Error	System encountered an internal communication error. Error occurred when message is being sent from source application [src:%s] to destination application [dst:%s] on ap [ip:%pI4][bssid:%m] at file [file:%s] function [func:%s] line [line:%d].	An application processes on the controller encountered an error sending message to AP. This could be a transient condition and the problem might go away.	In case the problem persists, please contact the technical support
399816	Error	[error:%s]	This is an internal system error log	This is a transient condition, please contact the technical support if the problem persists
399822	Error	Unable to [actionToFrom:%s] hardware in [function:%s], [file:%s]:[line:%d].	There was an error accessing the hardware data	If this problem persists please contact Aruba's support team.
399827	Error	|webserver| [error:%s]	This is a webserver internal error log	
399832	Error	|webserver| [error:%s]	This is a webserver error log.	

399833	Error	Error, forwarding traps to the controller.	This log indicates that an AP process failed to send a trap to the controller.	
399834	Error	Unable to close system file [sys_file:%s] in [function:%s], [file:%s]:[line:%d].	This log indicates that we were unable to close a system file. This indicates an internal system error, and could cause problems.	
399840	Error	Environment var [var: %s] is invalid	This is an system error log.	
399841	Error	Configuration error: [msg:%s] [code:%s] in [function:%s], [file:%s]:[line:%d].	This log indicates that a configuration error has occurred.	
300001	Info	Mobile IP service is enabled at line [ln:%d]	Mobility service is enabled with "router mobile" cli command	
300002	Info	Mobile IP service is disabled at line [ln:%d]	Mobility service is enabled with "no router mobile" cli command	
300003	Info	Mobile IP service initialization complete!	Mobile IP service has completed initialization and is ready to handle mobile clients, if enabled. This message is always logged regardless if mobility is enabled or not with "router mobile" cli command	
300011	Info	Mobileip at [func:%s], [line:%d]: [errorstr:%s]	Information message mobileip prints to monitor proper Initialization	
300100	Info	Starting license manager [[expiry:%u] day expiry]	The license manager is starting. The expiry interval for evaluation licenses is displayed	
300105	Info	[function:%s]: removing key [key:%s], for feature [feature:%s] [[id:%d]]; model is [model:%s]	During a model upgrade, the listed key was removed as it is not valid for the new model.	
300118	Info	Successfully created the license database	A new license database was created successfully at system initialization time.	
300122	Info	All licenses deleted successfully	All licenses were successfully deleted.	
300126	Info	OS variant is [os:%s]	This message indicates the OS variant of the operating system, for informational purposes.	
300139	Info	Upgrading of [name:%s] license to the new licensing scheme failed	This means when the controller is upgraded to the latest image, we tried to update the licenses, but failed. It will result in restricted functionality	
300143	Info	[function:%s]: Successfully exported the License Database to file: [file:%s]	Successfully exported the license database.	
300148	Info	[function:%s]: Successfully imported the License Database from file: [file:%s]	Successfully imported the license database.	
300165	Info	[function:%s]: Deleting key [key:%s] for [limit:%d] [lim_name:%s]	Deleting the key for limit license.	
300166	Info	[function:%s]: Deleting key [key:%s] for [feat_name:%s]	Deleting the key for feature license.	
300169	Info	[function:%s]: Enabling key [key:%s] for [limit:%d] [lim_name:%s]	Enabling the limit license key.	
300170	Info	[function:%s]: Enabling key [key:%s] for [feat_name:%s]	Enabling the feature license key.	
300171	Info	[function:%s]: Disabling key [key:%s] for [limit:%d] [lim_name:%s]	Disabling the limit license key.	
300172	Info	[function:%s]: Disabling key [key:%s] for [feat_name:%s]	Disabling the feature license key.	
300173	Info	License database being recreated	License database is being recreated.	
300175	Info	License database created successfully	Successfully created a new License Database.	
300186	Info	[function:%s]: Creating the license database...	Creating the license database...	
300191	Info	[function:%s]: All licenses being deleted	All licenses about to be deleted.	
300200	Info	Starting transport service	The transport service is starting.	
300202	Info	MMS Config sync is already in progress, new request ignored. State [state:%d]	The system received a request to sync its configuration with the MMS server, but a configuration sync is already being performed. The new sync request will be dropped. Please wait for the current sync to finish before trying again.	
300203	Info	MMS Config sync rejected per switch configuration.	The system received a request to sync its configuration with the MMS server, however the switch has been configured to not accept MMS configuration syncs. The sync request will be dropped.	
300306	Info	FIPS Info: [msg:%s]	This is a FIPS info log in system module.	
300502	Info	[func:%s], [line:%d], [msg:%s]	System related info messages logged in the user visibility process	
300802	Info	[msg:%s]		
300901	Info	[name:%s]	This is an internal info message	

301000	Info	SNMP Agent is initialized		
301001	Info	Agent Processing Switch IP change.		
301004	Info	Del: Boot And Time doesn't have an Entryn	BootTime Table entry missing	
301226	Info	Cannot process SNMP Requests: SNMP is Disabled	To_be_filled_out	
301228	Info	Source address is a broadcast address ([sin_addr:%s])	To_be_filled_out	
301252	Info	Sendto failed, unable to send inform to manager [tst:%s].	To_be_filled_out	
301258	Info	Received Inform response length is zero	To_be_filled_out	
301260	Info	Error parsing response/report to InformRequest(code: [code:%d])	To_be_filled_out	
301263	Info	Received a Not in Time Window Report	To_be_filled_out	
301264	Info	Received an unknown Engine ID report, Inserting authSnmpID	To_be_filled_out	
301265	Info	Received an unknown user Name report, Inserting authSnmpID	To_be_filled_out	
301269	Info	Error Making the Trap PDU	To_be_filled_out	
301270	Info	Error Making the UpTime VarBind	To_be_filled_out	
301271	Info	Error Making the Over Flow Trap OID	To_be_filled_out	
301272	Info	Error Making the Trap OID	To_be_filled_out	
301273	Info	Error Making the Time VB	To_be_filled_out	
301274	Info	Error Making the Host IP OID	To_be_filled_out	
301275	Info	Error Making the Host IP VB	To_be_filled_out	
301276	Info	Error Making the Host Port OID	To_be_filled_out	
301277	Info	Error Making the Host Port VB	To_be_filled_out	
301278	Info	Authentication failure, bad community string	To_be_filled_out	
301289	Info	Cannot Delete the User, User is used in Trap Host configuration. Delete the Trap Host configuration before deleting the user	To_be_filled_out	
301311	Info	Trying to insert the same host twice	To_be_filled_out	
301328	Info	Error Adding a Row in the Fault table	To_be_filled_out	
301329	Info	Completed AMP Initialization	To_be_filled_out	
301335	Info	Switch IP is not configured yet, ignoring the message	To_be_filled_out	
301340	Info	Initialized SNMP Agent	To_be_filled_out	
301341	Info	Switch IP Address is not configured	To_be_filled_out	
301400	Info	Unable to transition to new MMS server [ipaddr:%pI4]: Mobility server not configured.	The controller was unable to transition to a new MMS server since it's not being configured. Please make sure the MMS server is configured correctly under the mobility-manager command.	
301401	Info	Successfully transitioned to new MMS server [ipaddr:%pI4]	The controller successfully transitioned to the new MMS master server.	
301402	Info	New MMS server [ipaddr:%pI4] transition cancelled: Old MMS master still active	The transition to the new MMS master server was cancelled because the old master is still communicating with the controller. This can happen if the link between the MMS servers have been lost and both servers believe they are the master. Please make sure MMS server redundancy is working correctly.	
301403	Info	Transition to new MMS server [ipaddr:%pI4] started	The controller has received a communication request from a new MMS master and is in the process of transitioning to the new MMS master.	
301404	Info	Restarting transition for new MMS server [ipaddr:%pI4]	While in the transition process, the controller have received a communication request from a new MMS server that isn't the old active server. The pending transition is cancelled and the controller will now try to transition to the new MMS master server.	
301408	Info	Setting MMS server [ipaddr:%pI4] to active: [action:%s]	SNMP agent message for when we set a new active MMS server.	
301437	Info	[func:%s] [line:%d] MMS SYNC request error [err:%s]	An error has occurred during the validation of the MMS config sync request	

303002	Info	Nanny is starting; reboot is [enabled:%s]	Process Manager is active and will start monitoring other processes. If Reboot flag is enabled, system will reboot under certain conditions such as low memory and system critical process dying	
303092	Info	Completed SW FIPS KAT test	NA	
304037	Info	VPOOL: Initialized VLAN pool for virtual AP '[name:%s]' (size=[size:%d], VLAN-MAP=[addr:%p], Refcnt=[cnt:%d])		
304038	Info	VPOOL: VLAN Pool already initialized for VLAN-MAP [addr:%x], refcnt [cnt:%d]		
304042	Info	VPOOL: Adding VLAN [vid:%d] to hash table		
304043	Info	VPOOL: Free VLAN Pool for VLAN-MAP [addr:%p], refcnt [cnt:%d]		
304057	Info	[msg:%s]	AP Heartbeat Tunnel Timeout indication from Datapath	
304068	Info	[func:%s], [line:%d]: STM restarts and notifies datapath to clean up users	STM restarts and notifies datapath to clean up users.	
304116	Info	[msg:%s]	System related info messages logged in the station manager (stm).	
304117	Info	[msg:%s]		
305003	Info	AP [name:%s] is down	The controller has lost contact with the access point.	
305005	Info	Received message from unknown AP at IP [ip:%P].	A message was received from an AP which was not registered with the controller. The AP will rebootstrap.	
305006	Info	AP [name:%s] rebooted	The AP has registered with the controller after rebooting.	
305007	Info	AP [name:%s] bootstrapped	The AP has (re)registered with the controller without rebooting.	
305008	Info	AP [name:%s] redirected to [lms:%pI4].	The AP attempted to register with this controller but was redirected to a different controller based on the configured lms-ip.	
305009	Info	AP [name:%s] image version mismatch.	The ArubaOS image version on the AP is not the same as that on the controller. The AP will download a new image and reboot.	
305010	Info	AP [name:%s] upgrading flash image.	The AP is downloading a new ArubaOS image to store in flash. When this process completes, the AP will reboot.	
305011	Info	AP [name:%s] rebooting.	The AP is rebooting.	
305031	Info	Creating mesh recovery profile.	Creating the mesh recovery profile for use when no potential parents matching the provisioned clusters can be found.	
305053	Info	AP [name:%s] redirected to [lms:%s].	The v6 AP attempted to register with this controller but was redirected to a different controller based on the configured lms-ipv6.	
306404	Info	IKE Daemon synced with cfgm...	IKE Daemon synced with Configuration manager	
306405	Info	IKE Daemon synced with fpapps...	IKE Daemon synced with L2/L3 module	
306411	Info	IP pool [pool_name:%s] config updated, range unchanged.	IP pool configuration updated	
306601	Info	Changing the trace level to [level:%d]	NA	
306602	Info	Changing the logging level for [level:%d] facilities	NA	
306703	Info	[msg:%s]		
306704	Info	[func:%s], [msg:%s]		
307039	Info	The switch ip changed. rediscovering the switch role	Controller switch IP is changed, most probably a reboot is required to proceed further.	
307040	Info	The new switch role is [mySwitchRole:%s]	Controller got a new role, may be due to VRRP failover or config change by Administrator	
307096	Info	Local Switch ([switchip:%s]) is still using papi for configuration download. It is incompatible with the current conductor controller AirOS version and needs upgrading.	Local Switch is still using old PAPI messaging system for configuration download. It is incompatible with the current conductor controller AirOS version and requires an upgrade.	
307103	Info	[func:%s] [line:%d] Connection to the conductor failed, Will retry socket ID [sock_id:%d] state [sock_state:%s]	Local is unable to connect(TCP) to Conductor, please verify if there is any firewall or network connectivity issue	
307218	Info	CFGM IPSEC src_net:[srcIp:%s]:[srcMask:%s] dst_net:[dstIp:%s]:[dstMask:%s] vlan:[vlan:%d] mac1:[mac1:%s] mac2:[mac2:%s] caCert:[caCert:%s] serverCert:[serverCert:%s] suitBalgo:[suiteBalgo:%d] credType:[credType:%d]	This displays cfgm-ipsec configuration	

307242	Info	Failed to connect to the Conductor ([switchConductorIp:%s]),Configuration socket will try again: [err_str:%s]	Local is unable to establish connection (TCP) with conductor.	
307244	Info	Connection to the conductor is broken, re-initializing the connection: received bytes [ret:%d] : error [err:%s]	Local TCP connection to Conductor is down, Local will retry.	
309000	Info	IF-MAP session to [[svr:%s]] is established, Session_id:[sid:%s]	This indicates a session to an IF-MAP server is established.	
309108	Info	PAN session to [[svr:%s]] is established	This indicates a session to a PAN server is established.	
309124	Info	Renew Session to PAN server [[svr:%s]] failed-[cause:%s] using Conn:[conn:%lu], tries:[tries:%d]/[max:%d], Retry again!	This indicates a time out to renew session to a PAN server.	
309200	Info	No Web-Socket Connection to ClearPass NetWatch: DISABLED	This indicates no need to connect web-socket server in ClearPass NetWatch since it's disabled.	
309803	Info	[func:%s](): [msg:%s]	This shows an informational message in ExtIntfMgr.	
309805	Info	[func:%s](): extifmgr process is initialized	This indicates extifmgr daemon process is initialized.	
309839	Info	Successfully Connected to WebSocket Server '[host:%s]:[port:%d]/[uri:%s]'	This indicates connection to a WebSocket server is established.	
309840	Info	DisConnecting to WebSocket Server '[host:%s]:[port:%d]/[uri:%s]'	This is extifmgr internal debugging message.	
309844	Info	Connection to WebSocket Server '[host:%s]:[port:%d]/[uri:%s] is down'	This indicates the WebSocket connection is closed.	
309845	Info	Connection to WebSocket Server '[host:%s]:[port:%d]/[uri:%s] is destroyed'	This indicates the WebSocket connection is destroyed.	
309846	Info	WebSocket KeepAlive-Configuration: time=[time:%d] probes=[probes:%d] interval=[interval:%d]	This displays Keep-Alive configuration for a WebSocket connection.	
309900	Info	[func:%s](): MAPC-API is intialized	This indicates MAPC-API is intialized.	
309901	Info	[func:%s](): CPPM-IF-MAP is UP	This indicates CPPM IF-MAP is active.	
309902	Info	[func:%s](): CPPM-IF-MAP is DOWN	This indicates CPPM IF-MAP is inactive.	
310201	Info	[msg:%s]	Generic INFO level system log	
310301	Info	[msg:%s]	Generic INFO level system log	
310305	Info	[msg:%s]	Generic INFO level system log for Flow Manager	
310309	Info	[msg:%s]	Generic INFO level system log	
310313	Info	[msg:%s]	Generic INFO level system log	
310317	Info	[msg:%s]	Generic INFO level system log	
310321	Info	[msg:%s]	Generic INFO level system log	
310325	Info	[msg:%s]	Generic INFO level system log	
310329	Info	[msg:%s]	Generic INFO level system log	
311001	Info	LMS changed from [old_ip:%pI4] to [new_ip:%pI4]		
311031	Info	[msg:%s]		
311032	Info	[msg:%s]		
312001	Info	Ready	IP multicast process is ready to accept input	
312003	Info	[str:%s]	DPI config state changes	
312101	Info	ESI is ready	ESI module is ready to interface with external services	
312200	Info	Telemetryd started	This indicated the telemetryd process is started	
312205	Info	[func:%s](): Telemetryd process is initialized.	This indicates telemetryd process is initialized.	
312302	Info	[func:%s], [msg:%s]		
312401	Info	[msg:%s]		
312502	Info	[func:%s], [msg:%s]		
312602	Info	[msg:%s]		
313011	Info	Initializing Dot1q	System is initializing 802.1Q frame handling	
313012	Info	Converting Vlan [vid:%d] from Dynamic to Static	System is converting a dynamically registered VLAN to static	
313014	Info	Request to create Vlan [vlanID:%d]	System is creating a VLAN	
313023	Info	Adding Tunnel [tunnelId:0x%x] to Vlan [vlanId:%d]	System is adding a tunnel to VLAN	
313025	Info	Tunnel [tunnelId:0x%x] already present in the vlan interface [vid:%d]	While attempted to add a tunnel to a VLAN, system detected that tunnel is already present in the VLAN interface	
313027	Info	Interface for vlan [vid:%d] is not created	VLAN interface does not exist	
313029	Info	Removing Tunnel [tunnelId:0x%x] from Vlan [vlanId:%d]	System is removing a tunnel from VLAN	
313030	Info	Cannot find Vlan Interface [vlanId:%d] line [ln:%d]	System did not find VLAN configuration	
313037	Info	Retrieving Tunnel info for Vlan [vlanId:%d]	System is retrieving tunnel information for a VLAN	
313044	Info	Native Vlan Id for Port [prtid:%d] is [vId:%d]	This is a informational message indicating native VLAN id for a port	
313045	Info	Setting the Native Vlan Id [vlanId:%d] for Port [prtid:%d]	System is setting native VLAN ID for a port	

313093	Info	switch mac is [swmac:%m]	This is an information message indicating system MAC address	
313119	Info	[func_name:%s] Added vlan: [vlan_id:%d]	System added a VLAN	
313120	Info	[func_name:%s] Deleted vlan: [vlan_id:%d]	System deleted a VLAN	
313127	Info	Interface Address Cannot be the same as loopback address [if_ip:%s] line [ln:%d]	Interface IP address conflicts with loopback address	
313128	Info	Loopback address cannot be part of management port subnet [ps_ip:%s] line [ln:%d]	Loopback address cannot be part of management port subnet	
313129	Info	Address Conflicts with Loopback Address [ipAddr:%s]	Interface IP address conflicts with Loopback Address	
313132	Info	Address conflicts with management port address [mp_ip:%s]	Interface IP address conflicts with management port address	
313134	Info	Interface address cannot be part of Management Subnet	Interface IP address cannot be part of Management Subnet	
313135	Info	Address [ipAddress:%s] Conflicts with Interface Address of [if_num:%d]	System detected a conflict in interface IP addresses	
313136	Info	Ip Address [ipAddress:%s] matches with Interface Address of [if_num:%d]	System detected a conflict in interface IP addresses	
313140	Info	Modifying the arp entry for [ipAddress:%s]	System updated an ARP entry	
313142	Info	Address Conflicts with Local Route	Local route already exists for a static route	
313143	Info	Route Conflicts with a Tunnel Ip Address	Route conflicts with a tunnel IP address	
313149	Info	Vlan [vlanId:%d] has Tunnels configured	VLAN state cannot be set inactive because VLAN has tunnels configured	
313152	Info	vlan [vlanId:%d] is down for IP forwarding	System has marked an interface as down. For this interface, system will delete all routes, delete all dynamic ARP entries and disable IP forwarding	
313155	Info	IPMAP: RTO_ADD_ROUTE: intIfNum [if_num:%d], prefix [ip_net:%pI4] gateway [gw:%pI4] netmask[msk:%pI4] metric [met:%d]	A new route was added	
313156	Info	IPMAP: RTO_CHANGE_ROUTE: intIfNum [if_num:%d], prefix [ip_net:%pI4] gateway [gw:%pI4] netmask[msk:%pI4] metric [met:%d]	A route was updated	
313157	Info	IPMAP: RTO_DELETE_ROUTE: intIfNum [if_num:%d], prefix [ip_net:%pI4] gateway [gw:%pI4] netmask[msk:%pI4] metric [met:%d]	A route was deleted	
313159	Info	Failed to create DTL intf for router: intIfNum [intIfNum:%d]		
313169	Info	IPMAP: RTO_ADD_ROUTE: intIfNum [if_num:%d], prefix [ip_net:%s] gateway [gw:%s] metric [met:%d]	A new route was added	
313170	Info	IPMAP: RTO_CHANGE_ROUTE: intIfNum [if_num:%d], prefix [ip_net:%s] gateway [gw:%s] metric [met:%d]	A route was updated	
313171	Info	IPMAP: RTO_DELETE_ROUTE: intIfNum [if_num:%d], prefix [ip_net:%s] gateway [gw:%s] metric [met:%d]	A route was deleted	
313173	Info	Setting the proxy arp config to [cmd:%s]	Proxy ARP configuration for an interface has changed	
313174	Info	Enabling PIM for vlan [vlanId:%d]	Enabled PIM protocol for a VLAN	
313175	Info	Disabling PIM for vlan [vlanId:%d]	Disabled PIM protocol for a VLAN	
313176	Info	Enabling IGMP for vlan [vlanId:%d]	Enabled IGMP protocol for a VLAN	
313177	Info	Enabling IGMP Snooping for vlan [vlanId:%d]	Enabled IGMP protocol snooping on a VLAN	
313178	Info	Disabling IGMP for vlan [vlanId:%d]	Disabled IGMP protocol for a VLAN	
313179	Info	Enabling MLD for vlan [vlanId:%d]	Enables IPv6 multicast protocol MLD	
313180	Info	Enabling MLD Snooping for vlan [vlanId:%d]	Enables IPv6 multicast protocol MLD snooping	
313181	Info	Disabling MLD for vlan [vlanId:%d]	Disables IPv6 multicast protocol MLD	
313187	Info	Address Conflicts with Loopback Address [ipv6addr:%s] at line [ln:%d]	Interface IPv6 address conflicts with Loopback Address	
313188	Info	Address Conflicts with Local Route	Local route already exists for a static route	
313189	Info	Interface Address Cannot be the same as loopback address [if_ip:%s] line [ln:%d]	Interface IPv6 address conflicts with loopback address	
313190	Info	Loopback address cannot be part of management port subnet [ps_ip:%s] line [ln:%d]	Loopback address cannot be part of management port subnet	
313191	Info	Address [ipv6addr:%s] Conflicts with Interface Address of [if_num:%d]	System detected a conflict in interface IPv6 addresses	
313192	Info	Interface Address Cannot be the same as loopback address [if_ip:%s] line [ln:%d]	Interface IPv6 address conflicts with loopback address	
313216	Info	PPPoE: pppoed process has terminated. Process ID: [pid:%d]	The PPPoE session has terminated regularly.	None needed
313217	Info	PPPoE: Sending terminate request to pppoed	System is sending terminate request to PPPOE daemon for processing configuration changes	
313220	Info	PPPoE: started pppoed. Child pid: [pppoed_pid:%d]	PPPOE daemon (child) started	

313221	Info	PPPoE username changed to [uname:%s]	PPPoE user name updated	
313222	Info	Removed PPPoE username	PPPoE user name removed	
313223	Info	PPPoE password changed	PPPoE password updated	
313224	Info	Removed PPPoE password	PPPoE password removed	
313225	Info	PPPoE service name changed to [sname:%s]	PPPoE service name updated	
313226	Info	Removed PPPoE service name	PPPoE service name removed	
313228	Info	PPPoE: VLAN [pppoe_client_vlan:%d] is currently down	PPPoE daemon could not be restarted because PPPoE VLAN interface is down	
313229	Info	PPPoE: PPPoE client is enabled on vlan [vlan:%d]	PPPoE client enabled on VLAN	
313238	Info	PPPoE: pppoed is restarted	Dynamic IP: PPPoE restarted	
313239	Info	DHCPC: DHCP is restarted	Dynamic IP: DHCP restarted	
313240	Info	Dynamic IP is not enabled	PPPoE or DHCP process cannot be restared because Dynamic IP is not enabled	
313242	Info	Static ARP: no matching subnet for [ipAddr:%s]	A static entry could not be added to ARP table because there is no routing interface registered for a subnet to which this address belongs	
313246	Info	Sendin RTO_ADD_ROUTE request 0x[network:%x], 0x[netmask:%x], 0x[router:%x], 0x[metric:%x]	System is selecting a new best route	
313249	Info	Route Entry Successfully Inserted in Internal Route Table	Route entry successfully inserted in the route table	
313255	Info	Interface is Down, Not creating the route in kernel 0x[ifNum:%x]	System could not create route in the kernel because interface was down	
313258	Info	Deleting a Route Entry	A route entry was deleted (possibly because IP interface went down)	
313266	Info	Route Add Notification for network [network:%s], gateway [gateway:%s]n	System is adding a route	
313267	Info	Route Delete Notification for network [network:%s], gateway [gateway:%s]n	System is deleting a route	
313268	Info	Route Change Notification for network [network:%s], gateway [gateway:%s]n	System is updating a route	
313269	Info	Router Initialization is not done. n	System cannot process link state change because initialization was not completed	
313270	Info	Cannot create more than [max:%d] router interfaces.n	System cannot process link state change because of resource limitations	
313281	Info	IPv6 Router Initialization is not done. n	System cannot process link state change because initialization was not completed	
313282	Info	Cannot create more than [max:%d] IPv6 router interfaces.n	System cannot process link state change because of resource limitations	
313291	Info	Sending RTO6_ADD_ROUTE request [network:%s], [router:%s], 0x[metric:%x]	System is selecting a new best route	
313294	Info	Ipv6 route entry successfully Inserted in internal route table	Route entry successfully inserted in the route table	
313300	Info	Interface is Down, not creating the Ipv6 route in kernel 0x[ifNum:%x]	System could not create route in the kernel because interface was down	
313303	Info	Deleting a Ipv6 route entry	A route entry was deleted (possibly because IP interface went down)	
313330	Info	Sending Role change event to CFGMn	VRRP is sending role change event to configuration manager	
313341	Info	Initialization of slot [slot:%d] is [state:%s]. number of ports [numports:%d]	This message indicates initialization state of a card along with its port count	
313350	Info	Hardware interface returned success for Command DAPI_CMD_INTF_XSECn	XSEC MAC address for an interface was set successfully	
313360	Info	Received a card create event for slot [slot:%d] numports [numPorts:%d]n	A card has been inserted	
313388	Info	Setting the XSec for Port [intIfNum:%d] xsec is [xsec:%d] flag is [flag:%d]n	This message displays Xsec settings for the port	
313390	Info	xSec vlan active, sending tunnel configuration to Hardware.		
313399	Info	Xsec Port [i:%d] is added to Vlan [vlan:%d]n	A port running Xsec protocol was added to VLAN	
313434	Info	Interface address cannot be the same as management address [ip:%s]	There is an IP address conflict. Check configuration	
313443	Info	Received heartbeat on tunnel [tunId:%d]. Enabling the tunnel.	This message indicates that the tunnel is enabled because of the arrival of a heartbeat message	

313447	Info	Bringing the tunnel [xId:%d] [status:%s] because of vrrp [vid:%d] transition	This message indicates that the tunnel state is changed because of VRRP	
313451	Info	PPPD: pppd child [pid:%d] exited	The PPPD child process for cellular/modem devices have exited. It will be restarted as necessary	
313453	Info	PPPD: pppd is terminated. pid: [pid:%d]	The PPPD child process was successfully terminated by our request	
313454	Info	PPP: Sending terminate request to pppd unit [unit:%d]	The PPP subsystem have requested to stop the pppd process	
313457	Info	PPP: started child pppd: [pppd_pid:%d]	Child PPP Daemon was successfully started for calling the service provider	
313465	Info	User config data had been removed for interface [intIfNum:%d]	Internal user config data had been removed for the interface probably due to a race condition	
313500	Info	Received HAPI USB profile update ([operation:%s]) for [vendor:%x]/[prod:%x] [class:%d]	FPAPPS has received a USB profile update describing how to classify the USB device	
313501	Info	Received HAPI USB modeswitch update ([operation:%s]) for [vendor:%x]/[prod:%x] [method:%d]	FPAPPS has received a modeswitch update describing how to modeswitch the USB device	
313502	Info	Modeswitching USB device [vendor:%x]/[prod:%x], method [_method:%d]	The USB device has been issued a mode switch command to switch into data mode	
313504	Info	USB device [vendor:%x]/[prod:%x]:[type:%d]:[sernum:%s] :: [action:%s]	L2/L3 module detected an USB insert/remove event	
313505	Info	PPP status: [statusStr:%s]	This syslog is used for tracking the progress of PPP dialing session	
313506	Info	USB device status: [statusStr:%s]	This syslog is used for tracking the progress of USB device detection	
313510	Info	WanComp: [statusStr:%s]	This syslog is used for tracking Wan Compression	
313638	Info	[msg:%s]	IPv6 PD client debug information	
313639	Info	[msg:%s]	IPv6 DHCPv6 client debug information	
313640	Info	[msg:%s]	IPv6 PD-based address debug information	
314802	Info	Line card removed from slot [slot:%d]	A line card was removed from the system	
314803	Info	Optical card is [state:%s]	This message indicates presense or absense of optical card on select systems	
314804	Info	Line card ID [id:%ld] not recognized	System detected an unknown line card	
314805	Info	Line card detected in slot [slot:%d]	A line card was detected	
314813	Info	Capping POE in slot [slot:%d] at [cap:%d] Watts	NA	
315007	Info	Illegal Port Number([slot:%d], [port:%d]) in the configurationn	This log indicates that port configuration is not valid for this slot	
315009	Info	Invalid XSec key length [len:%zu], [str:%s]n	The configured XSec key isn't of correct length	
315030	Info	Xsec Point-to-Point is not configured on port ([slot:%d]:[port:%d])	No Xsec PTP information to show since the feature is not enabled on this port.	
315031	Info	Xsec Mac list is emptyn	No Xsec PTP information to show since the Xsec MAC list is empty.	
315051	Info	Route will be added when the Ipsec Map ([name:%s]) is created	The IPSec route has been inserted into the configuration table, but the corresponding IPSec map doesn't yet exist. The route will be added to the hardware routing table when the map has been created	
315157	Info	Unknown SNMP Object Type: [objId:%d]	SNMP Agent received an unknown object ID to process	
316000	Info	Starting WMS Initialization	To be filled out	
316003	Info	Stopping WMS modules	To be filled out	
316024	Info	Set Switch IP to [switch_ip:%s] [switc_ipv6:%s] and Service IP to [svc_ip:%s]	To be filled out	
316025	Info	Sending EXPORT_IMPORT_STATUS to dbsync	To be filled out	
316026	Info	Received mobility-manager update: IP [server_ip:%s] [rtls_port:%d] Optype [optype:%d]	To be filled out	
316043	Info	Marking probe [mac:%s] as wired-mac-dirty	To be filled out	
316046	Info	Received PROBE REGISTER from: IP [ip:%s] Type [type:%d] Device-name [d_name:%s] Status [status:%d]	To be filled out	
316047	Info	Received PROBE UNREGISTER from: [mac:%s]	To be filled out	
316048	Info	Detected mismatch in WMS on master setting. Probe [mac:%s] Switch-value: [switch_value:%d] Probe-value: [probe_value:%d]	To be filled out	

316049	Info	Deleting Probe [mac:%s]	To be filled out	
316050	Info	Deleting Duplicate Probe [mac:%m] IP [ip:%s]	To be filled out	
316061	Info	Destroying AP Tree	To be filled out	
316064	Info	Destroying AP table	To be filled out	
316069	Info	Ageing AP [bssid:%s] SSID:[ssid:%s] phy-type:[phy_type:%d]	To be filled out	
316070	Info	Ageing AP tree node BSSID [bssid:%s] Monitor [monitor_mac:%s]	To be filled out	
316090	Info	Destroying STA tree	To be filled out	
316091	Info	STA Probe: Deleting Table	To be filled out	
316093	Info	Destroying STA table	To be filled out	
316095	Info	Ageing STA [mac:%m]	To be filled out	
316096	Info	Ageing STA tree node MAC [mac:%s] Monitor [monitor_mac:%s]	To be filled out	
316104	Info	Received response from Sysmapper for unknown RAP BSSID [bssid:%s] phy-type:[phy_type:%d] rap-type:[rap_type:%d]	To be filled out	
316105	Info	Received response from SysMapper for unknown STA [mac:%s] phy-type:[phy_type:%d] rsta-type:[rsta_type:%d]	To be filled out	
316106	Info	Received response from SysMapper for AP [mac:%m] phy-type:[phy_type:%d] rap-type:[rsta_type:%d] conf-level:[conf_level:%d]	To be filled out	
316115	Info	Adding wired MAC [wired_mac:%s] from AP: [ap_name:%s]	To be filled out	
316116	Info	Adding wired MAC [wired_mac:%s] for AP: [ap_name:%s]	To be filled out	
316117	Info	Adding router MAC [router_mac:%s] from AP: [ap_name:%s]	To be filled out	
316202	Info	Classification Server IP has been reset	To be filled out	
316220	Info	Classification Server IP set to : [ip:%s]	To be filled out	
316227	Info	Reinitializing Configuration	To be filled out	
316241	Info	Creating AP Classification Rule Name:[name:%s] ID:[id:%d]	An AP Classification Rule has been created	
316242	Info	Enabling AP Classification Rule Name:[name:%s] ID:[id:%d]	To be filled out	
316243	Info	Disabling AP Classification Rule Name:[name:%s] ID:[id:%d]	To be filled out	
316244	Info	Deleting AP Classification Rule [name:%s]	To be filled out	
316245	Info	[fn:%s] AP Rule ID [id:%d] is greater than supported range	To be filled out	
316250	Info	Sending New-AP Message for AP: BSSID=[bssid:%m] Phy-type=[phy_type:%d] Channel=[ch:%d] SSID=[ssid:%s] Rap-type=[rapt:%s]	To be filled out	
316251	Info	Sending New-STA Message for Client: MAC=[mac:%m] BSSID=[bssid:%m] Phy-type=[phy_type:%d] Rsta-type=[rstat:%s]	To be filled out	
316291	Info	WMS Event Table Cleanup: [str: %s]	This log is generated during the periodic cleanup of the WMS Event Table.	
316294	Info	WMS Database Migration: [str: %s].	This log is generated by WMS to specify the processing time to migrate the mysql database to postgres.	
316297	Info	Performing an internal soft-reset of the WMS module	This log is generated when WMS receives a CLI action command to perform an internal soft-reset of the module.	
316310	Info	Process limit [resource:%d] set to [rlim_cur:%s] bytes.	This log is generated when the WMS process rlimit is set.	
317001	Info	restarting ntpd process [pid:%d]	Restarting the NTP daemon as result of command 'process restart ntpd'	
317002	Info	waitpid failed on ntpd child pid [pid:%d], errno [errno:%d]. Respawning ntpd	NTP helper process received an unexpected child exit condition. The NTP daemon will be restarted normally	
317005	Info	[str:%s]	NTP generic informational message	
325000	Info	[name:%s]	Publish object creation/deletion message to another module	
325010	Info	Auth Manager synchronized with '[module:%s]' module	Authentication manager has completed startup synchronization with another module	
325011	Info	Snapshot processing [action:%s]	Authentication manager on the local controller has started or finished processing configuration snapshot	
326000	Info	AM initialized.	Air Monitor is starting	
326075	Info	AM: Dropping PROBE_POLL_REQUEST from Switch IP [wms_ip:%s]	To be filled out	
326088	Info	AM: Marking Switch [ip:%s] as Down	To be filled out	
326097	Info	AM [bssid:%s]: Received a PROBE_POLL_REQUEST from [ip:%s]	To be filled out	
326098	Info	AM: PAPI_Send failed. [msg:%s]	PAPI Send failed	

326129	Info	AM: Setting PPP IP to [ip:%s] for interface [iface:%s]	To be filled out	
326130	Info	AM: Applying [type:%s] profile config	To be filled out	
326140	Info	AM: Max number of Valid OUIs reached.	To be filled out	
326141	Info	AM: Applying IDS Rate Thresholds profile config for frametype: [frametype:%d]	To be filled out	
326145	Info	AM: Applying IDS Signature profile config. Group: [group_num:%d] Number of Instances: [num_sign:%d]	To be filled out	
330004	Info	Connection failure with profile manager, [msg:%s]		
330005	Info	[VLAN:%d] does not exist		
330206	Info	Getting out of recovery mode after [time:%d] minutes to scan.	Exiting recovery mode to try and find potential parents matching provisioned clusters.	
330207	Info	Received association request from an already associated child [mac:%s] - clearing old state.	Received association request from an already associated child. Clearing old state before processing the new association request.	
334002	Info	Reinitializing hardware regulatory domain information	The controller detected an invalid regulatory domain format in the system hardware and has reinitialized the values. This is normal behavior for an old hardware upgrading from an older release. No action needs to be taken.	
334003	Info	Setting restricted country code to [country:%s]	The controller has set the country code to the restricted value stored in the system hardware.	
334004	Info	Setting country code to [country:%s]	The controller has set the country code to the value stored in the configuration file.	
334005	Info	Writing [country:%s] country code to system hardware	The controller has saved country values in the system hardware. This is normal behavior when upgrading from an older release.	
334006	Info	Setting restricted country code to subdomain [country:%s]	The controller has set the country code to a subdomain of the master ` regulatory domain stored in the system hardware.	
334007	Info	Communication failure with client [client:%s], [msg:%s]	Communication Failure with one of profile manager's client	
334013	Info	Profmgr GSM publish object action [act:%d] dev [mac:%s] ret [ret:%d]	Profile Manager publish GSM object update.	
334021	Info	There is no config update for command appid[app:%s] cmdtype [type:%d] optype [op:%d]	Profile Manager non-profile command update not needed.	
334022	Info	Key instance of command matched, update command appid[app:%s] cmdtype [type:%d] optype [op:%d]	Profile Manager non-profile command updated for key instance match.	
334027	Info	Set global config id to [id:%d]	Profile Manager encountered a file operation failure with config file open or update.	
334030	Info	Device add requested for [mac:%s] model [model:%s]	Configuration device add request received with MAC address and device model.	
334201	Info	PhoneHome service is enabled at line [ln:%d]	PhoneHome service is enabled with "router mobile" cli command	
334202	Info	PhoneHome service is disabled at line [ln:%d]	PhoneHome service is enabled with "no router mobile" cli command	
334203	Info	PhoneHome service initialization complete!	PhoneHome service has completed initialization and is ready to handle mobile clients, if enabled. This message is always logged regardless if PhoneHome is enabled or not with "router mobile" cli command	
334207	Info	PhoneHome service is initializing...	PhoneHome service is starting to initialize. This message is always logged regardless if phonehome is enabled or not with "phonehome enable" cli command	
334210	Info	Terminating PhoneHome transaction type [tt:%s] report type [rt:%s], previous state [ps:%s] current state [cs:%s]	PhoneHome is terminating particular transaction; this may happen to create room for new transaction	
334211	Info	Creating PhoneHome transaction type [tt:%s] report type [rt:%s], previous state [ps:%s] current state [cs:%s] after successful post	PhoneHome is creating new transaction	
334212	Info	Deleting PhoneHome transaction type [tt:%s] report type [rt:%s], previous state [ps:%s] current state [cs:%s] after successful post	PhoneHome is deleting successfully uploaded transaction	

334214	Info	PhoneHome failed to transport transaction type [tt:%s] report type [rt:%s] ID [tid:%s]; will re-try	PhoneHome is deleting successfully uploaded transaction	
334215	Info	PhoneHome made multiple unsuccessful attempt to transport transaction type [tt:%s] report type [rt:%s] ID [tid:%s]....terminating the transaction as it hit max retries	PhoneHome is unable to post transaction after multiple attempts. Please check SMTP/HTTPS settings, Network Connectivity and make sure controller can talk to SMTP/HTTPS server	
334230	Info	PhoneHome service initializing completed	PhoneHome process has been successfully setup on the controller	
334303	Info	[msg:%s]		
334304	Info	[func:%s]: [msg:%s]		
334401	Info	Initializing NCFG for UTILITY_PROCESS	Initializing NCFG for UTILITY_PROCESS	
334405	Info	[msg_log:%s]	Received PAPI message	
334407	Info	Received group_change_notify [function:%s] [group:%s] [instance:%s] [id:%d] [changed:%s]	Received group_change_notify message from NCFG	
334408	Info	Failed to retrieve ncfg_group data [function:%s] [group:%s] [instance:%s] [id:%d] [changed:%s]	Failed to retrieve ncfg_group	
334409	Info	Received group_delete_notify [function:%s] [group:%s] [instance:%s]	Received group_delete_notify message from NCFG	
334410	Info	Received profmgr_event_notify [function:%s] [event:%d] [result:%d]	Received profmgr_event_notify message from NCFG	
334556	Info	Socket send failed for intf [intf:%s] with err [err:%d]		
335005	Info	Received a packet on Backplane with action [action:%s] from an M3 in slot [slot:%d]	Received an action request on Back Plane	
335009	Info	Fan [fanid:%d] has returned to normal.	Fan returned to normal.	
335010	Info	Power Supply [PSid:%d] is functional.	Power Supply is back to normal.	
335012	Info	Power Supply [PSid:%d] [Status : %s].	PS failure or missing.	
335016	Info	Fan Tray Inserted.	Fan Tray Inserted.	
335022	Info	Clear Alarm: [Clear: %s]	Clear system alarm log.	
335103	Info	[msg:%s]		
335104	Info	[func:%s], [msg:%s]		
335302	Info	Keepalive Received from IP [addr:%s]. Peer address is [nbraddr:%s]		
336003	Info	[msg:%s]		
336004	Info	[func:%s], [msg:%s]		
337001	Info	[msg:%s]		
339303	Info	[msg:%s]		
339304	Info	[func:%s], [msg:%s]		
341002	Info	[msg:%s]		
341009	Info	AP [name:%s] is down, vc_cur_time [t1:%ld], ap_timestamp [t2:%ld], vc_cur_tick [t3:%d], ap_cur_tick [t4:%ld]	The virtual controller has lost contact with the access point.	
341010	Info	AP [name:%s] is up	The AP has registered with the virtual controller.	
341014	Info	AP rebooting [reason:%s].	The AP is rebooting.	
341016	Info	AP is operating in creating auth server-[name:%s], add-[flag:%d].	The AP is configuring auth server.	
341017	Info	AP is adding auth server-[ipaddr:%s], as_port-[as_port:%d], acctport-[acctport:%d].	The AP is configuring auth server.	
341018	Info	Auth server NAS ip-[ipaddr:%s].	The AP is configuring auth server.	
341019	Info	Auth server source ip-[ipaddr:%s].	The AP is configuring auth server.	
341020	Info	Add termination server-[ipaddr:%s].	The AP is configuring termination server.	
341021	Info	Add LDAP server-[ipaddr:%s], add-[flag:%d].	The AP is configuring LDAP server.	
341035	Info	Set boot partition for AP: convert_ap-[convert_ap:%d], partition id-[part_id:%d].	The AP is setting boot partition id.	
341059	Info	[func:%s]: can't find index for role-[name:%s].	The AP is setting acl.	
341060	Info	[func:%s]: unknown client subnet type-[type:%d] for [ip:%x]/[mask:%x].	The AP is setting acl.	
341061	Info	No SSID for vlan-[vlan:%d] for [ip:%x]/[mask:%x].	The AP is setting acl.	
341062	Info	No space for vlan-[vlan:%d] for [ip:%x]/[mask:%x].	The AP is setting acl.	
341065	Info	Activated tunnel route [desk:%x]/[mask:%x] to [dip:%x]/[ifindex:%x] usecnt-[cnt:%d].	The AP is setting kernal route.	

341066	Info	Activated tunnel route [desk:%x]/[mask:%x] to [dip:%x]/[ifindex:%x] usecnt-[cnt:%d].	The AP is setting kernal route.	
341069	Info	Corp tunnel [sip:%x] to [dip:%x]/[eip:%x]/[ifindex:%d] is up.	The AP is creating tunnel.	
341071	Info	Corp tunnel [sip:%x] to [dip:%x]/[eip:%x]/[ifindex:%d] is down.	The AP is creating tunnel.	
341073	Info	AP derived acl for post auth role-[name:%s], idx-[idx:%u], acl-[acl:%u].	The AP is creating SSID.	
341075	Info	[func:%s] AP can't find default post auth acl for SSID-[name:%s].	The AP is creating SSID.	
341076	Info	Using default acl-[acl:%d] for SSID-[name:%s].	The AP is creating SSID.	
341077	Info	AP add new acl-[name:%s], idx-[id:%d], vlan-[vid:%d], caleaOn-[on:%d].	The AP is configuring ACL.	
341078	Info	AP remove acl-[name:%s].	The AP is configuring ACL.	
341079	Info	AP flush acl-[name:%s].	The AP is configuring ACL.	
341080	Info	[func:%s]: can't find acl-[name:%s].	The AP is configuring ACL.	
341084	Info	Reset index of access rule profile [file:%s] from [old_id:%u] to [id:%u].	The AP is configuring ACL.	
341085	Info	[func:%s]: [line:%d]: payload empty.	The AP is upgrading image.	
341086	Info	[func:%s]: [line:%d]: version=[version:%s], image_url=[image:%s].	The AP is upgrading image.	
341087	Info	[func:%s]: [line:%d]: response payload=[payload:%s].	The AP is upgrading image.	
341088	Info	[func:%s]: [line:%d]: Html message=[msg:%s].	The AP is upgrading image.	
341096	Info	[func:%s]: url is [url:%s]!.	The AP is upgrading image.	
341099	Info	[func:%s]: user-[user:%s] [type:%s] use local DB.	User authenticate.	
341100	Info	[func:%s]: corp subnet [ipaddr:%x]/[mask:%x] updated for vlan-[vid:%d].	Corp configuration.	
341105	Info	[func:%s]: [line:%d] rip-[rip:%s], eip-[eip:%s], backup-[backup:%d],lip-[lip:%s], dev_name-[name:%s].	Handle papi message.	
341106	Info	[func:%s]: [line:%d] rip-[rip:%s], eip-[eip:%s], backup-[backup:%d],lip-[lip:%s], dev_name-[name:%s].	Handle papi message.	
341112	Info	[func:%s]: cert key is [psk:%s].	AP is setting cert.	
341115	Info	[func:%s]: set gre [ipaddr:%s] successfully.	AP is setting gre name.	
341117	Info	[func:%s]: clear gre successfully.	AP is setting gre name.	
341120	Info	SNMP get next mac-[mac:%s], index-[index:%d].	SNMP action.	
341121	Info	SNMP return [mac:%s]:[num:%d].	SNMP action.	
341128	Info	[func:%s], [line:%d]: index-[idx:%d] is [type:%s].	AP is setting SSID.	
341129	Info	[func:%s], [line:%d]: index-[idx:%d] of ssid-[ssid:%s]is set to [new_idx:%d].	AP is setting SSID.	
341134	Info	AP will remove alerts of client-[mac:%s].	AP is removing alerts.	
341136	Info	Perform image checking with conductor [conductor_ip:%s].	Slave check image with master.	
341139	Info	SNMP get mac-[mac:%s], index-[index:%d].	SNMP action.	
341140	Info	[func:%s], [line:%d]: payload is [payload:%s].	Airwave upgrade image.	
341145	Info	Cert type is [type:%s], format is [format:%s].	AP upload certificate for radius server.	
341146	Info	[func:%s]: result for CLI_EXECUTE_CERT_UPLOAD [result:%s].	AP upload certificate for radius server.	
341160	Info	Send reboot cmd to AP [ap:%s], reason [reason:%s].	Send reboot cmd.	
341161	Info	Send reboot ack to AP [ap:%s].	Send reboot ack cmd.	
341162	Info	Receive reboot ack from AP [ap:%s].	Recevice reboot ack.	
341168	Info	[func:%s],[line:%d]: uplink type [type:%s], state [state:%s].	Print the uplink info.	
341178	Info	[func:%s],[line:%d]: send message to awc [type:%d], [username:%s], [password:%s], [device_key:%s], [label:%s].	clid send papi message to awc.	
341179	Info	[func:%s],[line:%d]: receive message from awc [key:%s], [state:%d], [value:%s].	clid receives message from awc.	
341180	Info	[func:%s],[line:%d]: send mesh cfg.	Send mesh cfg.	
341186	Info	Find uplink fail, type [type:%d].	Find uplink fail.	
341187	Info	Add [mac:%m] to ap allowlist.	Add an ap to the whitelist.	
341188	Info	Del [mac:%m] from ap allowlist.	Del an ap from the whitelist.	
341189	Info	[func:%s]: discover client [mac:%s] [fapip:%s] [vlan:%d].	Discover client request.	
341190	Info	[func:%s]: found client [mac:%s] [vlan:%d] [hapip:%s] [oldapip:%s] [vcip:%s].	Found client response.	
341191	Info	[func:%s]: hap req for [mac:%s] [fapip:%s] [vcip:%s] [oldapip:%s] [rtid:%d] [vlan:%d] [vapvlan:%d].	HAP request.	
341192	Info	[func:%s]: hap ack for [mac:%s] [rtid:%d].	HAP Ack.	

341193	Info	[func:%s]: foreign client info [mac:%s] [type:%s] [vapvlan:%d] [vlan:%d] [ssid:%s] [vcip:%s] [hapip:%s].	Foreign client info.	
341195	Info	[func:%s]: clt del req for [mac:%s] [rehome:%d] [fapip:%s].	Client Delete Request.	
341196	Info	[func:%s]: clt del notification for [mac:%s] [hapip:%s].	Client Delete Notification.	
341203	Info	[func:%s]: foreign client rehome [mac:%s].	Foreign Client re-home.	
341204	Info	[func:%s]: client subnet info [mac:%s] [subnet:%s].	Foreign Client re-home.	
341209	Info	[func:%s]: mip tunnel down [tid:%d].	MIP tunnel down.	
341215	Info	[func:%s]: L3 Subnet Update [cmd:%d] [subnet:%s] [mask:%s] [vlan:%d] [vcip:%s] [flag:%x].	L3 Subnet Update.	
341216	Info	[func:%s]: awc logout from [ip:%s].	Awc logout.	
341217	Info	[func:%s]: awc connect to [ip:%s] successfully.	Awc connect successfully.	
341218	Info	[func:%s]: awc login to [ip:%s] successfully.	Awc login successfully.	
341219	Info	[func:%s]: awc identify [ip:%s] successfully.	Awc identify successfully.	
341220	Info	[func:%s]: L2 Roam session requested for client [mac:%s] [ssid:%s].	L2 Roam session requested.	
341221	Info	[func:%s]: Foreign sta info for [mac:%s] from [vcip:%s].	Foreign sta info.	
341222	Info	[func:%s]: Remote sta info for [mac:%s] from [vcip:%s].	Remote sta info.	
341223	Info	[func:%s]: L3 VC Update [cmd:%d] [vcip:%s] [flags:%d].	L3 VC Update.	
341225	Info	[func:%s]: VC Auto Discover.	VC Auto Discover.	
341226	Info	[func:%s]: VC IP changed [oip:%s] [nip:%s].	L3 VC Update.	
341231	Info	[func:%s]: Sta ACL changed for [mac:%s] [ssid:%s] [role:%s].	L3 Sta ACL changed.	
341295	Info	ale: encode [msg_type:%s] message succeed, total msg len [len:%d].	encode message succeed.	
341296	Info	Start key generation. PAN state:[state:%s] PAN ip:[ip:%s] port:[port:%d] user:[user:%s].	Start connect to PAN Firewall to do key generation	
341297	Info	PAN Firewall Integeration state changed from [old_state:%s] to [new_state:%s]. function:[func:%s] line:[line:%d]	PAN Firewall state change	
341298	Info	Send PAN user login or logout. User info : [cmd : %s].	Send user login and logout info to PAN firewall.	
341299	Info	ale: op [op:%s] encode [station:%s] message, total [op_str:%s] station count [count:%d].	encode message station count.	
341301	Info	Calculated csum [csum:%u] at [sec:%s].	AP checksum calculation.	
341302	Info	Add TACACS server-[ipaddr:%s], add-[flag:%d].	The AP is configuring TACACS server.	
341304	Info	ale: receive a reported rssi message from [ip:%s].	access point op.	
341319	Info	autojoin: A potential member comes to conductor, and it's not licensed by cloud, mac [mac:%s], current status [status:%s].	a potential slave comes, and it's not licensed by cloud.	
341321	Info	autojoin: A potential member [sn:%s] from [ap_list:%s] is encoded to cloud.	A potential slave is encoded to cloud.	
341328	Info	[func:%s]: look up mac entry for auth-survivability client-[mac:%m].	look up mac entry.	
341330	Info	[func:%s]:, look up user entry for auth-survivability username-[user:%s].	look up user entry.	
341333	Info	[msg:%s]	netlink info message	
342003	Info	[msg:%s]		
342004	Info	[func:%s], [msg:%s]		
343005	Info	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related info messages logged in the mDNS proxy (mdns)	
343503	Info	[func:%s] [line:%d] [msg:%s]	System related informational messages logged in AirGroup	
344003	Info	([func:%s] [line:%d]) [msg:%s]	System related informative messages logged in DDS	
345303	Info	[msg:%s]		
345304	Info	[func:%s], [msg:%s]		
346005	Info	([func:%s] [line:%d]) [msg:%s]	System related info messages logged in HA_MGR	
348303	Info	[msg:%s]		
348304	Info	[func:%s], [msg:%s]		
350002	Info	Wrapper got signal [sig:%d]	To be filled out	
350003	Info	from pid [pid:%d], status [st:%d], [errno:%d], [errstr:%s]	To be filled out	
350004	Info	httpd exited due to [sig:%d]	To be filled out	
350006	Info	Switch IP not configured	Not configuring the switch ip can result in breaking the certificate configuration	
351001	Info	Ready	LLDPD process is ready to process and transmit LLDP PDUs	
351008	Info	GSM PORT_INFO Lookup failed at Function: [function:%s] for port [port:%d] result [rval:%d]	NA	

351009	Info	GSM LLDP_INFO Lookup failed at Function: [function:%s] for port [port:%d] result [rval:%d]	NA	
351010	Info	GSM Lookup failed for Chassis Info with result [rval:%d]	NA	
351016	Info	Function: [function:%s] Chassis Hostname is either "(none)" or could not be found with return value [ret:%d]	NA	
351022	Info	Function: [function:%s] LLDP Max neighbors reached for port [port:%d]	NA	
355003	Info	[func:%s]: [msg:%s]	System related informative messages logged in Cert Download Mgr	
356004	Info	[msg:%s]	RNG mgr module informations message	
356101	Info	[msg:%s] [func:%s] [line:%d]	NA	
356302	Info	[msg:%s]	Information about condition in Mcell process	
357003	Info	([func:%s] [line:%d]) [msg:%s]	System related informative messages logged in Config Distributor	
358002	Info	[msg:%s]		
358003	Info	[func:%s]: [msg:%s]		
359003	Info	[msg:%s]	System related informative messages logged in HCM	
360003	Info	[msg:%s]		
360004	Info	[func:%s]: [msg:%s]		
381003	Info	[msg:%s]		
381004	Info	[func:%s], [msg:%s]		
386006	Info	[msg:%s]	UDMD system info log	
390003	Info	[msg:%s]		
390004	Info	[func:%s], [msg:%s]		
393004	Info	[func:%s] [line:%d] [msg:%s]	System related info messages logged in by DPI MGR	
394005	Info	[msg:%s]	Generic info level system log	
394102	Info	VRRP PAPI init failed	VRRP PAPI init failed	
397002	Info	[msg:%s]	System related info messages logged by DDNS_CLIENT	
398502	Info	[msg:%s]	System related informative messages logged in Policymgr	
398506	Info	Policy Manager synchronized with '[module:%s]' module	Policy Manager has completed startup synchronization with another module	
398507	Info	Snapshot processing [action:%s]	Policy Manager on the local controller has started or finished processing configuration snapshot	
398526	Info	[msg: %s]	This shows an internal information message.	
398551	Info	[msg: %s]	System related informative messages logged in Policy manager uplink.	Contact tech-support.
399005	Info	Received lacp pdu on interface [intf:%x]		
399502	Info	[module:%s] [msg:%s]	System related info messages logged by LHM	
399601	Info	[msg:%s] [func:%s] [line:%d]	NA	
399808	Info	Configuration error: [msg:%s] [code:%d] in [function:%s], [file:%s]:[line:%d].	This log indicates that a non-critical configuration error has occurred.	
399815	Info	[error:%s]	This is an internal system debugging log.	
399817	Info	Unsupported opcode [opcode:%d] received in [function:%s], [file:%s]:[line:%d].	This log indicates that the system application received an undefined operation code. The operation will be ignored.	
399818	Info	License check failed for the command, when processing the line#[line:%d]::[cmd:%s]	This log indicates that the License check failed when parsing the configuration file.	
399824	Info	[msg:%s]	This is an webserver system info log.	
399829	Info	[msg:%s]	This is an webserver system info log.	
399899	Info	[function:%s], [file:%s]:[line:%d]: [info:%s]	This log indicates that we encountered an internal system error. Technical support should be contacted with this information.	
300106	Notice	The [thing:%s] clock is older than the time at which key '[key:%s]' was installed. The key will be expired.	The system has determined that the clock has been set too far back, and the listed key will be expired. If this is inadvertent, use 'license add' to re-install the key.	

300107	Notice	Licenses will expire in [days:%u] days	Some evaluation licenses will expire in the stated number of days. For feature licenses, this will cause the controller to reload. At this level, fewer than 30 days remain until expiry.	Please make a list of licenses (from the "show license" command output) which are about to expire and contact support
300115	Notice	License manager expiring service limits	Evaluation licenses have expired and the controller is adjusting licensed limits as necessary.	
300132	Notice	Enabled configuration fragment for feature [name:%s] [id:%d] [fragment:%s]	After adding a license that requires a configuration file update, the update failed.	
300305	Notice	FIPS Notice: [msg:%s]	This is a FIPS notice log in system module.	
300803	Notice	[msg:%s]		
301246	Notice	[line:%d] SNMP Authentication Failed for Management station [t_ipAddr:%s] [reason:%s]	To_be_filled_out	
301262	Notice	Inform Response, did not find Source Request	To_be_filled_out	
301406	Notice	SNMP agent timed out when sending a request to application [app:%s] for object [obj:%d]. SNMP request from [src: %s].	Request from SNMP server to application timed out.	
304006	Notice	IGMP Drop Tx - [s_addr:%P]		
304007	Notice	IGMP Join Tx - [s_addr:%P]		
304031	Notice	PAPI message to [ip:%P] port [port:%d] timed out		
304032	Notice	902il Compatibility mode [enadis:%s]	NEC 902il compatibility mode was enabled or disabled	
304056	Notice	Stm (Station management) notice at [func:%s], [line:%d], [data:%s]	This log indicates the route point is an IP tunnel	
304119	Notice	IGMP Drop Tx - No IPv4 address for VLAN [igmp_vlan:%d]		
306401	Notice	VPN license [vpn:%s] VIA license [via:%s] IPSEC AP license [strap:%s]	Notification of installed VPN, VIA and IPSec AP licenses	
307028	Notice	Ageing out the local switch [switchip:%s] from the conductor list	Conductor waited long enough to hear again from local controller, conductor is purging this local from its database	
307310	Notice	dbsync: Completed manual Database synchronization on the active Conductor Switch		
311015	Notice	Wipe out AP flash.		
311024	Notice	Attempting to transfer panic dump to server [server:%s]	Transferring panic information file to server	Contact Technical Support
311029	Notice	[msg:%s]		
311030	Notice	[msg:%s]		
312104	Notice	ESI license is [state:%s]	This message indicates the state of ESI license. The state is either enabled or disabled	
312105	Notice	ESI [capacity:%s] limit reached [limit:%d]	Number of configured external servers has exceeded capacity. Review your licensing requirements	
312603	Notice	[msg:%s]		
314801	Notice	Configuration download is complete	NA	
316018	Notice	Handle Config Message: is_master [is_master:%d]	To be filled out	
316020	Notice	License Key - [name:%s]=[val:%d]	To be filled out	
316021	Notice	License Key - [name:%s] - [mode:%s]	To be filled out	
316044	Notice	Length mismatch in message. At [function:%s] line [line:%d] Expected [msg_len:%zu] Got [len:%zu]	To be filled out	
316045	Notice	Length mismatch in message. At [function:%s] line [line:%d] From Probe [probe:%s] Expected [msg_len:%zu] Got [len:%zu]	To be filled out	
316103	Notice	Database operation complete: Operation [type:%s] IP [ip:%s], User:[user:%s] Password:[password:%s] DB:[db:%s]	To be filled out	
316296	Notice	Invalid message contents. Msg type: [msg_type:%d] [event_type:%d]	This log is generated when invalid contents are detected during the parsing of a message received by WMS. This can indicate a corruption in the message.	
316301	Notice	In [function:%s], invalid radio number [phy_num:%d] found for probe [bssid:%m].	This log is generated when a probe is found to have an invalid radio number.	
325001	Notice	Network destination [action:%s] name='[name:%s]'	A network destination was created/modified/deleted	
325002	Notice	Network service [action:%s] name='[name:%s]'	A network service was created/modified/deleted	
325003	Notice	Access-list [action:%s] name='[name:%s]', type='[type:%s]'	An access-list was created/modified/deleted	
325004	Notice	User Role [action:%s] name='[name:%s]'	A User Role was created/modified/deleted	
325005	Notice	Add ACL to role; acl='[acl:%s]', type='[type:%s]', loc='[loc:%s]', role='[role:%s]'	An access-list was configured in a role	

325006	Notice	Remove access-list '[name:%s]' from role '[role:%s]'	An access-list was removed from role	
325007	Notice	Add VLAN [vlan:%d] IP='[ipaddr:%s]' mask='[mask:%s]'	Added VLAN	
325008	Notice	License key '[name:%s]' [mode:%s]	A feature is enabled or disabled based on license key	
325009	Notice	License key '[name:%s]' limit=[limit:%d]	This shows the limit enforced by the licensed feature	
325013	Notice	Set admin authentication mode to [mode:%s]	Admin authentication was enabled or disabled	
325014	Notice	Set admin authentication server-group to '[sg:%s]'	New server group was assigned for admin authentication	
325015	Notice	Set admin authentication default-role to '[role:%s]'	New default role was assigned for admin authentication	
325018	Notice	Set user idle timeout to [time:%d] minutes	User idle timeout is set. If a user remains inactive for this duration it is removed and must perform L3 authentication again	
325019	Notice	Disable user idle timeout	User idle timeout is disabled. L3 state will be maintained in spite of inactivity.	
325021	Notice	User fast aging [action:%s]	User fast aging was enabled or disabled. If enabled, multiple IP addresses for a MAC will trigger immediate PING test to detect inactivity. L3 state will cleared for IP address that fails to respond	
325027	Notice	IPv6 Extended Header alias [action:%s] name='[name:%s]'	An IPv6 Extender Header Alias was created/modified/deleted	
326009	Notice	AM: Wi-Fi Interface Reinit called for [bssid:%s]	To be filled out	
326010	Notice	AM: calling remove_ap [bssid:%s]	To be filled out	
326011	Notice	AM: calling remove_pot_sta [mac_addr:%s]	To be filled out	
326012	Notice	AM: calling remove_pot_ap [bssid:%s]	To be filled out	
326013	Notice	AM: SAPCP-Parse called	To be filled out	
326014	Notice	AM: SAPCP-Parse dropped	To be filled out	
326067	Notice	AM: IP [newbury_ip:%s] Port [newbury_port:%d] Socket [newbury_sock:%d]	To be filled out	
326091	Notice	AM: Radio Stats: APs=[num_ap:%d] STAs=[num_assoc_sta:%d] Mon-APs=[num_mon_ap:%d] Mon-STAs=[num_mon_sta:%d]	To be filled out	
326102	Notice	AM: unable to find AP [bssid:%s]	To be filled out	
326106	Notice	AM: unable to find STA [bssid:%s] PHY [phy_type:%d]	To be filled out	
326107	Notice	AM: RSTA Type: [rap_type:%d] Valid-exempt:[ve:%s] for STA [bssid:%s]	To be filled out	
326148	Notice	AM: set_mode called for [bssid:%s] type [probe_type:%d] active [active:%d]	To be filled out	
326205	Notice	AM: Adding new Gateway MAC: [mac:%s]	To be filled out	
326206	Notice	AM: Adding new Router MAC: [mac:%s]	To be filled out	
326215	Notice	AM: Adding new tagged Gateway MAC: VLAN:[vlanid:%d] MAC:[mac:%s] IP: [ip:%s]	To be filled out	
326218	Notice	AM: [mac:%s]	To be filled out	
326219	Notice	AM: Setting Gateway MAC to: [mac:%s]	To be filled out	
326220	Notice	AM: Sending ARP Request for Gateway IP: [ip:%s]	To be filled out	
326266	Notice	AM: MAC OUI: Range Entries = [ids_mac_oui_range_size:%d] Hash Entries = [IdsMacOuiHash:%d]	To be filled out	
326271	Notice	AM: New Node Detected Node = [addr:%s] SSID = [ssid:%s] BSSID [bssid_str:%s]	To be filled out	
326272	Notice	AM: New AP Detected Channel = [channel:%d] SSID = [ssid:%s] BSSID = [bssid:%s]	To be filled out	
326273	Notice	AM: SSID Change #2: BSS [bssid:%s] Old SSID [from_ssid:%s] New SSID [ssid:%s] Channel [channel:%d]	To be filled out	
326274	Notice	AM: Inactive Node Detected = [mac_addr:%s] SSID = [ssid:%s] BSSID [bssid_str:%s]	To be filled out	
326275	Notice	AM: Inactive IBSS Detected SSID = [ssid:%s] BSSID = [bssid_str:%s]	To be filled out	
326276	Notice	AM: Inactive AP Detected SSID = [ssid:%s] BSSID = [bssid_str:%s]	To be filled out	
326277	Notice	AM: Setting RAP Type for AP [bssid_str:%s] to: [rap_str:%s]	To be filled out	
326278	Notice	AM: STA [mac_addr:%s] Authenticated with AP [bssid_str:%s]	To be filled out	
326284	Notice	AM: Sending Router Solicitation message to Gateway6 IP=[ipv6:%s]	This log indicates that AM is sending Router Solicitation message to the Gateway6 IP to get the MAC address	
330002	Notice	[ptype:%s] "[pinst:%s]": Not using invalid channel [chan:%s]		

330003	Notice	Conversion failed at file [file:%s] function [function:%s] line [line:%d] error [error:%s].		
330100	Notice	SAPI initialization done	A module has completed synchronization initialization	
330101	Notice	set SAPI state for level [level:%d] to [state:%s]	A module has set internal synchronization state	
330102	Notice	SAPI sync with service [svc:%d] at level [level:%d]	An internal module will synchronization with another	
330103	Notice	SAPI sync (blocking) with service [svc:%d] at level [level:%d]	An internal module will synchronization with another	
330104	Notice	SAPI sync done with service [svc:%d] at level [level:%d]	An internal module has completed synchronization with another module	
334031	Notice	Command parsing failure for [cmd:%s] [error:%s]	Parser failed to parse command	
335018	Notice	Minor Alarm: [Minor: %s]	Minor system alarm log.	
341003	Notice	[msg:%s]		
341043	Notice	AP check image-[image:%s] successfully.	The AP is upgrading image.	
341045	Notice	Receive image upgrade successful for [ipaddr:%s].	The AP is upgrading image.	
341046	Notice	Receive download image successful for [ipaddr:%s].	The AP is upgrading image.	
341053	Notice	AP try version [version:%s] [number:%d] times.	The AP is setuping image.	
341057	Notice	[func:%s]: upgrade image file [file:%s], url [url:%s].	The AP is upgrading image.	
341147	Notice	Upimage: [msg:%s]	Upimage related messages.	
341148	Notice	Checking member [ap_ip:%s] [state:%s]	Master check image upgrade for a slave.	
341150	Notice	Local AP-[ipaddr:%s] start upgrade image.	The AP starts to upgrade image.	
341151	Notice	Local AP-[ipaddr:%s] start download image.	The AP starts to download image.	
341152	Notice	Receive image err [state:%s] for [ap_ip:%s].	Set AP image err state.	
341153	Notice	Sending upgrade write flash to [ap_ip:%s].	Master send upgrade write flash to slave.	
341154	Notice	Sending upgrade success to [ap_ip:%s].	Send upgrade success to Master.	
341155	Notice	Sending download success to [ap_ip:%s].	Send download success to Master.	
341156	Notice	Sending image err [state:%s] to [ap_ip:%s].	Send image err state to Master.	
341157	Notice	AP reaches count [count:%d]-[msg:%s].	AP image upgrade timeout.	
341158	Notice	[func:%s],[line:%d]: Setup image with code [ret:%d].	AP image upgrade timeout.	
341201	Notice	AP [name:%s] reports a spectrum alert: non-wifi device(ID: [id:%d],type: [type:%s]).	Non-wifi device is detected.	
341202	Notice	AP [name:%s] removes a spectrum alert: non-wifi device(ID: [id:%d],type: [type:%s]).	Non-wifi device is removed.	
341233	Notice	Saving AP config, reason [str:%s].	Save ap config	
341273	Notice	Config file length is [len:%d], allowed length is [len2:%d].	Check configuration file before saving it	
341282	Notice	managed mode: Applied the latest configuration from the server.	AP applied the latest configuration from the server.	
341283	Notice	managed mode: Could not download the configuration from the server, retrying - [num:%d].	Could not download the configuration from the server, retry in progress.	
341284	Notice	managed mode: Configuration download from server timed out.	Configuration download from server timed out.	
341285	Notice	managed mode: Configuration file download retry count over.	Configuration file download retry count over.	
341288	Notice	managed mode: Insufficient configuration to start this mode.	Because of insufficient configuration managed mode did not start.	
341290	Notice	[msg:%s]	Per ap settings are applied.	
341323	Notice	autojoin: age out a inactive potential APs [mac:%s] [sn:%s].	age out a inactive potential APs.	
341334	Notice	[msg:%s]	netlink notice message	
343006	Notice	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related notice messages logged in the mDNS proxy (mdns)	
343504	Notice	[func:%s] [line:%d] [msg:%s]	System related notice messages logged in the AirGroup	
346006	Notice	([func:%s] [line:%d]) [msg:%s]	System related notice messages logged in HA_MGR	
356003	Notice	[msg:%s]	RNG mgr module notice message	
386005	Notice	[msg:%s]	UDMD system notice log	
394004	Notice	[msg:%s]	Generic notice level system log	
398504	Notice	Network destination [action:%s] name='[name:%s]'	A network destination was created/modified/deleted	
398505	Notice	Network service [action:%s] name='[name:%s]'	A network service was created/modified/deleted	
398520	Notice	Policy [action:%s] name='[name:%s]'	A Policy table was created/modified/deleted	
398521	Notice	User Role [action:%s] name='[name:%s]'	A User Role was created/modified/deleted	

398522	Notice	Add Policy to role; pcl='[pcl:%s]', type='[type:%s]', loc='[loc:%s]', role='[role:%s]'	An access-list was configured in a role	
398523	Notice	Remove access-list '[name:%s]' from role '[role:%s]'	An access-list was removed from role	
398537	Notice	Threshold profile name='[name:%s]' [action:%s] for policy [policy:%s]	A Theshold profile was added/deleted to Policy table	
398538	Notice	Probe profile name='[name:%s]' [action:%s] for policy [policy:%s]	A Probe profile was added/deleted to Policy table	
398539	Notice	Position '[number:%d]' [action:%s] for policy [policy:%s]	Position was added/deleted to Policy table	
398540	Notice	Pathsteer prigrp='[prigrp:%s]' bkpgrp1='[bkpgrp1:%s]' bkpgrp2='[bkpgrp2:%s]' bkpgrp3='[bkpgrp3:%s]' fbgrp='[fbgrp:%s]' [action:%s] for policy [policy:%s]	A Theshold profile was added/deleted to Policy table	
399825	Notice	[msg:%s]	This is an webserver system notice log.	
399830	Notice	[msg:%s]	This is an webserver system notice log.	
300104	Warning	[function:%s]: failed to decrypt key [key:%s]	An existing key could not be decrypted.	
300128	Warning	License limit constrained to maximum ([max:%u]) for [limit:%s]	The indicated feature limit was capped at the maximum allowable value even though more licensed capacity is available.	
300145	Warning	Licenses sent by the server will expire in [days:%u] days	Licenses sent by the server will expire in the stated number of days. At this level, fewer than 30 days remain until expiry.	Please resolve connectivity issues with the license server.
300158	Warning	Licenses contributed by the client with mac address [mac:%m] will expire in [days:%u] days	Licenses contributed by the client will expire in the stated number of days. At this level, fewer than 30 days remain until expiry.	Please resolve connectivity issues with the license client.
300196	Warning	[function:%s]: PAPI_Alloc: Failed	PAPI_Alloc failed when trying to send the feature table to the processes.	
300198	Warning	[string:%s]	This shows an internal error message.	
300304	Warning	FIPS Warning: [msg:%s]	This is a FIPS warning log in system module.	
300503	Warning	[func:%s], [line:%d], [msg:%s]	System related warning messages logged in the user visibility process	
300804	Warning	[msg:%s]		
300902	Warning	[name:%s]	This is an internal warning message	
301010	Warning	Cannot bind to socket: [errno:%d]n	The system reported an error while initializing the SNMP process and it's unable to bind to the SNMP port. As a result, the SNMP process will be restarted.	
301030	Warning	Illegal value for first two subids	To_be_filled_out	
301033	Warning	Length Mismatch in OctetString. Should be [size:%d] and is [length:%d]	A warning message indicating comparison failed for an octet string type object.	
301034	Warning	[line:%d] Bad Octet String Length [length:%d]	A warning message indicating that string data length exceeds a supported range typically the maximum characters supported by an SNMP OctetString type object.	
301039	Warning	[line:%d] Unable to Make PDU: [reason:%s]	To_be_filled_out	
301042	Warning	Make OID Failed, Length is too big [length:%d]	An OID string exceeds the maximum supported length for an OID.	
301043	Warning	[line:%d] Unable to Clone Variable Binding: [VarbindName:%s]	To_be_filled_out	
301134	Warning	SNMP V3 Message parse error: [reason:%s]: Possible Privacy password mismatch. [line:%d]	To_be_filled_out	
301135	Warning	SNMP V3 Message parse error: [reason:%s].	To_be_filled_out	
301247	Warning	Processing of GET(next) request failed	The SNMP process was unable to create a SNMP response	If the error persists, please contact technical support
301249	Warning	Cannot bind SNMP Trap transport	The TRAPD process is unable to bind to the SNMP trap port	If the error persists, please contact technical support
301268	Warning	Reached the limit on Inform Notification queue for [addr:%s]:[port:%d]	To_be_filled_out	
303022	Warning	Reboot Reason: [reason:%s]	N/A	
303040	Warning	There is only [left:%d] MB left on the flash. At least [safe:%d] MB of free flash space is recommended to keep the system stable.	We are running low on memory. Please clean-up your flash filesystem. If this problem persists please report to technical support.	Clean-up flash filesystem.If this problem persists Contact Technical Support
303062	Warning	Free memory [free:%d] ([freed:%d] KB), Free memory (Cached) [cached:%d] ([cachedk:%d] KB), Total free memory [total:%d] ([totalk:%d])	This message indicates AP is running out of memory. AP will reboot if the condition persists	Contact Support
303095	Warning	Free memory [free:%d] KB, Num clients [clients:%d], Num leaked [leaked:%d]	This message indicates AP is hung due to node leak. AP will reboot if the condition persists	Contact Support

303097	Warning	There is only [left:%d] MB left on the flash1. At least [safe:%d] MB of free flash1 space is recommended to keep the system stable.	We are running low on memory. Please clean-up your flash1 filesystem. If this problem persists please report to technical support.	Clean-up flash1 filesystem.If this problem persists Contact Technical Support
304002	Warning	AP [name:%s]: No response from authmgr for BSSID [bssid:%m]	Unexpected condition occurred in the station manager (stm). Report to technical support.	
304004	Warning	License Check failed, dropping request		
304005	Warning	Ortronics AP support not licensed; dropping request		
304009	Warning	enet_move_tunnel: Tunnel [id:%d] not found		
304011	Warning	stop_signal: timestamp [ts:%ld] - Why was I called ... exiting		
304013	Warning	tunnel_timeout: Tunnel 0x[tunnel_id:%x] not found		
304014	Warning	received frame of unknown type [type:%x] (subtype [stype:%x])		
304015	Warning	handle_tunnel_info_request: Tunnel [tunnel_id:%d] not found		
304016	Warning	IP [tunnel_ip:%P] MAC [mac:%m] ARP Query failed		
304017	Warning	[func:%s]:[line:%d] Too many TCLAS. dropping...		
304018	Warning	[func:%s]:[line:%d] Unknown EID - [eid:%d]		
304019	Warning	Unknown Category in Action Frames: [category:%d]-[action:%d]... dropping		
304020	Warning	Unknown WMM Action [action:%d] in [__func__:%s] dropping		
304022	Warning	[func:%s]: dropped for license key enforcement		
304023	Warning	[func:%s]: Response from Server for [mux_client_mac:%s]: Client has no state		
304024	Warning	[func:%s]: Dropping Heartbeat from unknown mux [mac:%m]-[dest:%d]		
304025	Warning	[func:%s]: Invalid S-[slot:%d] P-[port:%d]		
304026	Warning	[func:%s]: New Id [new_id:%d] different than old [id:%d]		
304027	Warning	VoIP Start/Stop received ... VoIP hash table not created yet		
304028	Warning	[func:%s]: [ip:%P] message out of order		
304029	Warning	[func:%s]: too many voip clients		
304033	Warning	Mesh AP support not licensed; dropping request		
304044	Warning	Waiting for dbstart...	The application is waiting for the database to be ready for access.	
304048	Warning	User DB query issue in: [call: %s]. SQL command: [cmd: %s].	This log indicates that there was an issue when a command was executed on the user database.	
304050	Warning	Client denylist purged by Administrator.	This log indicates that the client denylist was purged by the administrator.	
304091	Warning	Station Up message parse error for AP [ip:%P]		
304096	Warning	stm mon update queue size reaches the threshold [threshold:%u], current [current:%llu]	This log indicates stm mon update queue size reaches the threshold. stm will start dropping sta and user mon update	
304104	Warning	[msg:%s]	System related warning messages logged in the station manager (stm).	
304109	Warning	No available license type [lic:%s] for Tunneled Node [name:%s]		
305012	Warning	AP [name:%s] wired MAC [mac:%m]: duplicate name.		
305013	Warning	No license for AP type [type_name:%s]		
305014	Warning	No available license type [lic:%s] for remote AP [name:%s]		
305015	Warning	Switch license not present; ignoring AP request		
305017	Warning	AP [name:%s]: Unable to assign bridge or split-tunnel mode virtual APs: Not remote AP.		
305018	Warning	Switch is backup master; ignoring AP request		
305019	Warning	Waiting for dbstart...		
305020	Warning	Unexpected message received from [ip:%P] port [port:%d]		
305021	Warning	Unexpected message received from controller at [ip:%P]; OS version may be incompatible.		
305022	Warning	AP [name:%s] radio [radio:%d]: Unable to assign virtual AP "[vap:%s]": Duplicate ESSID "[essid:%s]"		
305023	Warning	Switch role changed; reload required (ignoring received message)		
305024	Warning	AP [name:%s]: Group "[group:%s]" does not exist.		
305028	Warning	AP type [type:%s] serial [serial:%s] IP [ip:%P]: [msg:%s]		

305029	Warning	Adding AP [name:%s] will push the indoor mesh AP limits over the platform limit.	A request to provision an indoor mesh AP failed as the platform limit has been reached.	
305030	Warning	Creation of mesh recovery profile failed: [reason:%s]	Failed to create the mesh recovery profile. No recovery-cluster is available in the event that no potential parents matching the provisioned clusters can be found.	
305032	Warning	AP [name:%s]: Unable to assign split-tunnel enet mode: Not remote AP.		
305033	Warning	No available license for Ortronics AP [name:%s]		
305034	Warning	Over-temperature condition on AP [name:%s] (temp [temp:%d]); tx-power restricted to [pwr:%s]		
305035	Warning	No available license for mesh.	No mesh licenses are available - ignoring mesh provisioning request.	
305036	Warning	Adding the remote AP [name:%s] will push the AP limits over the platform limit.		
305038	Warning	No available license type [lic:%s] for AP [name:%s]		
305039	Warning	Adding the Outdoor Mesh AP [name:%s] will push the AP limits over the platform limit.	A request to provision an outdoor mesh AP failed as the platform limit has been reached.	
305040	Warning	No available 802.11n license for AP [name:%s]		
305041	Warning	Converting both radios to sensor mode for AP [name:%s] even though only one is in sensor mode.		
305042	Warning	RFprotect Server IP is not configured for AP [name:%s].		
305043	Warning	AP [name:%s] (type [type:%s]) can only be used as a remote AP.		
305046	Warning	Unsecure AP at [ip:%s]: address not allowed	An unsecure AP is trying to access the controller from an IP address that is not allowed for automatic certificate provisioning.	
305047	Warning	Dropping unsecure SAP message type [msgname:%s] from AP at [ip:%P] (MAC address [mac:%m])	An unsecure SAP message was received from a secure AP, or an unsecure non-HELLO SAP message was received from an unknown AP. The message will be dropped.	
305048	Warning	Dropping unsecure AP message code [code:%d] from AP at [ip:%P] (MAC address [mac:%m])	An unsecure AP message was received. The message will be dropped.	
305049	Warning	Unsecure AP "[name:%s]" (MAC [mac:%m], IP [ip:%s]) has been denied access because Control Plane Security is enabled and the AP is not approved.	An unsecure AP has been denied access to the controller by the the Control Plane Security mechanism.	
305050	Warning	AP [name:%s] radio [rnum:%d]: Not spectrum capable; entering air monitor mode.		
305051	Warning	Virtual AP "[vap:%s]" rejected for AP "[ap:%s]"; reason: [reason:%s]	The given virtual AP was configured for the given AP but could not be created for the given reason.	
305054	Warning	AP [name:%s] image preload failed: [msg:%s]; will retry	The AP was unable to preload the new image to flash. The preload will be retried after a delay.	
305056	Warning	AP [name:%s] No response from AP for [msg:%s] request for [t:%u] sec; deleting AP.		
305057	Warning	Unsecure AP "[name:%s]" (MAC [mac:%m], IP [ip:%s]) has been denied access because Control Plane Security is enabled and it does not support IPV6 AP.	An unsecure AP has been denied access to the controller by the the Control Plane Security mechanism which does not support IPV6.	
305058	Warning	AP [name:%s]: Drop hello message from [ip:%s] with different MAC, old MAC [mac1:%s], new MAC [mac2:%s].	The controller receive hello message, find AP entry by IP, but its MAC has changed, drop hello message.	
305059	Warning	Version [version:%s] is not compatible with AP [name:%s] with type [type_name:%s], mac [mac:%s]		
305061	Warning	[msg:%s]		
305101	Warning	[msg:%s]		
305104	Warning	Performing [operation:%s]: STM module will exit in 1 second	Log indicates that the process will be restarted intentionally due a previous action taken by an administrator.	
306510	Warning	Dropping message from [sender:%d] for service '[service:%s] (service not found)'	Warning message from Pub/Sub server that a message for non-existent service was received and will be dropped	
306707	Warning	[msg:%s]		

306708	Warning	[func:%s], [msg:%s]		
306709	Warning	stop_signal - Why was I called ... exiting		
307016	Warning	Cannot heartbeat with the conductor.	Conductor-local cannot exchange heartbeat, possible reasons (network connectivity issues, ipsec keys mismatch etc.)	
307019	Warning	Initializing the applications with the last snapshot configuration.	Local is unable to contact/download config from Conductor, local has loaded last received config from conductor	
307385	Warning	Initializing the applications with the last snapshot configuration, enforced by administrator	Local is unable to download latest instance of config from conductor. Local after waiting for configrable time(5 min) will push last learnt config it got from Conductor	
309001	Warning	Session to IF-MAP server [[svr:%s]] Failed - [err:%s]:[msg:%s]	This indicates a failure to esatblish session to an IF-MAP server.	
309002	Warning	Session to IF-MAP server [[svr:%s]] Failed - [err:%s]:[errstr:%s]	This indicates a failure to esatblish session to an IF-MAP server.	
309004	Warning	EndSession to IF-MAP server [[svr:%s]] Failed - [err:%s]:[msg:%s]	This indicates a failure to disconnect to an IF-MAP server.	
309005	Warning	EndSession to IF-MAP server [[svr:%s]] Failed - [err:%s]:[errstr:%s]	This indicates a failure to disconnect to an IF-MAP server.	
309007	Warning	Failed to Publish Request(req[id:%lu]) to IF-MAP server [[svr:%s]] using Conn:[conn:%lu] [sid:%s], [err:%s]:[msg:%s]	This indicates a failure to publish to an IF-MAP server.	
309008	Warning	Failed to Publish Request(req[id:%lu]) to IF-MAP server [[svr:%s]] using Conn:[conn:%lu] [sid:%s], [err:%s]:[errstr:%s]	This indicates a failure to publish to an IF-MAP server.	
309018	Warning	Renew Session to IF-MAP server [[svr:%s]] with SessionId:[sid:%s] Failed - [err:%s]:[msg:%s]	This indicates a failure to renew session to an IF-MAP server.	
309019	Warning	Renew Session to IF-MAP server [[svr:%s]] with SessionId:[sid:%s] Failed - [err:%s]:[errstr:%s]	This indicates a failure to renew session to an IF-MAP server.	
309103	Warning	Active PAN Profile [n:%s] NOT found.	This indicates PAN Active Profile not found in the system.	
309109	Warning	Session to PAN server [[svr:%s]] Failed - code:[err:%d][[msg:%s]]	This indicates a failure to esatblish session to a PAN server.	
309113	Warning	Failed to Post User-ID Request(req[req:%s]) to PAN server [[svr:%s]] using Conn:[conn:%lu], code:[err:%d]:[msg:%s]	This indicates a failure to post to a PAN server.	
309116	Warning	Renew Session to PAN server [[svr:%s]] Failed - code:[err:%d]:[msg:%s]	This indicates a failure to renew session to a PAN server.	
309120	Warning	authmgr is restarted. Clear User-ID Table with [num:%d] entries	This indicates authmgr is restarted and User-ID table needs be cleared.	
309123	Warning	Max Retried with Error([cause:%s]) on Posting User-ID Request(req[req:%s]) to PAN server [[svr:%s]] using Conn:[conn:%lu], tries:[tries:%d]/[max:%d], DisConnect It!	This indicates a failure to post UID to a PAN server.	
309125	Warning	Max retried on Renewing Session to PAN server [[svr:%s]] failed([cause:%s]) using Conn:[conn:%lu], tries:[tries:%d]/[max:%d], DisConnect It!	This indicates max retries reached with failure to renew session to a PAN server.	
309126	Warning	Renew Session to PAN server [[svr:%s]] failed using Conn:[conn:%lu], tries:[tries:%d]/[max:%d], DisConnect It!	This indicates a failure to renew session to a PAN server.	
309802	Warning	[func:%s](): [msg:%s]	This shows a warning message in ExtIntfMgr.	
309806	Warning	[func:%s](): Unable to create Dispatcher	This indicates extifmgr daemon process is not able to create dispatcher.	
309807	Warning	[func:%s](): Unable to initialize PAPI	This indicates extifmgr daemon process is not able to initialize PAPI.	
309808	Warning	[func:%s](): Unable to initialize SAPI	This indicates extifmgr daemon process is not able to initialize SAPI.	
309809	Warning	[func:%s](): Failed in PAPI_Send() - err:[err:%d] arg:[arg:%u]	This indicates error in sending PAPI messsage.	
309810	Warning	[func:%s](): Received message with wrong length([len:%d]), Ignore it.	This indicates a malformed message is received.	
309811	Warning	[func:%s](): Broadcast IF-MAP Status: CPPM:[st:%s].	This indicates current IF-MAP state is changed and is broadcasted .	
309818	Warning	[func:%s](): Error getting the CPPM IF-MAP profile data.	This indicates failure in getting CPPM Profile data.	
309822	Warning	[func:%s](): failed in sapi_sync() on [lvl:%s].	This indicates failure in calling ncfg_sync.	
309823	Warning	[func:%s](): Request Queue (size:[size:%lu]) is Full, Drop the request.	This indicates Request Queue is Full and the request can not be processed.	
309824	Warning	[func:%s](): failed in gsm_initialize() error:[err:%s].	This indicates failure in calling gsm_initialize().	
309838	Warning	Failed Connect to WebSocket Server '[host:%s]:[port:%d]/[uri:%s]'	This indicates failure to connect to a WebSocket server.	
309842	Warning	[func:%s](): Failed to Send [len:%lu] bytes to WebSocket Server '[host:%s]:[port:%d]/[uri:%s]', result:[res:%d]	This indicated failure in sending data to WebSocket server.	

309848	Warning	Failed in Setting Certificate CA-PATH '[capth:%s]' for WebSocket connection"	This indicates failure in setting up CA-PATH for a SecuredWebSocket Connection.	
309850	Warning	[func:%s](): FIPS mode in openSSL is enabled.	This indicates openSSL is set to FIPS mode.	
310203	Warning	[msg:%s]	Generic WARNING level system log	
310303	Warning	[msg:%s]	Generic WARNING level system log	
310307	Warning	[msg:%s]	Generic WARNING level system log	
310311	Warning	[msg:%s]	Generic WARNING level system log	
310315	Warning	[msg:%s]	Generic WARNING level system log	
310319	Warning	[msg:%s]	Generic WARNING level system log	
310323	Warning	[msg:%s]	Generic WARNING level system log	
310327	Warning	[msg:%s]	Generic WARNING level system log	
310331	Warning	[msg:%s]	Generic WARNING level system log	
311000	Warning	Attempt to change LMS of remote AP ignored		
311002	Warning	Rebooting: [reason:%s]		
311003	Warning	AP flash image is invalid		
311004	Warning	Missed [num:%d] heartbeats; rebootstrapping		
311006	Warning	Broken tunnel to switch detected on radio [radio:%d] VAP [vap:%d]; rebootstrapping		
311007	Warning	Broken tunnel to switch detected on wired AP interface [ifnum:%d]; rebootstrapping		
311010	Warning	AP could not boot from flash -- bad checksum		
311011	Warning	No Mesh Radio profile. Mesh role[role:%s] Band[band:%s] Radio[radio:%d].		
311012	Warning	Enet [enetnum:%d]: Unsupported speed [rspeed:%s]; using [using:%s]		
311026	Warning	[msg:%s]		
311028	Warning	AP LACP striping IP changed from [old_ip:%s] to [new_ip:%s]. Recreating VAPs of radio [radio:%d].		
311033	Warning	[msg:%s]		
311034	Warning	[msg:%s]		
312102	Warning	ESI pinger initialization failed	ESI pinger is used to monitor health of external servers by sending ICMP ECHO requests. Initialization of the pinger subsystem failed. ESI process will restart to correct this.	
312103	Warning	ESI server initialization failed	System encountered an internal error while creating queues to process notification from external servers. ESI process will restart	
312201	Warning	[func:%s](): Failed in PAPI_Send() - err:[err:%d] arg:[arg:%p].	This indicates error in PAPI_Send().	
312202	Warning	[func:%s](): Received message with wrong length([len:%d]), Ignore it.	This indicates error in receiving PAPI message.	
312203	Warning	[func:%s](): Unable to create Dispatcher.	This indicates error in creating dispatcher.	
312204	Warning	[func:%s](): Unable to initialize PAPI.	This indicates error in initializing PAPI.	
312304	Warning	stop_signal - Why was I called ... exiting		
312305	Warning	Waiting for dbstart...	The application is waiting for the database to be ready for access.	
312309	Warning	User DB query issue in: [call: %s]. SQL command: [cmd: %s].	This log indicates that there was an issue when a command was executed on the user database.	
312311	Warning	Client denylist purged by Administrator.	This log indicates that the client denylist was purged by the administrator.	
312402	Warning	[msg:%s]		
312504	Warning	stop_signal - Why was I called ... exiting		
312604	Warning	[msg:%s]		
313078	Warning	XSec Vlan Interface [vid:%d] not found line [ln:%d]	An error occured while adding/removing XSec port to/from VLAN, VLAN does not exist	
313185	Warning	Duplicate address detection failure for [ipv6addr:%s]/[prefix:%d] on vlan [vlanId:%d] interface	Configured IPv6 interface address is duplicate and is already in use in the network.	
313256	Warning	Route resolve returned an Error	A route could not be inserted because system could not find a matching interface for the gateway IP address	Check interface IP address configuration

313301	Warning	Ipv6 route resolve returned an error	A route could not be inserted because system could not find a matching interface for the gateway IP address	Check interface IP address configuration
313320	Warning	Error sending VRRP advertisement packet	A VRRP error message indicating that there was a failure while sending VRRP Advertisement	
313321	Warning	Error in periodic state check	An VRRP error message indicating that VRRP could not transition from BACKUP TO MASTER state	
313328	Warning	vrrp: vrid "[vrid:%d]" - VRRP state transitioned from [oldstate:%s] to [state:%s]	VRRP state has changed	
313331	Warning	VRRP: vrid "[vrid:%d]" - Missed 3 Hello Advertisements from VRRP Master [ipaddr:%s] for [period:%d] ms	Warning indicating that the VRRP Backup missed 3 Advertisements from Master	
313332	Warning	VRRP: vrid "[vrid:%d]"(Master) - Received VRRP Advertisement with HIGHER PRIORITY ([prio:%d]) from [ipaddr:%s]	Warning indicating that the VRRP Master received Advertisement with higher priority	
313445	Warning	Keepalives exhausted on tunnel [tunId:%d]	This message indicates that the tunnel is disabled because of lack of keepalive responses	
313600	Warning	Error sending VRRP IPv6 advertisement packet	A VRRP ipv6 error message indicating that there was a failure while sending VRRP ipv6 Advertisement	
313601	Warning	Error in periodic state check	An VRRP IPv6 error message indicating that VRRP could not transition from BACKUP TO MASTER state	
313608	Warning	vrrp ipv6: vrid "[vrid:%d]" - VRRP state transitioned from [oldstate:%s] to [state:%s]	VRRP state has changed	
313618	Warning	VRRP ipv6: vrid "[vrid:%d]" - Missed 3 Hello Advertisements from VRRP Master [ipaddr:%s] for [period:%d] ms	Warning indicating that the VRRP Backup missed 3 Advertisements from Master	
313619	Warning	VRRP ipv6: vrid "[vrid:%d]"(Master) - Received VRRP Advertisement with HIGHER PRIORITY ([prio:%d]) from [ipaddr:%s]	Warning indicating that the VRRP Master received Advertisement with higher priority	
313635	Warning	Function [function:%s]: LAGLIST get failed for interface [intIfNum:%d]	NA	
314807	Warning	Slot [slot:%d] CXE ports have [cells:%ld] cells, FFA [ffa:%ld] cells allocated	System is detecting if internal queue engine is stuck and needs restarting	Please contact support if this message persists
316001	Warning	Waiting for dbstart...	To be filled out	
316004	Warning	WMS Ready: AP Load Time (secs): [time1:%u], STA Load Time (secs): [time2:%u], Probe Load Time (secs): [time3:%u], Total Load Time (secs): [time4:%u]	To be filled out	
316006	Warning	Failed in adding probe from: IP [ip:%s] Type [type:%s]	Error in Addding Probe in the system	
316007	Warning	Unable to find/add a probe for IP [ip:%s] Type [type:%s]'	Error in finding/adding a probe	
316009	Warning	Unable to Update Device-LC-List mapping for '[mac:%s]/[ip:%s] hostname:[name:%s] status:[st:%d]'	This indicates LC-Map is unable to be updated due to invalid data	
316017	Warning	Invalid message received of type [msg_type:%d]	To be filled out	
316041	Warning	SQL Command at function [func: %s] line [line: %d] "[command:%s]" failed. Reason: [reason:%s]	To be filled out	
316042	Warning	Get probe list: Invalid probe [probe_mac:%s] for node [node_mac:%s]	To be filled out	
316063	Warning	Unable to create AP entry for [mac:%s]	To be filled out	
316068	Warning	RBTree Operation Error: At [function:%s] line:[line:%d] function:[rb_tree_fn:%s] info: [info:%s]	To be filled out	
316080	Warning	Connection to MMGRDB failed	To be filled out	
316081	Warning	Command [command:%s] failed. Reason: MMGRDB is NULL	To be filled out	
316092	Warning	Unable to create STA context for [mac:%s]. Num rows [nr:%d], num processed [np:%d], num added [na:%d]	The creation of in-memory data from persistent data from the database failed. The counts indicate the number of rows in the db, the number that had been processed, and the number added in memory.	
316101	Warning	Unknown RAP message from probe [ip:%s] on AP [bssid:%s]	To be filled out	
316102	Warning	Database operation failed: Operation [type:%s] IP [ip:%s], User:[user:%s] Password:[password:%s] DB:[db:%s]	To be filled out	
316110	Warning	Probe not found: PROBE BSSID [bssid:%m]	To be filled out	
316111	Warning	Performing [operation:%s]: wms module will exit in 1 second	To be filled out	
316208	Warning	Monitor [bssid:%s] extracted from SNMP tree not found in table.	To be filled out	
316226	Warning	Classification Server IP has changed :	To be filled out	

316230	Warning	CT command failed at:[fn:%s] line:[line:%d] operation:[op:%s]	To be filled out	
316231	Warning	CT command failed at:[fn:%s] line:[line:%d] operation:[op:%s] [info:%s]	To be filled out	
316232	Warning	ct_results() error. At:[fn:%s] line:[line:%d] type:[type:%s] info:[info:%s]	To be filled out	
316234	Warning	Cannot find Probe. At:[fn:%s] line:[line:%d] Probe [mac:%m]	This log indicates that the WMS process was notified by Station Management that a probe is down, and WMS does not have that Probe in its internal state. This can happen if WMS has already aged out the probe because it has not heard from it .	
316247	Warning	Event DB query failed in: [call: %s]. SQL command: [cmd: %s].	This log indicates that there was an issue when a command was executed on the event database.	
316260	Warning	Could not open file: [file: %s].	This log indicates that there was an issue when a file open command was executed.	
316261	Warning	Controller gateway IP is not configured.	This log indicates that the gateway IP of the controller may not be correctly configured.	
316262	Warning	Controller gateway MAC could not be determined.	This log indicates that the MAC address of the controller's gateway could not be determined.	
316263	Warning	Msg to get next bridge table entry has failed.	This log indicates that there was an issue while processing an internal message to retrieve bridge table entries.	
316264	Warning	Msg response from sos has unexpected length.	This log indicates that there was an issue while processing an internal message to retrieve bridge table entries.	
316265	Warning	Controller's MAC addresses could not be determined.	This log indicates that the MAC addresses owned by the controller could not be determined.	
316266	Warning	The RAP WML table [name: %s] profile could not be found.	This log indicates that the RAP WML Table profile could not be found.	
316267	Warning	Current state indicates that WMS is reaching capacity, so it is recommended to enable WMS-offload.	This log indicates that current state in the WMS module shows that WMS is reaching capacity, and so it is recommended to enable WMS-Offload.	
316274	Warning	[logstr:%s]. This log is for test purposes only; there is no error.	This log is for test purposes only. It should not appear in a released build.	
316285	Warning	Query to fix possible db corruption failed [retries:%d] times, and then succeeded. This likely occurred due to a wait for the db process to start.	This can occur in the situation where a query on a corrupt database has caused the database process to restart. The system will run a query to try and fix possible db corruption. During the time that the database process is restarting, the query being run to try and fix the corruption will not succeed, and is retried.	
316286	Warning	Unable to create AP context for [mac:%s]. Num rows [nr:%d], num processed [np:%d], num added [na:%d]	The creation of in-memory data from persistent data from the database failed. The counts indicate the number of rows in the db, the number that had been processed, and the number added in memory.	
316290	Warning	Invalid AMON message operation received of type [msg_type:%d]	Invalid AMON message operation type received.	
316292	Warning	WMS Event Table Cleanup: [str: %s]	This log is generated when issues are detected during the periodic cleanup of the WMS Event Table.	
316298	Warning	mallopt [str:%s] with status [status:%d]	This log is generated when mallopt fails to set the M_TRIM_THRESHOLD or the M_MMAP_THRESHOLD thresholds to disable the dynamic adjustment of mmap.	
316300	Warning	SQL Command [command:%s] has invalid parameters. Reason: [reason:%s]	This log is generated when an SQL Command has invalid or missing parameters to execute properly. The log includes debug info to help diagnose the issue.	
316302	Warning	[item:%s] set by [override:%s] at [function:%s] line:[line:%d].	This log is generated when the WMS system behavior is being overridden due to the presence of a test file.	
316303	Warning	Checking for DB schema upgrade...	This log is generated when wms starts and reads the existing DB for the first time.	
316304	Warning	DB [component:%s] upgrade [result:%s] Upgrade Time (secs) [time:%u].	This log is generated when wms starts and indicates if a DB upgrade was required or not.	

316308	Warning	Unexpected bssid [bssid:%s] detected for valid AP [base_bssid:%s]. Current classification [classification:%s].	This log is generated when WMS detects un-configured bssids with the same base BSSID as other valid APs	
317004	Warning	[str:%s]	NTP generic warning message	
325025	Warning	Reverting to default factory certificate.	Notification message to indicate reverting to default certificate	
326004	Warning	AM: Error Adding STA [mac_addr:%s] to AP [bssid_str:%s] SSID [ssid:%s]	To be filled out	
326070	Warning	AM: message too large:[len:%d]. Dropping!	To be filled out	
326073	Warning	AM: [line:%d]: response too long [bl:%d]	NOT USED	
326077	Warning	AM: [function:%s]: length mismatch expected [bytes_read:%d], got [msg_len:%d]	To be filled out	
326083	Warning	AM: Setting the communication path of state info to: Master switch	To be filled out	
326084	Warning	AM: Setting the communication path of state and stats info to: Local switch	To be filled out	
326085	Warning	AM: Setting collection of statistics to : [mode:%s]	To be filled out	
326096	Warning	AM: message too long [bl:%d]	To be filled out	
326101	Warning	AM: length mismatch for message [msg_type:%d], expected [bytes_read:%d], got [msg_len:%d]	To be filled out	
326157	Warning	AM: Too many Wi-Fi(s) interfaces = [wifi_index:%d]	To be filled out	
326158	Warning	AM: MAX_SIZE = [DET_STATS_READ:%d], actual size = [det_proc_stats_size:%d]	To be filled out	
326159	Warning	AM: Name of WIFI_INT is invalid([proc_interface:%s])	To be filled out	
326200	Warning	AM: Unable to find WIF for [bssid:%s]	To be filled out	
326201	Warning	AM: Calibration already in progress for [bssid:%s]	To be filled out	
326202	Warning	AM: Invalid Channel [channel:%d] for [bssid:%s]	To be filled out	
326229	Warning	AM: Signature name too big: [name:%s]	To be filled out	
326279	Warning	AM: Setting Learn Wired MACs at Controller to : [mode:%s]	This log indicates that the configuration has changed for the feature Learn Wired MACs at Controller.	
330000	Warning	Unable to create predefined profile [cmd:%s] "[inst:%s]": already exists in configuration.		
334307	Warning	stop_signal - Why was I called ... exiting		
334526	Warning	OSPF LSDB is 95% full. Number of LSAs [num:%d]		
334527	Warning	OSPF LSDB is 90% full. Number of LSAs [num:%d]		
335019	Warning	Major Alarm: [Major: %s]	Major system alarm log.	
335107	Warning	stop_signal - Why was I called ... exiting		
336007	Warning	stop_signal - Why was I called ... exiting		
339307	Warning	stop_signal - Why was I called ... exiting		
341004	Warning	[msg:%s]		
341011	Warning	AP image version mismatch [vcmodel:%s] [version:%s] [apmodel:%s]	The image version on the AP is not the same as that on the virtual controller. The AP will download a new image and reboot.	
341012	Warning	AP downloading flash image [url:%s].	The AP is downloading a new image to store in flash.	
341013	Warning	[role:%s] AP upgrading flash image [cmd:%s].	The AP is writing a new image in flash. When this process completes, the AP will reboot.	
341015	Warning	AP is operating in regulatory [domain:%s] [code:%d].	The AP is in specified regulatory domain.	
341032	Warning	Read configuration successfully, retry [time:%d], image size [size:%d].	The AP is loading configuration.	
341097	Warning	[func:%s]: mac-[mac:%s], version-[version:%s], ccode_idx-[id:%d].	The AP is upgrading image.	
341098	Warning	[func:%s]: Convert AP url-[url:%s], mode-[mode:%d], conductor-[ip:%s].	The AP is converting ap.	
341101	Warning	Execute command-[cli:%s].	Cli command.	
341102	Warning	Incorrect format for message type [type:%d]:[msg_len:%d]:[recv_len:%d]:[bytes_read:%d]:[from_ip:%s]:[from_port:%d].	Handle papi message.	
341103	Warning	Unknown version from [ipaddr:%s] in message type-[type:%d].	Handle papi message.	
341104	Warning	Invalid version for message type-[type:%d] from [ipaddr:%s] (local [ver:%s] vs. conductor [m_ver:%s]).	Handle papi message.	
341131	Warning	AP sends meshd parameters [cs_key:%s]-[key:%s]-[country_code:%d]-[over_air_provision:%d].	AP is sending mesh parameters.	

341132	Warning	Check sum mismatch for AP-[ip:%s], member [s_sum:%u] vs conductor [m_sum:%u], error_cnt [e_cnt:%u], recover_sent [sent:%u].	AP is checking configuration.	
341135	Warning	Conductor Changed - new [new_ip:%s] old [old_ip:%s] current swarm state [state:%d].	Master in network changed.	
341149	Warning	Sending upgrade url [url:%s] to [ap_ip:%s], mode [mode:%d], ip [ip:%s].	Master send upgrade url to slave.	
341159	Warning	Got AMP from dhcp ([org:%s]-[ip:%s]) vs. mine ([org1:%s]-[ip1:%s]).	Learning AMP info from DHCP.	
341164	Warning	send ap not allowed to [ip:%s].	Send not allowed msg to an AP.	
341165	Warning	send image match to [ip:%s].	Send image match msg to an AP.	
341166	Warning	Get interface [ifname:%s] ip: [ip:%s]/[mask:%s].	Print interface ip.	
341167	Warning	Uplink [uplink_name:%s], state [old:%s]->[new:%s].	Uplink state changed.	
341169	Warning	Add uplink [type:%s], priority [pri:%d].	Add new uplink.	
341170	Warning	Del uplink [type:%s].	Del uplink.	
341171	Warning	Active 3g uplink, enable [yes: %d].	Active 3g uplink.	
341172	Warning	Find enet0 name [name: %s].	Find enet0 uplink name.	
341173	Warning	Current uplink set to [type:%s], state [state:%s].	Print current uplink.	
341174	Warning	No current uplink, pick the highest one - [uplink_name:%s], state [state:%s]/[rstate:%s], priority [priority:%u].	Pick the highest uplink.	
341175	Warning	Connecting with current uplink - [type:%s].	Connect with current uplink.	
341176	Warning	Probing too long with current uplink - [type:%s].	Probe too long.	
341177	Warning	Try next uplink because current uplink is down: [current:%s] --> [next:%s].	Try next uplink.	
341181	Warning	Setup ip for uplink [uplink_name:%s].	Setup ip for uplink interface.	
341182	Warning	Setup vpn for rap conversion - [ip:%s].	Setup vpn for rap conversion.	
341183	Warning	Downloading rap image via vpn - url [url:%s].	Downloading rap image via vpn.	
341184	Warning	Downloading rap image via vpn timeout - count [count:%d].	Downloading rap image via vpn timeout.	
341185	Warning	Retrieving ip address from [inf:%s], ip [ip:%s], mask [mask: %s].	Retrieving ip address from an interface.	
341194	Warning	Loading configuration, func [func:%s], line [line:%d].	loading AP configuration.	
341199	Warning	[func:%s]: send config to member [ip:%s], csum [csum: %u], using url [url:%d], auto save disable [flag:%d].	Send ap config to slave.	
341205	Warning	Applying enet config : port [name:%s].	Apply enet config.	
341206	Warning	Command syntax error: [cmd:%s].	Command syntax error.	
341207	Warning	AP support up to [num: %d] SSID.	Max ssid support	
341208	Warning	Activate SSID [SSID1: %s], remove SSID [SSID2:%s].	Deacive SSID	
341227	Warning	uplink detection: total_icmp_sent [sent:%d], total_icmp_lost [lost:%d], continuous_icmp_lost [clost:%d].	Uplink detetction statistics.	
341228	Warning	uplink switchover internet since link threshold is reached [thld:%d].	Uplink switchover internet.	
341229	Warning	uplink switchover vpn since ipsec goes down for a while, cnt [cnt:%d] vs. threshold [thld:%d].	Uplink switchover vpn.	
341245	Warning	Not allowed ap [mac:%s] for invalid subscription status [status:%s] in function[function:%s] [line:%d] .	Not allowed ap for invalid subscription status	
341250	Warning	VC record delta configuration, malloc error. len [len:%d] port [port:%d] flags [flags:%d] seq [seq:%d] case [case:%s]	VC record delta configuration, malloc error.	
341251	Warning	VC record new delta configuration entry. cfg_id [cid:%d] current [c:%d] top [t:%d] len [len:%d] port [port:%d] flags [flags:%d] seq [seq:%d]	VC record new delta configuration entry.	
341252	Warning	VC send delta configurations to ap error. ap [ap_ip:%s] ap_cfg_id [acid:%d] current_cfg_id [cid:%d] top_cfg_id [tid:%d] case [case:%s]	VC send delta configuration to ap error.	
341254	Warning	VC add delta configuration id [id:%d] to msg [msg:%s].	VC add delta configuration to msg.	
341258	Warning	AP receive delta configuration id [acid:%d] current_cfg_id [cid:%d] from msg [msg:%s] is not correct.	AP receive delta configuration id from msg is not correct.	
341260	Warning	VC rejects the [number:%d]th ap because IAP9x in the swarm.	VC rejects slave for ap number	
341261	Warning	VC rejects the IAP9x becuase we have [number:%d] users in local DB.	VC rejects slave for internal DB	
341262	Warning	switch to higher uplink [uplink_name:%s] by preemption.	switch to highest uplink.	
341263	Warning	enable uplink [uplink_name:%s].	enable a uplink.	
341264	Warning	disable uplink [uplink_name:%s].	disable a uplink.	
341265	Warning	enable ethernet uplink [uplink_name:%s].	enable ethernet uplink.	

341266	Warning	uplink preempt to [uplink_name:%s].	uplink preempt.	
341267	Warning	Add wired port [port_name:%s] to bonding table.	wired port add to bonding table.	
341268	Warning	del wired port [port_name:%s] from bonding table.	wired port delete from bonding table.	
341269	Warning	uplink [uplink_name:%s] is exist update it.	update uplink table because uplink is already exist.	
341274	Warning	Update election ip from [inf:%s], election ip [elect_ip:%s]/[elect_mask:%s].	Update election ip and mask.	
341289	Warning	Sending full configuration to member ip = [ip:%s], ap config dirty = [dirty:%d] error cnt = [cnt:%d]	Sending full configuration from Master to slaves APs.	
341307	Warning	[func:%s]: receive config from conductor [ip:%s], len [len: %u], new csum [ncsum: %u], old csum [ocsum: %u], using url [url:%d], auto save disable [flag:%d], swarm state is [state:%d].	Receive ap config from Master.	
341317	Warning	Regulatory table file init at version [version:%s], build [build:%s].	Initialize regulatory table file	
341318	Warning	autojoin: member auth failed, conductor send write erase to member [mac:%s] [sn:%s].	VC send write erase to slave.	
341320	Warning	autojoin: A potential member comes to conductor, and it's licensed by cloud, mac [mac:%s].	a potential slave comes, and it's not licensed by cloud.	
341322	Warning	autojoin: A member AP [mac:%s] [sn:%s] auth failed from cloud, remove it.	A slave AP auth failed from cloud, remove it.	
341325	Warning	autojoin: A potential APs created, mac [mac:%s], sn [sn:%s].	A potential APs created.	
341326	Warning	autojoin: get central config flag from flash, flag is [flag:%s].	get central config flag from flash.	
341329	Warning	[func:%s]: not find mac entry for auth-survivability client-[mac:%m].	look up mac entry fail.	
341331	Warning	[func:%s]:, not find user entry for auth-survivability username-[user:%s].	look up user entry fail.	
341335	Warning	[msg:%s]	netlink warning message	
341339	Warning	Uplink [uplink_name:%s], reach-state [old:%s]->[new:%s].	Uplink reach-state changed.	
342007	Warning	[msg:%s]		
342008	Warning	[func:%s], [msg:%s]		
342009	Warning	stop_signal - Why was I called ... exiting		
343007	Warning	[thread:%u] [func:%s] [line:%d] [msg:%s]	System related warning configuration messages logged in the mDNS proxy (mdns)	
343505	Warning	[func:%s] [line:%d] [msg:%s]	System related warning messages logged in the AirGroup	
345307	Warning	stop_signal - Why was I called ... exiting		
346007	Warning	([func:%s] [line:%d]) [msg:%s]	System related warning messages logged in HA_MGR	
347002	Warning	[msg:%s]	Warning condition occurred in UCM.	
347005	Warning	VoIP Start/Stop received ... VoIP hash table not created yet		
347007	Warning	[func:%s]: [ip:%pI4] message out of order		
347008	Warning	[func:%s]: too many voip clients		
348307	Warning	stop_signal - Why was I called ... exiting		
350001	Warning	Error sending SIGHUP to Apache	To be filled out	
351014	Warning	LLDP NULL handle returned at Function: [function:%s] for port [port:%d]	NA	
354023	Warning	[__FUNCTION:%s]: URL lookup failed : [url: %s]		
356002	Warning	[msg:%s]	RNG mgr module warning message	
356304	Warning	[msg:%s]	Warning message about a condition in Mcell process	
356305	Warning	stop_signal - Why was I called ... exiting	Custom warning message about stop signal sent to Mcell process	
358006	Warning	stop_signal - Why was I called ... exiting		
359002	Warning	[msg:%s]	System related warning messages logged in HCM	
360007	Warning	stop_signal - Why was I called ... exiting		
381007	Warning	stop_signal - Why was I called ... exiting		
386004	Warning	[msg:%s]	UDMD system warning log	
390007	Warning	stop_signal - Why was I called ... exiting		
393003	Warning	[func:%s] [line:%d] [msg:%s]	System related warning messages logged in by DPI MGR	
394003	Warning	[msg:%s]	Generic warning level system log	
397001	Warning	[msg:%s]	System related warning messages logged by DDNS_CLIENT	
398503	Warning	[msg:%s]	System related warning messages logged in Policymgr	
398553	Warning	[msg: %s]	System related warning messages logged in Policy manager uplink.	Contact tech-support.
399501	Warning	[module:%s] [msg:%s]	System related warning messages logged by LHM	

399826	Warning	[msg:%s]	This is an webserver system warning log.	
399831	Warning	[msg:%s]	This is an webserver system warning log.	
399838	Warning	[error:%s]	This is an internal system debugging log.	

ID	Type	Message	Description	Action
509001	Alert	FIPS Alert: [msg:%s]	This is a FIPS alert log in user module.	
509002	Critical	FIPS Critical: [msg:%s]	This is a FIPS critical log in user module.	
500001	Debug	Station [mac:%m], [ip:%s]: Mobile IP PROXY finite state machine event [event:%s]: current: [curstate:%s], next: [nextstate:%s]	Mobile IP state machine debugging	
500003	Debug	Station [mac:%m], [ip:%s]: Event threshold exceeded timer started	NA	
500005	Debug	Station [mac:%m], [ip:%s]: Event threshold exceeded timer expired, mobile current state [cs:%s] prev state [ps:%s]	NA	
500023	Debug	Proxy mobile [mac:%m], [ip:%s]: call status [cs:%s] clientip [cip:%pI4], action ==> [act:%s]		
500030	Debug	Station [mac:%m], [ip:%s]: Added bridge entry for local station on vlan [vlan:%d] v6-vlan [v6_vlan:%d] to [interface:%s] data path flags [flags:%s]	Indicates the port or tunnel that mobility has for a station location, this destination is downloaded in the data path	
500032	Debug	Station [mac:%m], [ip:%s]: Added home bridge entry for local station on home vlan [vlan:%d] v6-vlan [v6_vlan:%d], data path flags [flags:%s]	On inter-VLAN roaming, the data path implementation requires a dummy bridge entry to be installed on the station's home VLAN, This message should be issues with the station home vlan and should be paired with a message id 500006 on the currently visited VLAN.	
500037	Debug	Station [mac:%m], [ip:%s]: Updated bridge entry for local station on vlan [vlan:%d] v6-vlan [v6_vlan:%d] to [interface:%s] data path flags [flags:%s]	Indicates the port or tunnel that mobility has for a station location has changed, the new destination is downloaded in the data path	
500039	Debug	Station [mac:%m], [ip:%s]: Updated home bridge entry for local station on home vlan [vlan:%d] v6-vlan [v6_vlan:%d], data path flags [flags:%s]	On inter-VLAN roaming, the data path implementation requires a dummy bridge entry to be installed on the station's home VLAN, This message should be issues with the station home vlan and should be paired with a message id 500013 on the currently visited VLAN.	
500045	Debug	Station [mac:%m], [ip:%s]: Removed bridge entry for local station on vlan [vlan:%d] v6-vlan [v6_vlan:%d]; ingress interface: [if:%s]	Mobility state is being deleted for station, removing the bridge entry for a station in the data path	
500047	Debug	Station [mac:%m], [ip:%s]: Removed home VLAN bridge entry for local station on VLAN [vlan:%d] v6-vlan [v6_vlan:%d]	Mobility state is being deleted for station, removing the home bridge entry for a station in the data path	
500049	Debug	Station: [mac:%m], [ip:%s]: HomeVlan: [hv:%d] Current Vlan: [cv:%d] v6-vlan: [v6_vlan:%d] roaming status: [rs:%s] Proxy state: [ps:%s] at line [ln:%d]		
500051	Debug	Station: [mac:%m], [ip:%s]: Home Vlan [hv:%d] will be De-Authenticated as its using stale IP address that cannot be served locally		
500054	Debug	Station [mac:%m]: Re-Added bridge entry for station on vlan [vlan:%d] assigned vlan [avlan:%d] v6-vlan [v6_vlan:%d] to [interface:%s] data path flags [flags:%s] roam case [roam:%s]	Indicates that mobility has reprogrammed station bridge entry due to station re-assoc without disassoc	
500055	Debug	Station [mac:%m]: [ip:%pI4] IP address change to [pip:%pI4] on vlan [vlan:%d] etype [etype:%x] protocol [proto:%d]	Mobility detected an IPv4 address change in the packet received from datapath	
500056	Debug	Station [mac:%m]: Info for local station current vlan [cvlan:%d]; previous vlan [pvlan:%d]; station home vlan [svlan:%d]; delete vlan [dvlan:%d]; v6-vlan [v6_vlan:%d]; current ingress interface: [if:%s]; previous ingress interface: [iif:%s] at [fn:%s] [ln:%d]	Debug information for a local mobility station	
500057	Debug	Station [mac:%m], [ip:%s]: L2 miss on pkt IP [pip:%p] ingress port [ing:%s] vlan [vlan:%d] v6-vlan [v6_vlan:%d] etype [etype:%x] protocol [proto:%d] state current [cs:%s] previous [ps:%s]	Debug information for L2 miss event from a mobility station	
500058	Debug	Station [mac:%m], [ip:%s]: No mobility delete initiated at [line:%d]	Debug information indicating when no mobility station delete is initiated	
500059	Debug	Station [mac:%m]: [str:%s] at [line:%d]	Debug information indicating when mobility station disassociates or L2 station gets deleted by authmgr	
500079	Debug	Station [mac:%m], [ip:%s]: Initiating Proxy mobile (current state [cs:%s], prev state [ps:%s]) delete reason [rs:%s] Roaming Status: [stu:%s]		
500080	Debug	Station [mac:%m], [ip:%s]: Station is not authenticated and tries to use and IP address not matching incoming VLAN, station will be assign to incoming VLAN [vlan:%d] at line [lin:%d]	NA	

500102	Debug	Station [mac:%m], [ip:%s]: FA FSM recv event [evt:%s] current: [cur:%s] next: [nxt:%s]	NA	
500104	Debug	Station [mac:%m], [ip:%s]: Cannot find a proper HA Security Association to send discovery Registration Request to Home Agent at [ha:%pI4]	NA	
500105	Debug	Station [mac:%m], [ip:%s]: Received a Registration Reply without the expected Vendor session extension while performing Home agent discovery; Ignoring	NA	
500106	Debug	Station [mac:%m], [ip:%s]: Received a Registration Reply without the expected Home Agent address while performing Home agent discovery; Ignoring	NA	
500107	Debug	Station [mac:%m], [ip:%s]: Received HA discovery reply from candidate HA [ha:%pI4]; [session:%s] have a session line [ln:%d]	NA	
500109	Debug	Station [mac:%m], [ip:%s]: HA discovery failed; assigned local switch as HA, station is at home	NA	
500111	Debug	Station [mac:%m], [ip:%s]: Found Home Agent address [ha:%pI4] in Home Agent Table (HAT)	NA	
500112	Debug	Station [mac:%m], [ip:%s]: Found [hacnt:%d] possible(s) Home Agent(s) in HAT [halist:%s], will perform HA discovery	NA	
500113	Debug	Station [mac:%m], [ip:%s]: Cannot find a proper Visitor Security Association to send Registration Registration Request to Home Agent at [ha:%pI4]	NA	
500118	Debug	Station [mac:%m], [ip:%s]: Added/Updated bridge entry for visitor on vlan [vl:%d], datapath flags [flg:%s]	NA	
500120	Debug	Station [mac:%m], [ip:%s]: Visitor entry timeout expired and entry is not in active state	NA	
500122	Debug	Active Visitor's [mac:%m], [ip:%s]: entry will be deleted; station proxy state: [prxst:%s] IP [sta_ip:%s]	NA	
500123	Debug	Pending Visitor's [mac:%m], [ip:%s]: entry will be deleted; station proxy state: [prxst:%s] IP [sta_ip:%s]	NA	
500124	Debug	Station [mac:%m], [ip:%s]: (RRV, FA): I bit support has not been negotiated. Setting I bit to 0 in message	NA	
500125	Debug	Station [mac:%m], [ip:%s]: Setting Revocation Retransmit after [tm:%d] millisecs. Number of retransmits [rtrns:%d]	NA	
500127	Debug	Station [mac:%m], [ip:%s]: Deleting Auth entry for visitor, reason [cd:%x]	NA	
500128	Debug	Station [mac:%m], [ip:%s]: Error deleting Auth state for visitor	NA	
500134	Debug	Station [mac:%m], [ip:%s]: Deleted bridge entry for visitor on vlan [vl:%d]	NA	
500136	Debug	Station [mac:%m], [ip:%s]: FA Received dissassociation from proxy for visitor; starting stale timeout	NA	
500137	Debug	Station [mac:%m], [ip:%s]: Stopping stale timeout	NA	
500138	Debug	Station [mac:%m], [ip:%s]: FA Mobility stale entry timeout, visitor state will be deleted	NA	
500139	Debug	Station [mac:%m], [ip:%s]: Pending visitor's entry found for Registration Reply received from [srcip:%pI4], home-agent-addr [ha:%pI4], HAT HA [hat_ha:%pI4]	NA	
500140	Debug	Station [mac:%m], [ip:%s]: Active visitor's entry found for Registration Reply received from [srcip:%pI4], home-agent-addr [ha:%pI4], HAT HA [hat_ha:%pI4]	NA	
500141	Debug	Station [mac:%m], [ip:%s]: (FA): Pending visitor's entry found for Registration Revocation received from [ha:%pI4] for visitor [vistype:%s]	NA	
500142	Debug	Station [mac:%m], [ip:%s]: (RRV FA): Active visitor's entry found for Registration Revocation received from [ha:%pI4] for visitor [vistype:%s]"	NA	
500143	Debug	Station [mac:%m], [ip:%s]: (RRV FA): Home Agent Address mismatch in Revocation Message. Visitor Entry: [ve:%pI4] Revocation Message: [ha:%pI4]	NA	
500144	Debug	Station [mac:%m], [ip:%s]: (RRV FA): COA Address mismatch in Revocation Message. Visitor Entry: [ve:%pI4] Revocation Message: [fa:%pI4]	NA	
500145	Debug	Station [mac:%m], [ip:%s]: (RRV FA): Previous Registration Reply Reg ID [rrid:%d] greater than Revocation Reg ID [rrvid:%d]	NA	

500146	Debug	Station [mac:%m], [ip:%s]: (FFV FA): Active visitor's entry NOT found for Registration Revocation received from [ha:%pI4] for visitor, ignore	NA	
500147	Debug	Station [mac:%m], [ip:%s]: (RRV FA): Visitor entry found for Registration Revocation ACK received from [agt:%pI4] for visitor	NA	
500148	Debug	Station [mac:%m], [ip:%s]: Could not match Registration ID [regh:%x]h:[regl:%x]h on Registration Reply received from [agt:%pI4] for visitor	NA	
500149	Debug	Station [mac:%m], [ip:%s]: MIP message: Agent Discovery Reply [rp:%s] received from [agt:%pI4], user [us:%s], Regid [regh:%x]h:[regl:%x]h, [sess:%s] have active session	NA	
500150	Debug	Station [mac:%m], [ip:%s]: MIP message: Registration Reply [rp:%s] received from [agt:%pI4] for visitor, user [us:%s], Regid [regh:%x]:[regl:%x]h	NA	
500151	Debug	Station [mac:%m], [ip:%s]: Registration Reply Details: from [agt:%pI4]:[port:%d] [rp:%s], lifetime [lft:%d] seconds, Home Address [ha:%pI4], Home Agent Address [hagt:%pI4], Vendor Extensions: [ext:%s]	NA	
500152	Debug	Station [mac:%m], [ip:%s]: MIP message: [typ:%s] Request sent to [agt:%pI4], user [us:%s], Regid [regh:%x]h:[regl:%x]h	NA	
500153	Debug	Station [mac:%m], [ip:%s]: Registration Request Details: to [agt:%pI4]:[port:%d], lifetime [lft:%d] seconds, Home Address [ha:%pI4], Home Agent Address [hagt:%pI4], care-of Address [coa:%pI4], Vendor Extensions: [aext:%s]	NA	
500154	Debug	Station [mac:%m], [ip:%s]: Cannot find a proper HA Security Association to send Registration Registration Request to Home Agent at [haip:%pI4]	NA	
500155	Debug	Station [mac:%m], [ip:%s]: Visitor Entry will go down as FA-HA L2-GRE Tunnel with Start IP [sip:%s] End Point IP [eip:%s] is detected DOWN	NA	
500156	Debug	Station [mac:%m], [ip:%s]: Visitor Entry created with proxy state [st:%s]	NA	
500158	Debug	Visitor: [mac:%m], [ip:%s]: Received RRV message as mobile client is deleted due to ESI Blacklisting on HA [homeaddr:%pI4]		
500160	Debug	User: [mac:%m], [ip:%s]: [msg:%s]		
500161	Debug	Visitor: [mac:%m], [ip:%s]: Session Table entries update for Tunnel-id [tun:%d] [status:%s]		
500162	Debug	Station [mac:%m], [ip:%s]: Ignoring HA discovery reply as source [ha_reply:%pI4] does not match with visitor cached home agent addr [vha:%pI4]	NA	
500164	Debug	Station [mac:%m]: Derived Vlan update: proxy current vlan [cvlan:%d], proxy home vlan [hvlan:%d], visitor received derived vlan [dvlan:%d], visitor home vlan [vhvlan:%d], visitor station vlan [vsvlan:%d], visitor previous station vlan [vpsvlan:%d], data ready vlan [drvlan:%d] [ln:%d]	NA	
500165	Debug	Station [mac:%m]: Visitor bridge info: visitor station vlan [vsvlan:%d], visitor previous station vlan [vpsvlan:%d]	NA	
500166	Debug	Station [mac:%m]: Updating MIP with STM Assoc info, BSSID [bssid:%m]	NA	
500200	Debug	Station [mac:%m], [ip:%s]: HA FSM recv event: [evt:%s] current: [cur:%s], next: [nxt:%s]	NA	
500202	Debug	Station [mac:%m], [ip:%s]: Registration Request from [agt:%pI4] rejected because of registration ID mismatch	NA	
500203	Debug	Station [mac:%m], [ip:%s]: Cannot obtain Home VLAN for binding	NA	
500204	Debug	Station [mac:%m], [ip:%s]: Registration Request from [agt:%pI4] rejected because the station HAT HA address was not received in Vendor extension	NA	
500205	Debug	Station [mac:%m], [ip:%s]: Updating binding authentication state from proxy; name [nm:%s], type [ty:%d], l2 role [rl:%s]	NA	
500206	Debug	Station [mac:%m], [ip:%s]: "Creating binding authentication state from Registration request name [nm:%s], type [ty:%d], l2 role [rl:%s]	NA	
500211	Debug	Station [mac:%m], [ip:%s]: Added/Updated bridge entry for binding on vlan [vl:%d], datapath flags [fl:%s]	NA	

500213	Debug	Station [mac:%m], [ip:%s]: Error sending Registration Revocation Acknowledgement for binding	NA	
500214	Debug	Station [mac:%m], [ip:%s]: Home Agent binding expired for station	NA	
500215	Debug	Station [mac:%m], [ip:%s]: Registration Request from [agt:%pI4] rejected because of registration ID mismatch	NA	
500217	Debug	Station [mac:%m], [ip:%s]: Station moved; creating/using new tunnel from local address [addr:%pI4] to remote COA address [coa:%pI4]	NA	
500220	Debug	Station [mac:%m], [ip:%s]: Binding handoff from previous COA [coa:%pI4] to new COA [nwcoa:%pI4], will send revocation to previous FA	NA	
500221	Debug	Station [mac:%m], [ip:%s]: Binding handoff from previous COA [coa:%pI4] to new COA [nwcoa:%pI4], Update failed, but will send revocation to previous FA regardless	NA	
500225	Debug	Station [mac:%m], [ip:%s]: Deleted bridge entry for binding on vlan [vl:%d]	NA	
500227	Debug	Station [mac:%m], [ip:%s]: Notify AAA binding entry deleted	NA	
500229	Debug	Station [mac:%m], [ip:%s]: Binding entry can't be removed from active list	NA	
500230	Debug	Station [mac:%m], [ip:%s]: Binding entry is deleted	NA	
500231	Debug	Station [mac:%m], [ip:%s]: (HA): I bit support has not been negotiated	NA	
500232	Debug	Station [mac:%m], [ip:%s]: (HA): Interrupting revocation retransmission for COA [coa:%pI4] lifetime expired	NA	
500233	Debug	Station [mac:%m], [ip:%s]: (HA): Interrupting revocation retransmission for COA [coa:%pI4]; maximum number of retransmissions reached	NA	
500234	Debug	Station [mac:%m], [ip:%s]: (HA): Binding entry found for Registration Revocation ACK received from [agt:%pI4] for station [stm:%pI4]	NA	
500235	Debug	Station [mac:%m], [ip:%s]: (HA): Active binding entry found for Registration Revocation received from [agt:%pI4] for station [stm:%pI4]	NA	
500236	Debug	Station [mac:%m], [ip:%s]: (HA): Home Agent Address mismatch in Revocation Message. Binding Entry: [ha:%pI4] Revocation Message: [dom:%pI4]	NA	
500237	Debug	Station [mac:%m], [ip:%s]: (HA): COA Address mismatch in Revocation Message. Binding Entry: [ha:%pI4] Revocation Message: [dom:%pI4]	NA	
500238	Debug	Station [mac:%m], [ip:%s]: (HA): Previous Registration Reply Reg ID [gid:%d] greater than Revocation Reg ID [rgid:%d]	NA	
500239	Debug	Station [mac:%m], [ip:%s]: Mobile IP message from [ha:%pI4] rejected: RegId high is out of range, received=[rcv:%x]h, local=[lcl:%x]h, allowed difference=[diff:%x] (timestamps)	NA	
500240	Debug	Station [mac:%m], [ip:%s]: Mobile IP message from [ha:%pI4] rejected: RegID is lower than last received RegId (timestamps)	NA	
500241	Debug	Station [mac:%m], [ip:%s]: Received deregistration; we have no binding, ignoring	NA	
500242	Debug	Station [mac:%m], [ip:%s]: Received deregistration; lifetime is 0), ignoring	NA	
500244	Debug	Station [mac:%m], [ip:%s]: Received an RRQ while already processing an event for binding	NA	
500245	Debug	Station [mac:%m], [ip:%s]: Received an RRQ for existing binding with a new SPI	NA	
500246	Debug	Station [mac:%m], [ip:%s]: MIP message: Agent Discovery Reply sent to [agt:%pI4], user [usr:%s] Regid [gid:%x]h:[gidl:%x]h, [sess:%s] have active session	NA	
500247	Debug	Station [mac:%m], [ip:%s]: MIP message: Registration Reply [code:%s] sent to [agt:%pI4] for binding, user [usr:%s], Regid [gid:%x]h:[gidl:%x]h	NA	
500248	Debug	Station [mac:%m], [ip:%s]: Registration Reply Details to [agt:%pI4]:[prt:%d] [stm:%s], lifetime [lft:%d] seconds, Home Address [ha:%pI4], Home Agent Address [haa:%pI4], Vendor Extensions: [ext:%s]	NA	
500249	Debug	Station [mac:%m], [ip:%s]: Received an RRQ with a too small lifetime	NA	
500250	Debug	Station [mac:%m], [ip:%s]: MIP message: [typ:%s] received from [agt:%pI4] for binding, user [usr:%s], Regid [gid:%x]h:[gidl:%x]h	NA	

500251	Debug	Station [mac:%m], [ip:%s]: Registration Request Details: from [agt:%pI4]:[prt:%d], lifetime [lft:%d] seconds, Home Address [ha:%pI4], Home Agent Address [haa:%pI4], care-of Address [coa:%pI4] Vendor Extensions: [ext:%s]	NA	
500254	Debug	Binding: [mac:%m], [ip:%s]: Received RRV message as mobile client is deleted due to ESI Blacklisting on FA [coa:%pI4]		
500255	Debug	Station [mac:%m], [ip:%s]: Registration Request from [agt:%pI4] rejected because the station MAC address was not received in Vendor extension	NA	
500348	Debug	Station [mac:%m], [ip:%s]: not yet data ready OR its a wired/3rd-Party-AP user off untrusted port and Standalone AP is disabled (ip mobile proxy stand-alone-AP) ...dropping packet -- line [ln:%d]	NA	
500400	Debug	Station [mac:%m], [ip:%s]: Received AUTH_DONE msg from Auth	NA	
500402	Debug	Station [mac:%m], [ip:%s]: Receive User delete from Auth, proxy mobile prev state [ps:%s] current state [cs:%s] delete reason [drs:%s]	NA	
500405	Debug	Station [mac:%m], [ip:%s]: Sending MSG_INTERMS_MOVE to AAA, Vlan [vl:%d], port [pt:%s], tunnel id [tun:%d], flag [fl:%s] HA-IP [ha:%s]	NA	
500407	Debug	Station [mac:%m], [ip:%s]: Sending User update for visitor, User name [us:%s], L2 Role [rl:%s], Auth type [ty:%d], Auth status [st:%d], ESSID [ess:%s], AP: Name [ap:%s] Group [apgrp:%s]	NA	
500409	Debug	Station [mac:%m], [ip:%s]: Sending MSG_MOVE_USER to Auth	NA	
500411	Debug	Station [mac:%m], [ip:%s]: Sending User update for binding, User name: [us:%s], L2 Role: [rl:%s], Auth type: [ty:%d], Auth status: [sts:%d], ESSID: [ess:%s], AP: Name [ap:%s] Group [apgrp:%s]	NA	
500414	Debug	Station [mac:%m], [ip:%s]: Received User Update from Auth, User name [us:%s], L2 Role [rl:%s], Auth type [ty:%d], Auth status [as:%d], ESSID [ess:%s], AP: Name [ap:%s] Group [apgrp:%s]	NA	
500415	Debug	Station [mac:%m], [ip:%s]: Data ready message from auth default vlan [dvl:%d] assigned vlan [avl:%d], mobile assigned vlan [mavl_id:%d], mobile home vlan [mhvl_id:%d]	NA	
500416	Debug	Station [mac:%m], [ip:%pI4]: Delete user : does not match with AuthMsg Ip [aip:%s], proxy mobile prev state [ps:%s] current state [cs:%s] delete reason [drs:%s], ignoring auth message	NA	
500417	Debug	Station [mac:%m], [ip:%s]: Derived vlan [dvl:%d] added to mobility data ready database	NA	
500418	Debug	Station [mac:%m], [ip:%s]: Derived vlan [dvl:%d] deleted from mobility data ready database	NA	
500419	Debug	Station [mac:%m], [ip:%s]: Sending MIP_AUTH_MSG_MSMOVE to Auth, mobile state [st:%s]	NA	
500420	Debug	Station [mac:%m], [ip:%s]: Sending MSG_DELETE_USER to Auth, mobile state [st:%s]	NA	
500421	Debug	Station [mac:%m], [ip:%s]: binding will be deleted, updating Auth	NA	
500422	Debug	Station [mac:%m], [ip:%s]: Sending IGMP membership query message to pim	NA	
500423	Debug	Station [mac:%m], [ip:%s]: Received IGMP host membership for [mip:%pI4], MCG details [mcg:%s]	NA	
500424	Debug	Station [mac:%m], [ip:%s]: Sending notification [msgtype:%s] flags [flg:%s], roaming state [rms:%s], current vlan [cv:%d], v6-vlan [v6_vlan:%d], ingress [cing:%s] to pim	NA	
500425	Debug	Station [mac:%m], [ip:%s]: Sending notification [msgtype:%s] flags [flg:%s], roaming state [rms:%s], current vlan [cv:%d], v6-vlan [v6_vlan:%d], ingress [cing:%s], MCG: [mcgs:%s] to pim	NA	
500426	Debug	Station [mac:%m], [ip:%s]: Received L2 miss opcode [op:%s] from Auth	NA	
500427	Debug	Station [mac:%m], [ip:%s]: Receive Unknown IP [aip:%s] from Auth, proxy mobile prev state [ps:%s] current state [cs:%s], ignoring	NA	

500428	Debug	Station [mac:%m], [ip:%s]: Receive Unknown IP from Auth, proxy mobile no state, ignoring	NA	
500429	Debug	Station [mac:%m], [ip:%s]: Receive Unknown IP [aip:%s] from Auth, proxy mobile prev state [ps:%s] current state [cs:%s] delete reason [drs:%s]	NA	
500430	Debug	Station [mac:%m], [ip:%s]: Receive Unknown IP from Auth, proxy mobile no state, notify auth to delete user	NA	
500431	Debug	Station [mac:%m], [ip:%s]: Receive Unknown IP [aip:%s] from Auth, proxy mobile prev state [ps:%s] current state [cs:%s], notify auth to delete user	NA	
500432	Debug	Station [mac:%m], [ip:%s]: User miss message from auth HA-UUID [ha_uuid:%s]	NA	
500433	Debug	Station [mac:%m]: User miss station IPv4 address updated from [oip:%s] to [nip:%s]	NA	
500434	Debug	Station [mac:%m]: User miss station IPv6 address added [ip6:%s] count [count:%d] idx [idx:%d]	NA	
500435	Debug	Station [mac:%m]: User delete station IPv6 address deleted [ip6:%s] count [count:%d] idx [idx:%d]	NA	
500436	Debug	Station [mac:%m]: Requesting data ready from Auth	NA	
500437	Debug	Station [mac:%m]: User miss station IPv4 address changed from [oip:%s] to [nip:%s]	NA	
500438	Debug	Station [mac:%m]: Update HA-UUID [ha_uuid:%s]	NA	
500450	Debug	Station [mac:%m], [ip:%pI4]: Received frame with source IP on Automatic Private IP Addressing (APIPA) subnet, Dropping	NA	
500462	Debug	Station [mac:%m], [ip:%s]: Error sending Gratuitous ARP to datapath on VLAN [vl:%d]	NA	
500463	Debug	Station [mac:%m], [ip:%s]: Sent Gratuitous ARP on VLAN [vl:%d] with mac [mc:%m] for IP address [sta:%pI4]	NA	
500491	Debug	Station [mac:%m], [ip:%s]: Added RRV entry for station to match replies	NA	
500492	Debug	Station [mac:%m], [ip:%s]: Removed RRV entry	NA	
500493	Debug	Station [mac:%m], [ip:%s]: MIP message: Registration Revocation sent to switch [sw:%pI4]	NA	
500494	Debug	Station [mac:%m], [ip:%s]: MIP message: Registration Revocation ACK sent to switch [sw:%pI4]	NA	
500495	Debug	Station [mac:%m], [ip:%s]: Received Reflection of sent Registration Revocation Message from [sw:%pI4], discarding	NA	
500496	Debug	Station [mac:%m], [ip:%s]: Received Registration Revocation Message from peer at [sw:%pI4] for RRV pending station	NA	
500497	Debug	Station [mac:%m], [ip:%s]: RRV entry found for Registration Revocation ACK received from [sw:%pI4]	NA	
500498	Debug	Station [mac:%m], [ip:%s]: Could not match Registration ID ([reg:%x]) on Revocation ACK received from [sw:%pI4]	NA	
500499	Debug	Station [mac:%m], [ip:%s]: MIP message: Registration Revocation received from agent [agt:%pI4]	NA	
500500	Debug	Station [mac:%m], [ip:%s]: MIP message: Registration Revocation ACK received from [sw:%pI4]	NA	
500504	Debug	Station [mac:%m], [vlan:%d], [ip:%s]: Started ha discovery in datapath	Mobility started ha discovery in datapath	
500505	Debug	Station [mac:%m]: Received ha discovery NACK from datapath	Received ha discovery NACK from datapath	
500506	Debug	Station [mac:%m] HA [ip:%s]: Received ha discovery ACK from datapath	Received ha discovery ACK from datapath	
500509	Debug	HAT bulk download response received with [entries:%d] entries	Mobility failed to add Hat entry in bulk	
500511	Debug	Station [mac:%m], [ip:%pI4]: Received [typ:%s] on ESSID: [ess:%s] Mobility service [ms:%s], HA Discovery on Association [ha_disc:%s], Fastroaming [frs:%s], AP: Name [ap:%s] Group [apgrp:%s] BSSID [bss:%m], phy [ph:%s], VLAN [vl:%d] V6-VLAN [v6_vlan:%d]	NA	
500512	Debug	Downloading HAT to datapath	Downloading HAT to datapath	
500513	Debug	HAT download to datapath failed	HAT download to datapath failed	
500514	Debug	Could not download HAT to datapath	Could not download HAT to datapath	

500515	Debug	Failed to create tunnel: [local:%pI4] to [remote:%pI4] [id:%d]	Failed to create tunnel	
500516	Debug	Could not tunnel: [local:%pI4] to [remote:%pI4]	Could not find tunnel	
500517	Debug	Registration has different ip: [rrpip:%pI4] [proxyip:%pI4]	Could not find tunnel	
500520	Debug	Station [mac:%m] : Station Update with mobility data bssid [bssid:%m], home vlan:[home_vlan:%d], Mobility GRE Tunnel:[lkup_tun_id:%x], action [action:%s] [dbg_str:%s]	Updating (add/del) Station entry with Mobility info - home-vlan and gre-tunnel	
500526	Debug	Vrrp [vr:%pI4] configured, Delete dynamic tunnel [tun:%pI4]	Delete dynamic tunnel	
500527	Debug	Vrrp [vr:%pI4] configured, Delete HAT tunnel [tun:%pI4]	Delete Hat tunnel	
500528	Debug	Visitor [mac:%s] [ip:%s] Status [s:%d] early terminated. Tunnel: [src:%s] to [dst:%s] ref count [r:%d]	Visitor early terminated	
500529	Debug	Station [mac:%m], [vlan:%d], [ip:%s]: Started ha discovery in [path:%s]	Mobility started ha discovery in datapath / controler plane	
500530	Debug	Station [mac:%m]: ha discovery returned error [err:%d]	ha discovery returned error	
500531	Debug	Station [mac:%m]: GSM: cha mip_proxy :[act:%s] [sta:%d]		
500532	Debug	GSM: cha mip_tunnel [ip:%s] :[act:%s]		
500990	Debug	Station [mac:%m], [ip:%s]: proxy mobile node deleted code [dc:%x] reason [r_str:%s]	Mobile IP Proxy State Machine debugging	
501000	Debug	Station [mac:%m]: Clearing state	NA	
501042	Debug	Station [sta:%m]: DA [da:%m] not found trying to de-authenticate to BSSID [bss:%m] on AP [name:%s]		
501050	Debug	Station [sta:%m]: No bssid found for management frame type [type:%d], subtype [stype:%d] to BSSID [bss:%m]		
501052	Debug	Station [sta:%m]: Dropping management frame type [type:%d], subtype [stype:%d], bss [bss:%m]		
501065	Debug	[msg:%s]		
501066	Debug	Source: [sa:%m] Failed AP [ip:%P]-[bssid:%m]-[name:%s] SSID Mismatch		
501082	Debug	Probe request: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s]		
501085	Debug	Probe request: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] SSID [essid:%s]		
501090	Debug	Probe response: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] SSID [essid:%s]		
501140	Debug	Denylist client added from db: [mac:%m]. Reason: [reason:%s]	This log indicates that a client denylist entry was added from the database at startup.	
501142	Debug	Derive user vlan: [mac:%m] Derive user Vlan [vlan:%d] from [reason:%s]	This log indicates that user vlan derivation information .	
501143	Debug	Derive user vlan: [mac:%m] Can't derive user Vlan from [vlan1:%d] to [vlan2:%d] through [reason:%s]	This log indicates that user vlan derivation error information .	
501144	Debug	stm_user_dhcp_role_msg: [reason:%s]	This log indicates dhcp role debug information .	
501145	Debug	DHCP option signature: DHCP option [option:%d] signature [reason:%s]	This log indicates dhcp option signature information .	
501146	Debug	Derive user role: [mac:%m] Match user role [role:%s] acl [acl:%d] rule_index [index:%x]	This log indicates that matched user role information.	
501147	Debug	Update user role: [mac:%m] Update user role [role:%d] rule_index [index:%x] from conductor msg	This log indicates that update user role information from conductor.	
501148	Debug	Receive portal auth acl: [mac:%m] ip str [ip:%s] port [port:%s] essid [essid:%s] user [usr:%s]	This log indicates that we received portal auth acl msg from cli0.	
501149	Debug	Send radius auth info: authtime [time:%s] timeouts [to:%u], authdone [true:%u]	This log indicates that we are sending radius auth info to cli0.	
501150	Debug	Derive user role: [mac:%m] Derive user role [role:%s] acl [acl:%d] rule_index [index:%x]	This log indicates that derive user role information.	
501151	Debug	user-agent signature: signature [reason:%s]	This log indicates user-agent signature information .	
501152	Debug	Dot1x-auth-type signature: signature [reason:%s]	This log indicates dot1x-auth-type signature information .	
501157	Debug	Station [sta:%m]: Unexpected SA-Query Response bss [bss:%m]		
501158	Debug	Station [sta:%m]: SA-Query Request from non-MFP STA to bss [bss:%m]		
501160	Debug	[msg:%s]		
501161	Debug	Client Match Received probe report: AP [ap:%s] ESSID [essid:%s] Assoc ESSID [a_essid:%s] for client [mac:%s] with signal -[sig:%d]		
501162	Debug	Client Match: Unsteerable STA [mac:%m] consec_fails [fails:%d], giving up		

501163	Debug	Client Match: Adding new unsteerable client [mac:%m] reason 0x[reason:%x]		
501164	Debug	Client Match: Found 11v Capable STA [mac:%m]		
501165	Debug	Client Match: Skip steer for client [mac:%m], Assoc SAP [assoc_sap:%m] not found in VBR		
501166	Debug	Client Match: Skip steer for client [mac:%m] from [src_ap:%m] to [dst_ap:%m], Stale entry for dst or src: Src [sts:%ld] dst [dst_ts:%ld] now [now:%ld]		
501167	Debug	Client Match: Denylist STA [mac:%m] on AP [ap:%s] [bss:%m] Reason [reason:%s] Timeout [timeout:%d]		
501168	Debug	Client Match: Invalid trigger from AP [ap:%m] for client [client:%m] - [reason:%s]		
501169	Debug	Client Match: Client trigger [reason:%s] for client [client:%m] from AP [name:%s] [bss:%m] to AP [d_name:%s] [d_bss:%m]		
501170	Debug	Client Match: LoadBal Band mismatch Skipping match for Client [mac:%m] Dest AP [name:%s] [bss:%m]		
501171	Debug	Client Match: LoadBal Found match for Client [mac:%m] Dest AP [name:%s] [bss:%m] signal -[signal:%d] snr thresh [thresh:%d]		
501172	Debug	Client Match: LoadBal Not found match for Client [mac:%m] Dest AP [name:%s] [bss:%m] signal -[signal:%d] snr thresh [thresh:%d]		
501173	Debug	Client Match: LoadBal Adding pot sta [mac:%m] for move from AP [name:%s] [bss:%m] Current SNR [snr:%d]		
501174	Debug	Client Match: Deleting BSS [bss:%m] from client [mac:%m] AP may be down or AM		
501175	Debug	Client Match: Deleting STA [mac:%m] from VBR table		
501176	Debug	Client Match: For client [mac:%m] Not found SAP [bss:%m]		
501177	Debug	Client Match: For client [mac:%m] No weaker AP found, ignoring new AP %s [bss:%m]		
501178	Debug	Client Match: Client [mac:%m] Adding AP [bss:%m] by replacing weakest AP idx [idx:%d] [w_bss:%m]		
501179	Debug	Client Match: Client [mac:%m] Adding AP [name:%s] [bss:%m] at idx [idx:%d]		
501180	Debug	Client Match: Unknown Assoc AP: skipping update from AP [name:%s] [bss:%m] for client [mac:%m]		
501181	Debug	Client Match: Mismatched ESSID: skipping update from AP [name:%s] [bss:%m] ESSID [essid:%s] Assoc ESSID [a_essid:%s] for client [mac:%m]		
501182	Debug	Client Match: Denylist STA [mac:%m] on AP [bss:%m] Timeout [timeout:%d] Mode [mode:%d]		
501183	Debug	Client Match: Deauth STA [mac:%m] on AP [bss:%m]		
501184	Debug	Client Match: Successful move for client [mac:%m] Source AP [s_name:%s] [s_bss:%m] Signal [s_sig:%d] to Target AP [name:%s] [bss:%m] Signal [t_sig:%d] Time diff [diff:%d] Reason [rsn:%s]		
501185	Debug	Client Match: Unsuccessful move for client [mac:%m] from Source AP [s_name:%s] [s_bss:%m] Signal [s_sig:%d] to Target AP [name:%s] [bss:%m] Signal [t_sig:%d] Actual AP [a_name:%s] [a_bss:%m] Time diff [diff:%d] Reason [rsn:%s]		
501186	Debug	Client Match: Tracking unsuccessful failure for client [mac:%m] num fails [numfails: %d]		
501187	Debug	Client Match: Skip stale entry [mac:%m] for client [cl:%m]		
501188	Debug	Client Match: Replacing stale entry [mac:%m] for client [cl:%m] at index [idx:%d] signal -[sig:%d] dBm		
501192	Debug	Client Match: Potentially unsteerable STA [mac:%m] [device_type:%s], throttling steers	Client Match rate limits steering when detecting devices that have trouble with receiving multiple deauths	
501193	Debug	Client Match: Clearing potentially unsteerable client [mac:%m]		
501194	Debug	Derive user role from dhcp-option(applied): [mac:%m] Match user role [role:%s] acl [acl:%d] rule_index [index:%x]	This log indicates that matched user role information using dhcp-option.	
501195	Debug	Update dhcp-opt: [mac:%m] Update dhcp-opt [vlan:%d] [vlanhow:%s] [role:%s] rule_index [index:%x] essid [essid:%s] from conductor msg	This log indicates that update user dhcp-opt information from conductor.	

501196	Debug	Update dhcp-opt: [mac:%m] Update dhcp-opt [vlan:%d] [vlanhow:%s] [role:%s] rule_index [index:%x] essid [essid:%s] to cli0 msg	This log indicates that update user dhcp-opt information to cli.	
501197	Debug	Send user role info: mac-[mac:%m], acl-[acl:%d], idx-[idx:%d], essid-[essid:%s]	This log indicates that we are sending user role info to cli0.	
501198	Debug	Receive disconnect user, mac-[mac:%m], bssid-[bssid:%m], logout-[logout:%d], deauth-[deauth:%d], term-[trem:%d]	This log indicates that we are receiving disconnect user msg from cli0.	
501200	Debug	Rap bridge user msg, flags-[flags:%d] action-[action:%d] aclnum-[aclnum:%d] ip-[ip:%pI4] mac-[mac:%m],bssid-[bssid:%m] vlan-[vlan:%d] wired-[wired:%d]	This log indicates that stm received ASAP_STM_BRIDGE_USER message	
501202	Debug	Receive user acct req, mac-[mac:%m], bssid-[bssid:%m], acctreq-[acctreq:%d], term-[trem:%d]	This log indicates that we are receiving user acct req msg from cli0.	
501203	Debug	Receive user accounting info: mac-[mac:%m], status-[status:%d], inocts-[inocts:%d], giginocts-[giginocts:%d], outocts-[outocts:%d], gigoutocts-[gigoutocts:%d], inpkts-[inpkts:%d], outpkts-[outpkts:%d], sesstim-[sesstim:%d], sessid-[sessid:%s], multisessid-[multisessid:%s], cpradip-[cpradip:%s]	This log indicates that we are sending user acct info to cli0.	
501204	Debug	Send user accounting info: mac-[mac:%m], status-[status:%d], inocts-[inocts:%d], giginocts-[giginocts:%d], outocts-[outocts:%d], gigoutocts-[gigoutocts:%d], inpkts-[inpkts:%d], outpkts-[outpkts:%d], sesstim-[sesstim:%d], sessid-[sessid:%s], multisessid-[multisessid:%s], cpradip-[cpradip:%s]	This log indicates that we are sending user acct info to cli0.	
501205	Debug	Client Match: Initialize bandsteer window for [mac:%m] Radio [rad:%m] Start time [st:%ld] End Time [end:%ld]		
501206	Debug	Client Match: Update bandsteer window for [mac:%m] Radio [rad:%m] Start time [start:%ld] End time [end:%ld] Now [now:%ld] Num steers [st:%d]		
501207	Debug	Client Match: Pausing bandsteer for [mac:%m] Radio [rad:%m] Start time [start:%ld] End time [end:%ld] Now [now:%ld] Num steers [st:%d]		
501208	Debug	Client Match: Reset bandsteer window for [mac:%m] Radio [rad:%m] Start time [start:%ld] End time [end:%ld] Now [now:%ld] Num steers [st:%d]		
501212	Debug	AP sent old style Assoc request for Station [sta:%m]: bss [bss:%m]		
501213	Debug	Client Match: Skip steer for client [mac:%m] from [src_ap:%m] to [dst_ap:%m], mismatched essids: src [s_essid:%s] dst [d_essid:%s]		
501214	Debug	[func: %s]: ppsk response for client [mac:%m], [ppsk:%s]	This log indicates that we are receiving client ppsk response.	
501215	Debug	[func: %s]: send ppsk req for client [mac:%m]	This log indicates that we are sending client ppsk request.	
501219	Debug	Malloc error for [sta:%m]: bss [bss:%m]		
501221	Debug	[func: %s]: received set sta_os_type messsage for [mac:%m] [os:%s]		
501222	Debug	[func: %s]: set sta [mac:%m] os_type to [os:%s]		
502200	Debug	IGMP station [mac:%m] associated with VLAN [vlan:%d] and dest [dest:%x]	NA	
502201	Debug	Received IGMP [version:%d] REPORT from user [ip:%pI4] for group [group:%pI4]	NA	
502202	Debug	Received IGMP LEAVE from user [ip:%pI4] for group [group:%pI4]	NA	
502203	Debug	Adding User mac [mac:%m] ip [ip:%s] Opcode [opc:%d] Action [act:%d] L2 check enforced [l2chk:%d]	NA	
502204	Debug	Deleting User mac [mac:%m] ip [ip:%s] Opcode [opc:%d] Action [act:%d]	NA	
502205	Debug	User mac [mac:%m] ip [ip:%s] Opcode [opc:%d] Action [act:%d] transaction status failed	L2 or L3 User entry add/del failed, Please check if Layer 3 interface IP/subnet conflicts with IKE local pool or S2S map etc	
502900	Debug	Sending user event change message to auth for user [user:%s]		
506000	Debug	[User-Agent] [type:%s]-[[macstr:%s]/[ipstr:%s]]-"[uastr:%s]..." ==> [num:%d] CPPM Server(s)	This shows an internal debug message	
506001	Debug	[mDNS-Info] [[macstr:%s]]-"[info:%s]..." ==> [num:%d] CPPM Server(s)	This shows an internal debug message	
506100	Debug	[User-ID] [type:%s]-[[macstr:%s]/[ipstr:%s]]-[user:%s]([devid:%s]) ==> [num:%d] PAN Server(s)	This indicates successfully renew session to a PAN server.	

506200	Debug	Device-Profile received from ClearPass, mac [mac:%s] device-name:'[name:%s]' upd-timestamp:[ts:%u] CONVERT TO dev-id:[type:%s]([id:%d]) os-version:[osname:%s]([osid:%d])	This indicates Device-Profile for a station is received from ClearPass NetWatch.	
506201	Debug	Successfully update cppm section for mac [mac:%s] dev-id:[type:%s]([id:%d]) os-version:[osname:%s]([osid:%d]) device-name:'[name:%s]' upd-timestamp:[ts:%u]	This indicates Device-Profile for a station is received from ClearPass NetWatch.	
506202	Debug	Failed to update cppm section for mac [mac:%s], reason:[reason:%s]	This indicates Device-Profile for a station is received from ClearPass NetWatch.	
506902	Debug	[func:%s](MAC/IP=[macstr:%s]/[ipstr:%s]): delivers to MAPC successfully.	This indicates request is delivered to MAPC successfully	
506903	Debug	[func:%s](MAC/IP=[macstr:%s]/[ipstr:%s]): Skip the request due to CPPM is inactive.	This indicates request is not delivered to MAPC	
506906	Debug	[func:%s](MAC=[macstr:%s]): delivers to MAPC successfully.	This indicates request is delivered to MAPC successfully	
506907	Debug	[func:%s](MAC=[macstr:%s]): Skip the request due to CPPM is inactive.	This indicates request is not delivered to MAPC	
507002	Debug	[msg:%s]		
507003	Debug	Client Match: No other radio		
507004	Debug	Client Match: Other radio [bss:%m] not strong enough: Min Signal -[ms:%d] dBm Sticky thresh [st:%d] dB, cur signal [cs:%d] new signal [ns:%d] (-dBm)		
507005	Debug	Client Match: Found 5G radio [bss:%m] with signal -[sig:%d] dBm		
507006	Debug	Client Match: No other radio or other radio not much stronger cur signal [sig:%d] other signal [o_sig:%d] (-dBm)		
507007	Debug	Client Match: For client [mac:%m] Trigger [tr:%s] No better candidate AP		
507008	Debug	Client Match: For client [mac:%m] Trigger [tr:%s] Better candidate [bss:%m] with Eff_Signal -[e_sig:%d] dBm (signal -[sig:%d] dBm EIRP [pwr:%s] dBm) Channel [ch:%d] Current Eff_Signal -[e_cs:%d] dBm (Signal -[cs:%d] dBm, Current EIRP [cp:%s] dBm)		
507009	Debug	Client Match: For client [mac:%m] No steering 5G in DFS non-occupancy		
507010	Debug	Client Match: For client [mac:%m] No steering Single radio AP		
507011	Debug	Client Match: For client [mac:%m] No steering Band Balance A Clients [a_cl:%d] G Clients [g_cl:%d]		
507012	Debug	Client Match: Unsteerable client [mac:%m] Reason [rsn:%s]		
507013	Debug	Client Match: Detected client [mac:%m] Assoc BSSID [bss:%m] channel [ch:%d] with low RSSI [rssi:%d] dB		
507014	Debug	Client Match: End of steer backoff for client [mac:%m] now [now:%d] last moved [moved:%d]		
507015	Debug	Client Match: Active voice client, defer client match steer [mac:%m]		
507016	Debug	Client Match: Skip [reason:%s] move, missing assoc BSS in VBR for client [mac:%m]		
507017	Debug	Client Match: New assoc backoff, defer steering [sta:%m] now [now:%d] assoc_ts [ats:%d]		
507018	Debug	Client Match: New assoc [client:%m] Assoc time [atime:%d]		
507019	Debug	Client Match: VBR Client [client:%m] Assoc AP [assoc_bss:%m] Candidate AP [cnt:%d] [bss:%m] Signal -[sig:%d] dBm, EIRP [pwr:%s] dBm, Trigger [tr:%s]		
507020	Debug	Client Match: Steer backoff for client [client:%m] Last steer [moved:%d] Now [now:%d] backoff end [end:%d]		
507021	Debug	Client Match: Active voice client [client:%m] Roam to Target Radio [mac:%m] Signal -[sig:%d] dBm Required Sig -[reqsig:%d]		
507022	Debug	Client Match: Active voice client [client:%m] No roam Target Radio [mac:%m] Signal -[sig:%d] dBm Required Sig -[reqsig:%d]		
508050	Debug	Station [sta:%m]: No bssid found for management frame type [type:%d], subtype [stype:%d] to BSSID [bss:%m]		
508065	Debug	[msg:%s]		
508161	Debug	Client Match Received probe report: AP [ap:%s] ESSID [essid:%s] Assoc ESSID [a_essid:%s] for client [mac:%s] with signal -[sig:%d]		
508162	Debug	Client Match: Unsteerable STA [mac:%m] consec_fails [fails:%d], giving up		

508163	Debug	Client Match: Adding new unsteerable client [mac:%m] reason 0x [reason:%x]		
508164	Debug	Client Match: Found 11v Capable STA [mac:%m]		
508165	Debug	Client Match: Skip steer for client [mac:%m], Assoc SAP [assoc_sap:%m] not found in VBR		
508166	Debug	Client Match: Skip steer for client [mac:%m] from [src_ap:%m] to [dst_ap:%m], Stale entry for dst or src: Src [sts:%ld] dst [dst_ts:%ld] now [now:%ld]		
508167	Debug	Client Match: Block STA [mac:%m] on AP [ap:%s] [bss:%m] Reason [reason:%s] Timeout [timeout:%d]		
508168	Debug	Client Match: Invalid trigger from AP [ap:%m] for client [client:%m] - [reason:%s]		
508169	Debug	Client Match: Client trigger [reason:%s] for client [client:%m] from AP [name:%s] [bss:%m] to AP [d_name:%s] [d_bss:%m]		
508174	Debug	Client Match: Deleting BSS [bss:%m] from client [mac:%m] AP may be down or AM		
508175	Debug	Client Match: Deleting STA [mac:%m] from VBR table		
508176	Debug	Client Match: Could not found [reason:%s] SAP for client [mac:%m] in [func:%s] [line:%d]		
508177	Debug	Client Match: For client [mac:%m] No weaker AP found, ignoring new AP %s [bss:%m]		
508178	Debug	Client Match: Client [mac:%m] Adding AP [bss:%m] by replacing weakest AP idx [idx:%d] [w_bss:%m]		
508179	Debug	Client Match: Client [mac:%m] Adding AP [name:%s] [bss:%m] at idx [idx:%d]		
508180	Debug	Client Match: Unknown Assoc AP: skipping update from AP [name:%s] [bss:%m] for client [mac:%m]		
508181	Debug	Client Match: Mismatched ESSID: skipping update from AP [name:%s] [bss:%m] ESSID [essid:%s] Assoc ESSID [a_essid:%s] for client [mac:%m]		
508182	Debug	Client Match: Block STA [mac:%m] on AP [bss:%m] Timeout [timeout:%d] Mode [mode:%d]		
508185	Debug	Client Match: move status: [status:%s] complete move for client [mac:%m] from Source AP [s_name:%s] [s_bss:%m] Eff_Signal -[s_esig:%d] dBm (Signal -[s_sig:%d] dBm EIRP [s_pwr:%s] dBm) to Target AP [name:%s] [bss:%m] Eff_Signal -[t_esig:%d] dBm (Signal -[t_sig:%d] dBm EIRP [t_pwr:%s] dBm) Assoc Sig: -[a_sig:%d] dBm Actual AP [a_name:%s] [a_bss:%m] Time diff [diff:%d] Reason [rsn:%s]	Client Match move complete event	
508186	Debug	Client Match: Tracking unsuccessful failure for client [mac:%m] num fails [num_d_fails: %d] btm rejects [br: %d] btm timeouts [bt: %d]		
508187	Debug	Client Match: Skip stale entry [mac:%m] for client [cl:%m]		
508188	Debug	Client Match: Replacing BSS entry [mac:%m] for client [cl:%m] at index [idx:%d] signal -[sig:%d] dBm, [reason:%s]		
508192	Debug	Client Match: Potentially unsteerable STA [mac:%m] [device_type:%s], throttling steers	Client Match rate limits steering when detecting devices that have trouble with receiving multiple deauths	
508193	Debug	Client Match: Clearing [reason:%s] potentially unsteerable client [mac:%m]		
508194	Debug	Client Match: Initialize bandsteer window for [mac:%m] Radio [rad:%m] Start time [st:%ld] End Time [end:%ld]		
508195	Debug	Client Match: Update bandsteer window for [mac:%m] Radio [rad:%m] Start time [start:%ld] End time [end:%ld] Now [now:%ld] Num steers [st:%d]		
508196	Debug	Client Match: Pausing bandsteer for [mac:%m] Radio [rad:%m] Start time [start:%ld] End time [end:%ld] Now [now:%ld] Num steers [st:%d]		
508197	Debug	Client Match: Reset bandsteer window for [mac:%m] Radio [rad:%m] Start time [start:%ld] End time [end:%ld] Now [now:%ld] Num steers [st:%d]		
508198	Debug	Client Match: VBR Client [mac:%m] Assoc AP [assoc_bss:%m] Candidate AP [cnt:%d] [rad:%m] Signal -[sig:%d] dBm EIRP [pwr:%s] dBm, Trigger Load Balance		
508199	Debug	Client Match: Skip steer for client [mac:%m] from [src_ap:%m] to [dst_ap:%m], mismatched essids: src [s_essid:%s] dst [d_essid:%s]		

508200	Debug	Client Match: Recd BSS transition rsp from client [mac:%m] Status [rs:%s] Token [dtoken:%d]		
508201	Debug	Client Match: Sending BSS transition req to client [mac:%m] token [dtoken:%d]		
508202	Debug	Client Match: Timer started for BTM response STA [mac:%m] timerid [tid:%ld]		
508203	Debug	Client Match: Timer cleared for BTM response STA [mac:%m] timerid [tid:%ld]		
508204	Debug	Client Match: 11v BTM Response timeouts exceeded for sta [mac:%m], falling back to deauth based steers		
508206	Debug	Client Match: For client [mac:%m] VBR list is full, ignoring new AP %s [bss:%m] on unsupported channel [ch:%d]		
508207	Debug	Client Match: Replacing entry [mac:%m] on unsupported channel [ch:%d] for client [cl:%m] at index [idx:%d] signal -[sig:%d] dBm		
508208	Debug	Client Match: 11v BTM Response timeouts exceeded for Active Voice sta [mac:%m], continue to use BTM		
508209	Debug	Client Match: Potentially unsteerable STA [mac:%m] [device_type:%s], throttling 11v BTM steers	Client Match rate limits dot11v steering when detecting devices that reject BTM request with status code 1 (Reject-Unspecified)	
508210	Debug	Client Match: VBR record for client [mac:%m] not found		
508211	Debug	Client Match: Stat entry for client [mac:%m] not found		
508212	Debug	Client Match: Adding client [mac:%m] into VBR list, Num cl [num:%d]		
508213	Debug	Client Match: Replace the oldest arm unsteerable client entry for [old_mac:%m] with the new arm unsteerable client entry for [mac:%m]		
508214	Debug	Client Match: Unsteerable STA [mac:%m] band steer rate limiting		
508215	Debug	Client Match: Could not find [reason:%s] radio [bss:%m] for client [mac:%m] in [func:%s] [line:%d]		
508216	Debug	Client Match: Could not find client [mac:%m] in [func:%s] [line:%d]		
508217	Debug	Client Match: Could not find radio [bss:%m] in client [mac:%m] VBR list Index [num:%d] (ch [ch:%d], sig [sig:%d], pkt_time [time:%s])		
508218	Debug	Client Match: Could not find radio for SAP [bss:%m] in [func:%s] [line:%d]		
508219	Debug	Client Match: Skip CHA steer since cellular HA disabled on VAP [bss:%m] Cl [cl:%m]		
508220	Debug	Client Match: Updating estimated throughput for client [cl:%m] snr [snr:%d] max_neg_rate [mr:%d] est_tput [et:%d]		
508221	Debug	Client Match: Skip steer for client [mac:%m] from [src_ap:%m] to [dst_ap:%m]. Client is a dot11v-capable IOS device marked unsteerable due to BTM Reject.	Client Match limits steering for a short interval, for IOS devices that rejected a BTM request with Reject-Unspecified	
508222	Debug	Client Match: Skip steer for MBO capable client [mac:%m] from [src_ap:%m] to [dst_ap:%m] on non pref chan [chan:%d]	Client Match avoids steering MBO capable STA that have advertized a non-preferred channel list to radios that are operating on one of these non-preferred primary channels	
509007	Debug	FIPS Debug: [function:%s], [file:%s]:[line:%d]: [msg:%s]	This is a FIPS debugging log in user module.	
520001	Debug	[[file:%s]:[line:%d]] [message:%s]	aaa module's debug message	
520004	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] sending acct req tput=[tput:%d] discard=[discard:%d] reest=[reest:%d] keepalive=[keepalive:%d]		
520005	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] tput=[tput:%d] discard=[discard:%d] reest=[reest:%d] keepalive=[keepalive:%d], starting short timer period=[period:%d]		
520006	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] tput=[tput:%d] discard=[discard:%d] reest=[reest:%d] keepalive=[keepalive:%d], starting long timer period=[period:%d]		
520007	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] timer for acct req NOT set due to invalid values: enabled=[enabled:%d] reest=[reest:%d] keepalive=[keepalive:%d]		
520008	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] timer for acct already running		
520009	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] enabled=[enabled:%d] tput=[tput:%d] discard=[discard:%d] reest=[reest:%d]		
520011	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] Added VSA for throughput [tput:%d]		
520012	Debug	[msg:%s]	This shows an internal clarity auth debug log	

520015	Debug	[func:%s] ([line:%u]): acct-start user-[user:%m] server-[server:%s] timestamp-[sec:%u]-[usec:%u]	log for start accounting for client	
522000	Debug	Unable to perform ESI action on user '[user:%s]': User not found	Auth received a user denylist/role change request from ESI, but was unable to lookup the user to perform the action on. The request is ignored.	
522001	Debug	Unable to derive user '[user:%s]' to role '[role:%s]': Role not found	Auth received a user role change request from ESI or COA, but was unable to find the role to move the user to. The request is ignored.	
522002	Debug	[func:%s]: Ignored the DHCP Fingerprint UDR for the user [mac:%s]	This shows an internal debug message	
522003	Debug	Received Changing user '[user:%s]' to role '[role:%s]'	Auth received an ESI request to move the user to a new role.	
522004	Debug	[string:%s]	This shows an internal debug message	
522011	Debug	MAC=[mac:%s] IP=[ip:%s] User idle timeout ignored: reason=[r:%s]	User idle timeout was ignored due to specified reason	
522014	Debug	MAC=[mac:%s] IP=[ip:%s] Notify IKE (IP DN): outerIP=[ip2:%s] Reason=[r:%d]	Send IP DN	
522048	Debug	AP-Group is present in the Radius server for username=[user:%s]	If ap-group is set in Radius server the AP will take it; else AP will take ap-group as provisioned	
522053	Debug	PMK Cache getting updated for [mac:%s], (def, cur, vhow) = ([def:%d], [cur:%d], [vhow:%d]) with vlan=[vlan:%d] vlanhow=[how:%d] essid=[essid:%s] role=[role:%s] rhow=[rhow:%d]	PMK cached info for the user getting added/updated	
522054	Debug	[_funtion_:%s]:user [mac:%s] might have switched to NON-bridge port user->fw_mode =[fw_mode:%d],so will drop this	This shows an internal user debug message	
522055	Debug	AP-Bridge-Wired user ([mac:%s]) from AP : [apip:%s] exists, continue to updating	This shows an internal user debug message	
522056	Debug	Removing existing AP-Bridge-Wired user MAC:[mac:%s] IP:[ip:%s] on AP: [apname:%s] Wired port:[port_str:%s]	This shows an internal user debug message	
522057	Debug	adding AP-Bridge-Wired station ([mac:%s])	This shows an internal user debug message	
522058	Debug	failed to add AP-Bridge-Wired station ([mac:%s])	This shows an internal user debug message	
522059	Debug	AP-Bridge-Wireless station ([mac:%s],[bssid:%s]) not found, skipping update (no operation)	This shows an internal user debug message	
522060	Debug	AP-Bridge station ([mac:%s]) invalid ACL num:[aclnum:%d]	This shows an internal user debug message	
522061	Debug	AP-Bridge-Wired User: mac:[mac:%s] dot1x-enabled:[dot1x:%d]	This shows an internal user debug message	
522062	Debug	Adding AP-Bridge-Wired User [mac:%s] to STM stats tree	This shows an internal user debug message	
522063	Debug	AP-Bridge-Wireless User: mac:[mac:%s] dot1x:[dot1x:%d], keytype:[keytype:%d]([encr_alg:%s])	This shows an internal user debug message	
522064	Debug	AP-Bridge station: mac:[mac:%s] DeviceType Classification is set in aaa-profile	This shows an internal user debug message	
522065	Debug	AP-Bridge station: mac:[mac:%s] DeviceType from cache: [devid_cache_str:%s]	This shows an internal user debug message	
522066	Debug	AP-Bridge-[type:%s] User: Updating current role from [l2role:%s]/[l3role:%s] to [role:%s]/NULL for user [mac:%s]	This shows an internal user debug message	
522068	Debug	Deleting AP-Bridge-[type:%s] User: mac:[mac:%s] IP:[ip:%s] apip:[apip:%s]	This shows an internal user debug message	
522069	Debug	AP-Bridge-[type:%s] User: mac:[mac:%s] IP:[userip:%s] (not station) for apip:[apip:%s] is Removed	This shows an internal user debug message	
522070	Debug	AP-Bridge-Wired station: Removing mac:([mac:%s])	This shows an internal user debug message	
522071	Debug	AP-Bridge user: station ([mac:%s]) not found, no-operation	This shows an internal user debug message	
522072	Debug	No user to cleanup	This shows an internal user debug message	
522073	Debug	user has not changed essid, skipping cleanup	This shows an internal user debug message	
522074	Debug	Skipping deletion of L3 entries, no change in ap/port-ingress/fw_mode	This shows an internal user debug message	
522075	Debug	removing existing L2 station ([mac:%s]) associated to AP:[apname:%s],user->apip:[userapip:%s]([apip:%s]),[port_str:%s], user->fw->mode : [user_fw_mode:%d] ([fw_mode:%d])	This shows an internal user debug message	
522076	Debug	MAC=[mac:%s] ingress [ingres:%x] ([usr_dest:%s]), u_encr [u_encr:%d], m_encr [m_encr:%d], slotport [slot:%x] [port:%s], type: [type:%s], FW mode: [fw_mode:%u], AP IP: [apip:%s] is invalid	This shows an internal user debug message	
522077	Debug	MAC=[mac:%s] ingress [ingres:%x] ([usr_dest:%s]), u_encr [u_encr:%x], m_encr [m_encr:%x], slotport [slot:%x] [port:%s], type: [type:%s], FW mode: [fw_mode:%u], AP IP: [apip:%s] mdie [mdie:%d] ft_complete [ft_complete:%d]	This shows an internal user debug message	

522078	Debug	MAC=[mac:%s], wired: [wired:%d], vlan:[vlan:%d] ingress:[ingess:%x] ([dst:%s]), ingress:[ingress:%x] new_aaa_prof: [aaa_prof:%s], stored profile: [stored_prof:%s] stored wired: [stored_wired:%d] stored essid: [stored_essid:%s], stored-ingress: [stored_ingress:%x]	This shows an internal user debug message	
522079	Debug	MAC=[mac:%s] (vlan:[vlan:%d]) Detecting [wuser:%s] AAA-Profile mismatch [extra:%s]	This shows an internal user debug message	
522080	Debug	MAC=[mac:%s], detected a wired to wireless move ESSID [essid:%s]	This shows an internal user debug message	
522081	Debug	MAC=[mac:%s], VLAN:[vlan:%d] - Anchor(VLAN:[user_vlan:%d]) exists. Do nothing for wired Non-clubbed User	This shows an internal user debug message	
522083	Debug	Skip User-Derivation, mba:[mba:%d] udr_exist:[user:%d],default_role:[default_role:%s],pDefRole:0x[pDefRole:%p]	This shows an internal user debug message	
522084	Debug	MAC=[mac:%s], no user_download on FA	This shows an internal user debug message	
522085	Debug	Validate client ip[ip: %s] mac [mac:%s] user [resp:%d] apname [apname:%s]	This shows an internal user debug message	
522086	Debug	Cannot find a user with mac [mac:%s]	This shows an internal user debug message	
522087	Debug	Cannot get user role for user with mac [mac:%s]	This shows an internal user debug message	
522088	Debug	(mac,"mac([mac:%s]), role([role_name:%s])	This shows an internal user debug message	
522089	Debug	Cannot create dynamic ACE for ip([ip:%s]), role([role_name:%s]). Capacity reached	This shows an internal user debug message	
522090	Debug	Dynamic H323 ACL for [ip:%s]:[port:%d] already present in role [name:%s]	This shows an internal user debug message	
522091	Debug	adding h323 service and policy for port [port:%d]	This shows an internal user debug message	
522092	Debug	mac([mac:%s]), acl([acl_name:%s]) present in role([name:%s])	This shows an internal user debug message	
522093	Debug	mac([mac:%s]), ADD acl([acl_name:%s]) to role([name:%s])	This shows an internal user debug message	
522094	Debug	[mac:%s]: Sending STM station data-ready: AP [bssid:%s]	This shows an internal user debug message	
522095	Debug	[mac:%s]: Sending STM new vlan info: vlan [vlan:%d], AP [bssid:%s] caller [callfunc:%s]	This shows an internal user debug message	
522096	Debug	[mac:%s]: Sending STM new Role ACL : [acl:%d], and Vlan info: [vlan:%d] on [ipaddr:%s], action : [action:%d], AP IP: [apip:%s], flags : [flags:%d] idle-timeout: [idle_tmo:%d]	This shows an internal user debug message	
522097	Debug	Communication error occurred between Auth and AP:[apip:%s] (AP stm), ip:[ipuser:%s], mac:[mac:%s], acl:[acl:%d], vlan:[vlan:%d], action:[action:%d], flags:[flags:%d]	This shows an internal user debug message	
522098	Debug	[_function_:%s]: clearing bridge entries for MAC [mac:%s]	This shows an internal user debug message	
522099	Debug	Profile not found for [userip:%s]	This shows an internal user debug message	
522100	Debug	No user attached to station [mac:%s] ip [userip:%s]	This shows an internal user debug message	
522101	Debug	User [userip:%s] not found	This shows an internal user debug message	
522102	Debug	Missing CP profile for [userip:%s]	This shows an internal user debug message	
522107	Debug	SAP lookup failed for MAC=[mac:%s] in dot1x station down	This shows an internal debug message	
522108	Debug	SAP lookup failed for MAC=[mac:%s] during lookup for UDR	This shows an internal debug message	
522109	Debug	mobility: port=[port:%x] ([portstr:%s]), flags=[flags:%x], apname=[apname:%s].	This shows an internal debug message	
522110	Debug	Adding AP Wired User (mobility) (tunnel) [mac:%s] to STM stats tree.	This shows an internal debug message	
522111	Debug	AU[authenticated:%d]([authtype:%d]), HA[homeagent:%d], TAP[trustedAP:%d], PARP[proxyarp:%d] OIP[oip:%d] IIP[iip:%d] INT[internal:%d] WD[wired:%d] FW[fwMode:%d] DT[destTunnel:%d].	This shows an internal debug message	
522112	Debug	Mark rap users for ageout, Reason - AP down.	This shows an internal debug message	
522113	Debug	Deleting AP Wired User (tunnel) [mac:%s]/[ipstr:%s] from STM stats tree.	This shows an internal debug message	
522114	Debug	Delete [updownstream:%s] bandwidth contract role=[role:%s], contract=[contract:%s] (#[contracttype:%d]/[contractid:%d]).	This shows an internal debug message	
522115	Debug	User idle ip=[ipaddr:%s], role=[role:%s] [macmismatch:%s].	This shows an internal debug message	
522116	Debug	User moved ip=[ipaddr:%s], role=[role:%s].	This shows an internal debug message	
522117	Debug	user_authenticate : Ignoring Duplicate Authetication message. User [mac:%s] already in authenticated role [role:%s].	This shows an internal debug message	

522118	Debug	user_authenticate : Sending SOS_USER_ACTION_ADD for updation to RAP [rapip:%s]: IP=[userip:%s], Role: [role:%s], ACL:[acl:%d], authtype:[authtype:%d] Idle-timeout: [idle_tmo:%d].	This shows an internal debug message	
522119	Debug	Reauthentication timer restarted for user [mac:%s] ([reauth:%d] seconds, type [type:%s]).	This shows an internal debug message	
522120	Debug	DYNAMIC-BWM: Delete current [updownstream:%s] [type:%s]-BWM contract: contract=[contract:%s] (#[contracttype:%d]/[contractid:%d]).	This shows an internal debug message	
522121	Debug	DYNAMIC-BWM: Add [updownstream:%s] Dynamic-BWM contract: contract=[contract:%s] (#[contracttype:%d]/[contractid:%d]) for mac : [mac:%s].	This shows an internal debug message	
522122	Debug	Reset BWM contract: MAC=[macstr:%s] userrole=[userrole:%s], contract=[contract:%s] ([contracttype:%d]/[contractid:%d]), type=[type:%s], newrole=[newrole:%s], bwmname=[bwmname:%s].	This shows an internal debug message	
522123	Debug	Delete [updownstream:%s] BWM contract: role=[role:%s], contract=[contract:%s] (#[contracttype:%d]/[contractid:%d]).	This shows an internal debug message	
522124	Debug	Unknown BWM contract type [bwmperuser:%d].	This shows an internal debug message	
522126	Debug	Add [updownstream:%s] BWM contract: role=[role:%s], contract=[contract:%s] (#[contracttype:%d]/[contractid:%d]) type=[type:%s].	This shows an internal debug message	
522127	Debug	{[l2orl3:%s]} Update role from [role:%s] to [name:%s] for IP=[ip:%s], MAC=[mac:%s].	This shows an internal debug message	
522128	Debug	download-L2: acl=[acl:%d]/[std_acl:%d] role=[role:%s], tunl=[tunl:%x], PA=[pa:%d], HA=[ha:%d], RO=[ro:%d], VPN=[vpn:%d] L3MOB=[l3mob:%d].	This shows an internal debug message	
522129	Debug	download: ip=[ipaddr:%s] acl=[acl:%d]/[stdacl:%d] role=[role:%s], Ubwm=[ubwm:%d], Dbwm=[dbwm:%d] tunl=[tunl:%x], PA=[pa:%d], HA=[ha:%d], RO=[ro:%d], VPN=[vpn:%d].	This shows an internal debug message	
522130	Debug	{[ipuser:%s]} datapath entry deleted.	This shows an internal debug message	
522131	Debug	User update: {[ipuser:%s]} HA recv "[tmpBuf:%s]".	This shows an internal debug message	
522132	Debug	User update: curr name=[name:%s] l2 role=[l2role:%s] l3 role=[l3role:%s] aaa profile=[aaaprofile: %s] meth=[meth:%d] state=[state:%d] essid=[essid:%s] loc=[apname:%s]/[apgroupname:%s] bssid=[bssid:%s] phy=[phy:%d].	This shows an internal debug message	
522133	Debug	{[ipaddr:%s]}: [debugbuf:%s].	This shows an internal debug message	
522134	Debug	[func:%s]: deleting bridge entry for vlan [vlan:%d] assigned_vlan [assignedvlan:%d].	This shows an internal debug message	
522136	Debug	{[utype:%s]} [name:%s] from profile "[aaa_profile:%s]" for user [mac:%s].	This shows an internal debug message	
522137	Debug	[where:%s]-[mac:%s]/[ipaddr:%s] : No match for User-Agent: [useragent:%s].	This shows an internal debug message	
522138	Debug	[where:%s]-[mac:%s]/[ipadd:%s] : User-Agent: [useragent:%s], final=[fin:%d], index=[ind:%d] stringindex=[strind:%d] os-version=[os:%s].	This shows an internal debug message	
522139	Debug	Deleting AP Wired User (tunnel) [mac:%s] from STM stats tree.	This shows an internal debug message	
522140	Debug	pkt from mac [mac:%s] : src ip [ipaddr:%s] unknown to mobility.	This shows an internal debug message	
522141	Debug	[mac:%s] IP [userip:%s]: drop pkt as ip not assigned through dhcp.	This shows an internal debug message	
522142	Debug	Setting [type: %s] role to [role:%s] for user [mac: %s]".	This shows an internal debug message	
522143	Debug	user_miss from RAP:[rap:%s], ([wired:%s]) user IP:[userip:%s], VLAN:[vlan:%d], BSSID:[mac:%s] MAC:[smac:%s]:AP:[apname:%s], flags=[f:%x].	This shows an internal debug message	
522144	Debug	L2 entry updated from RAP:[rapip:%s], [wired:%s] user IP:[userip:%s], MAC : [mac:%s], VLAN:[vlan:%d], BSSID:[bssid:%s].	This shows an internal debug message	
522145	Debug	[func:%s](): Entered. MAC:[mac:%s], IP:[ip:%s], apName:[apname:%s] action:[act:%d] acl:[acl:%s].	This shows an internal debug message	
522146	Debug	Adding AP Wired User (split) [mac:%s] to STM stats tree.	This shows an internal debug message	
522147	Debug	rap user : Sending SOS_USER_ACTION_ADD to RAP [rap:%s]: IP=[ipaddr:%s], Role: [role:%s], ACL:[acl:%d], authtype:[authtype:%d] idle-timeout:[idle_tmo:%d].	This shows an internal debug message	
522148	Debug	Update L3 entry role to [rolename:%s]: IP=??.	This shows an internal debug message	
522149	Debug	Reauthentication timer cancelled for IP=[ipaddr:%s].	This shows an internal debug message	

522150	Debug	Reauthentication timer restarted for user [mac:%s] ([seconds:%d] seconds, type [type:%s]).	This shows an internal debug message	
522151	Debug	Adding AP Wired User (tunnel) [mac:%s] to STM stats tree.	This shows an internal debug message	
522152	Debug	station free: bssid=[bssid:%s], mac=[macsta:%s].	This shows an internal debug message	
522153	Debug	tunnel #[tunid:%d], acl #[aclnum:%d].	This shows an internal debug message	
522154	Debug	Deleting AP Wired User (fw_mode [fwmode:%d]) [mac:%s] from STM stats tree.	This shows an internal debug message	
522155	Debug	[func:%s]: sta_ap--.	This shows an internal debug message	
522156	Debug	Deleting AP Wired User (split/bridge) [mac:%s] from STM stats tree.	This shows an internal debug message	
522158	Debug	Role Derivation for user [ipuser:%s]-[mac:%s]-[username:%s] [role: %s] [event: %s].	This shows an internal debug message	
522160	Debug	Error setting l2 role for user [ipuser:%s] [mac:%s] [username:%s] [oldrole: %s] [oldrolehow: %s] ([rh: %d]) [newrole: %s] [newrolehow: %s]([nrh: %d]).	This shows an internal debug message	
522161	Debug	Valid Dot1xct, remote:[remote:%d], assigned:[assigned:%d], default:[default:%d], current:[current:%d],termstate:[termstate:%d], wired:[wired:%d], dot1x enabled:[dot1x:%d], psk:[psk:%d] static:[static:%d] bssid=[bssid:%s].	This shows an internal debug message	
522162	Debug	No dot1xctx, remote:[remote:%d], assigned:[assigned:%d], default:[default:%d], current:[current:%d],termstate:[termstate:%d], wired:[wired:%d], dot1x enabled:[dot1x:%d], psk:[psk:%d] static:[static:%d] bssid=[bssid:%s].	This shows an internal debug message	
522163	Debug	Station authentication is deferring Vlan assignment.	This shows an internal debug message	
522164	Debug	[t:%s] Handling station up - down : mac: [mac:%m] User type: [ut:%s] cluster enabled: [cl:%d]	This shows an internal debug message	
522165	Debug	station_authenticate : Sending SOS_USER_ACTION_SETACL for updation to RAP [rap:%s]: IP=??, Role: [role:%s], ACL:[acl:%d], authtype:[authtype:%d], ingress:[ingress:%d] idle-timeout:[idle_tmo:%d].	This shows an internal debug message	
522166	Debug	[func:%s]: deleting bridge entry for vlan [vlan:%d] assigned_vlan [assignedvlan:%d].	This shows an internal debug message	
522167	Debug	[func:%s]: adding bridge entry for vlan [vlan:%d] assigned_vlan [assignedvlan:%d].	This shows an internal debug message	
522168	Debug	Station is l2 authenticated, retain the l2 role : [l2role:%s].	This shows an internal debug message	
522169	Debug	Station inherit: IP=[ipaddr:%s] start bssid:[bssid:%s] essid: [essid:%s] port:[userport:%x] ([port:%x]).	This shows an internal debug message	
522170	Debug	SKIP bssid:[bssid:%s] essid:[essid:%s] port:[port:%x].	This shows an internal debug message	
522171	Debug	station inherit IP=[ipaddr:%s] bssid:[bssid:%s] essid: [essid:%s] auth:[auth:%d] type:[type:%s] role:[role:%s] port:[portid:%x].	This shows an internal debug message	
522172	Debug	[func:%s]: SKIP bssid:[bssid:%s] essid:[essid:%s] port:[portid:%x].	This shows an internal debug message	
522173	Debug	Station inherit FA: IP=[ipaddr:%s] bssid:[bssid:%s] essid: [essid:%s] auth:[auth:%d] type:[type:%s] role:[role:%s] name:[name:%s] port:[portid:%x].	This shows an internal debug message	
522174	Debug	{user [mac:%s] ip [userip:%s], type [type:%s]} Reauthentication timer expired.	This shows an internal debug message	
522175	Debug	skipping mac : [mac:%s], from AP : [ap:%s], with authtype : [authtype:%s].	This shows an internal debug message	
522176	Debug	dot1x threshold has not exceeded for mac : [mac:%s], from AP : [ap:%s].	This shows an internal debug message	
522177	Debug	tunnel not found for mac : [mac:%s], port : [portid:%x], from AP : [ap:%s].	This shows an internal debug message	
522178	Debug	failed to map enet, [enet:%s], ap wired port: [wiredport:%d] APHW_MAX_ENETS: [maxenets:%d].	This shows an internal debug message	
522179	Debug	Bridge role is not configured/applied in ap wired port profile of AP : [apip:%s].	This shows an internal debug message	
522180	Debug	Invalid Bridge role : [role:%s].	This shows an internal debug message	
522181	Debug	Dot1x profile : [dot1xprofile:%s] configured, skipping sending bridge role : [bridgerole:%s].	This shows an internal debug message	
522182	Debug	Setting SOS_USER_ACTION_SETACL_ON_AUTH_FAIL, RAP:[rapip:%s], MAC:[mac:%s] updating fw :[fw:%d] to [tofw:%d], ACL :[acl:%d] to [toacl:%d] ([authtype:%s]) Authtype: '[none:%s]' to NONE.	This shows an internal debug message	
522183	Debug	Denylist state cp:[cp:%d] [cpgrp:%d] mac:[mac:%d] [macgrp:%d] vpn:[vpn:%d] [vpngrp:%d] 1x:[dot1x:%d] [dot1xgrp:%d] ([wispr:%d] [wisprgrp:%d]) wispr:[one:%d] [two:%d] sid:[sid:%d] [sidgrp:%d].	This shows an internal debug message	

522184	Debug	Sending denylist message; Authentication=[auth:%s], Failures=[failure:%d].	This shows an internal debug message	
522185	Debug	Auth failure [fcount:%d] of [maxf:%d], method=[auth_type:%s].	This shows an internal debug message	
522186	Debug	Denylist fail state cp:[cp:%d] mac:[mac:%d] vpn:[vpn:%d] 1x:[dot1x:%d] ([dot1xserver:%d]) sid:[sid:%d].	This shows an internal debug message	
522187	Debug	Removing user from denylist table.	This shows an internal debug message	
522188	Debug	Creating controller entry with IP:[cntrip:%s],mac:[mac:%s],ACL:[acl:%d],Vlan:[vlan:%d], on AP:[ap:%s].	This shows an internal debug message	
522189	Debug	Changing RAP split user IP: [rapip:%s], ACL : [acl:%d].	This shows an internal debug message	
522191	Debug	Mac Auth failed wired [wired:%d] currvlan [currvlan:%d], UDR vlan [udrvlan:%d].	This shows an internal debug message	
522192	Debug	Mac Auth failed, continuing with dot1x.	This shows an internal debug message	
522193	Debug	Changing RAP split user IP: [ip:%s], ACL : [acl:%d]	This shows an internal debug message.	
522194	Debug	Sending pool l2tp [l2tppool:%s], pptp [pptppool:%s] in auth PAP response	This shows an internal debug message.	
522195	Debug	Sending pool l2tp [l2tppool:%s], pptp [pptppool:%s] in auth CPAP response	This shows an internal debug message.	
522196	Debug	Sending pool l2tp [l2tppool:%s], pptp [pptppool:%s] in auth MSCHAP response	This shows an internal debug message.	
522197	Debug	Sending pool l2tp [l2tppool:%s], pptp [pptppool:%s] in auth EAP response	This shows an internal debug message.	
522198	Debug	Sending pool l2tp [l2tppool:%s], pptp [pptppool:%s] in auth MSCHAPV2 response	This shows an internal debug message.	
522199	Debug	Sent dialer response ([dialer:%d]) for user [user:%s]	This shows an internal debug message.	
522200	Debug	Got dialer validate request for user [user:%s]	This shows an internal debug message.	
522201	Debug	PAP authenticate user (PAPI) [user:%s]	This shows an internal debug message.	
522202	Debug	VPN authenticate user (SOCKET) [user:%s]	This shows an internal debug message.	
522203	Debug	PAP authenticate user (SOCKET) [user:%s]	This shows an internal debug message.	
522204	Debug	CHAP authenticate user [user:%s]	This shows an internal debug message.	
522205	Debug	MS_CHAP authenticate user [user:%s]	This shows an internal debug message.	
522206	Debug	EAP authenticate user [user:%s]	This shows an internal debug message.	
522207	Debug	MS-CHAPV2 authenticate user [user:%s]	This shows an internal debug message.	
522208	Debug	PAP authenticate user (GTC)[user:%s]	This shows an internal debug message.	
522209	Debug	query user [user:%s]	This shows an internal debug message.	
522210	Debug	authorize user [user:%s]	This shows an internal debug message.	
522212	Debug	MAC=[mac:%s] IP=[ipaddr:%s]: MAC auth start: entry-type=[accesstype:%s], bssid=[bssid:%s], essid=[essid:%s] sg=[sgname:%s].	This shows an internal debug message	
522213	Debug	Mac Auth failed, wired [wired:%d] curvlan [currvlan:%d], UDR vlan [udrvlan:%d].	This shows an internal debug message	
522214	Debug	User [mac: %s] is in L3 Authenticated role: [role:%s], ignoring the DHCP UDR during client's ip-address renewal.	This shows an internal debug message	
522215	Debug	RELEASE received.	This shows an internal debug message	
522216	Debug	MAC [mac:%s], dhcp option [dhcp:%d], signature [signature:%s].	This shows an internal debug message	
522217	Debug	MAC=[mac:%s] IP=[ip:%s] Mobility prev state: default_vlan=[vlan:%d],port=[port:%x],flags=[flags:%d],tunid=[tunid:%d],apname=[apname:%s].	This shows an internal debug message	
522218	Debug	mac [mac:%s] : ip [ipaddr:%s] unknown to mobility.	This shows an internal debug message	
522224	Debug	{[l2l3:%s]} Update role from [role:%s] to [dynrole:%s] for visitor with IP=[ipstr:%s].	This shows an internal debug message	
522225	Debug	MAC=[mac:%s] IP=[ipaddr:%s] Create tunnel [tunid:%d], and role acl [roleacl:%d]/[stdacl:%d] for visitor.	This shows an internal debug message	
522226	Debug	MAC=[mac:%s] IP=[ipaddr:%s] MOVED AWAY: default_vlan=[defvlan:%d],port=[portid:%d],flag=[flag:%d],tunid=[tunid:%d],apname=[apname:%s].	This shows an internal debug message	
522229	Debug	MAC=[mac:%s] IP=[ipstr:%s] Delete user on [ha:%s]: role=[role:%s],age=[age:%s],default_vlan=[defvlan:%d],port=[port:%d],flag=[flags:%d],tunid=[tunid:%d],apname=[apname:%s].	This shows an internal debug message	
522230	Debug	MAC=[mac:%s] IP=[ipstr:%s] User delete: Send mobility delete message, flags=[flags:%x].	This shows an internal debug message	
522231	Debug	MAC=[mac:%s] Send Station delete message to mobility.	This shows an internal debug message	

522232	Debug	Data ready: MAC=[mac:%s] def_vlan [defvlan:%d] derive vlan: [derivevlan:%d] auth_type [authtype:%d] auth_subtype [authsubtype:%d].	This shows an internal debug message	
522234	Debug	Setting idle timer for user [mac: %s] to [time: %d] seconds (idle timeout: [idle: %d] ageout: [ageout: %d]).	This shows an internal debug message.	
522235	Debug	user_age_handler() called for user [mac: %s].	This shows an internal debug message.	
522236	Debug	user_age_byip() called for MAC [mac:%s] IP [ip: %s] ageout [ageout:%d] flags [flags:%x].	This shows an internal debug message.	
522237	Debug	Using cached dhcp option to derive role [dhcpopt:%s].	This shows an internal debug message.	
522238	Debug	Using cached dhcp option to derive vlan [dhcpopt:%s].	This shows an internal debug message.	
522239	Debug	{[ipuser:%s]} skip datapath entry deletion - Not downloaded yet.	This shows an internal debug message	
522240	Debug	Setting fallback idle timer for user [mac: %s] to [time: %d] seconds.	This shows an internal debug message.	
522241	Debug	Setting idle timer for outer VPN user [mac: %s] to [time: %d] seconds.	This shows an internal debug message.	
522242	Debug	MAC=[mac:%s] Station Created Update MMS: BSSID=[b:%s] ESSID=[e:%s] VLAN=[v:%d] AP-name=[n:%s]	Send station created update mms message	
522243	Debug	MAC=[mac:%s] Station Updated Update MMS: BSSID=[b:%s] ESSID=[e:%s] VLAN=[v:%d] AP-name=[n:%s]	Send station updated update mms message	
522244	Debug	MAC=[mac:%s] Station Deleted Update MMS	Send station deleted update mms message	
522245	Debug	user_age() called for MAC [mac: %s] IP [ip:%s].	This shows an internal debug message.	
522246	Debug	Idle timeout should be driven by STM for MAC [mac: %s].	This shows an internal debug message.	
522247	Debug	User idle timer removed for user with MAC [mac: %s].	This shows an internal debug message.	
522249	Debug	Station [mac:%s] : After Update from CPPM, device-type=[type:%s] os-version=[os:%s].	This shows an internal debug message	
522253	Debug	VDR - mac [mac:%s] derivation_type [type:%s] derived vlan [vlan:%d].	This shows an internal debug message	
522254	Debug	VDR - mac [mac:%s] rolename [rn:%s] fwdmode [fwdm:%d] derivation_type [type:%s] vp [vp:%s].	This shows an internal debug message	
522255	Debug	VDR - set vlan in user for [mac:%s] vlan [vlan:%d] fwdmode [fwdm:%d] derivation_type [type:%s]. This shows an internal debug message 522256@VDR - Getting highest non-auth vlan for [mac:%s] which is vlan [vlan:%d].	This shows an internal debug message	
522257	Debug	VDR - send current vlan for user [mac:%s] vlan [vlan:%d] derivation_type [type:%s] trace [trc:%s]. This shows an internal debug message 522258@VDR - Add to history of user user [mac:%s] vlan [vlan:%d] derivation_type [type:%s] index [index:%d].	This shows an internal debug message	
522259	Debug	VDR - Do Role Based VLAN Derivation user [mac:%s] role [role:%s] rolehow [rolehow:%s]. This shows an internal debug message 522260@VDR - Cur VLAN updated [mac:%s] mob [m:%d] inform [i:%d] remote [r:%d] wired [w:%d] defvlan [d:%d] exportedvlan [e:%d] curvlan [c:%d].	This shows an internal debug message	
522261	Debug	User MAC:[mac:%s]: purge IP:[ip:%s]. This shows an internal debug message 522262@User MAC:[mac:%s]: Total users purged = [count:%d].	This shows an internal debug message	
522263	Debug	MAC:[mac:%s]: User-Agent: [str:%s]. This shows an internal debug message 522264@MAC:[mac:%s]: Allocating UUID: [uuid:%s]	This shows an internal debug message	
522265	Debug	MAC:[mac:%s]: UBT case, Role vlan [rvlan:%d] current vlan [cvlan:%d].	This shows an internal debug message	
522266	Debug	Calling derive_role2 for user [mac: %s]	This shows an internal debug message	
522268	Debug	AP-Bridge-Wired User: current-l2acl:[l2acl:%d], current-Role:[l2role:%s]	This shows an internal user debug message	
522269	Debug	AP-Bridge-Wired User: updated-l2acl:[l2acl:%d], updated-l2role:[l2role:%s]	This shows an internal user debug message	
522270	Debug	During User miss marking the user [mac:%s] with ingress [i:%x], connection-type [c:%d] as [w:%s], muxtunnel = [m:%s]	This shows an internal debug message	
522271	Debug	MAC=[mac:%s], detected a wireless to wired move ESSID [essid:%s]	This shows an internal user debug message	
522272	Debug	AP-Group is present in the Internal Database or provisioning profile for username=[user:%s]	Ap-group is set in internal database or provisioning profile	
522277	Debug	MAC[mac: %s]RADIUS Accounting to next server as multiple server accounting enabled. Server=[name: %s]	This shows an internal user debug message	

522281	Debug	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] User enqueued, total enqueued: [count: %d]	User put onto pending queue for downloadable role till role download completes	
522282	Debug	MAC=[mac:%s] Dldb Role: [r:%s] User will be assigned default role for the auth-type	User will be assigned default role for the auth-type because of error or downloadable role is pending	
522283	Debug	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] User dequeued, total enqueued: [count: %d]	User removed from pending queue for downloadable role after role download completes	
522284	Debug	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] Skip queueing user to role	This shows an internal debug message	
522285	Debug	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] Adding user ref as [type: %s], total refs: [count: %d]	This shows an internal debug message	
522286	Debug	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] Deleting user ref as [type: %s], total refs: [count: %d]	This shows an internal debug message	
522287	Debug	Auth GSM : MAC_USER publish for mac [m: %s] bssid [b: %s] vlan [v: %d] type [t: %d] data-ready [d: %d] HA-IP [ha: %s]	This shows an internal user debug message	
522289	Debug	Auth GSM : MAC_USER mu_delete publish for mac [m: %s] bssid [b: %s] vlan [v: %d] type [t: %d] data-ready [d: %d] deauth-reason [dr: %d] HA-IP [ha: %s]	This shows an internal user debug message	
522290	Debug	Auth GSM : MAC_USER delete for mac [m: %s]	This shows an internal user debug message	
522291	Debug	Auth GSM : MAC_USER delete failed for mac [m: %s] result [r: %s]	This shows an internal user debug message	
522292	Debug	Auth GSM : MAC_USER notify for mac [m: %s] vlan [v: %d]	This shows an internal user debug message	
522295	Debug	Auth GSM : USER_STA event [e: %d] for user [m: %s]	This shows an internal user debug message	
522296	Debug	Auth GSM : USER_STA delete event for user [m: %s] age [a: %d] deauth_reason [dr: %u]	This shows an internal user debug message	
522297	Debug	Auth GSM : MAC_USER response event for user [m: %s]	This shows an internal user debug message	
522298	Debug	Auth GSM : MAC_USER response dropped for user [m: %s]	This shows an internal user debug message	
522299	Debug	Auth GSM : DEV_ID_CACHE publish for mac [m: %s] dev-id:[devname: %s]([devid: %d]) os-version:[osname: %s]([osid: %d]) cassified-by: [cname: %s]([cid: %d])	This shows an internal user debug message	
522301	Debug	Auth GSM : USER publish for uuid [u:%s] mac [m: %s] name [n: %s] role [r: %s] devtype [d: %s] wired [w: %d] authtype [au: %d] subtype [s: %d] encrypt-type [e: %e] conn-port [c: %d] fwd-mode [f: %d] roam [or: %d] repkey [rep:%d]	This shows an internal user debug message	
522303	Debug	Auth GSM : USER delete for mac [m: %s] uuid [u:%s]	This shows an internal user debug message	
522304	Debug	Auth GSM : USER delete failed for mac [m: %s] uuid [u: %s] result [r: %s]	This shows an internal user debug message	
522305	Debug	Auth GSM : DEV_ID_CACHE validate cb for mac [m: %s] result [r:%d]	This shows an internal user debug message	
522307	Debug	Reauthentication timer exists for user [mac:%s] for [seconds:%d] seconds type [type:%s]).	This shows an internal debug message	
522308	Debug	Device Type index derivation for [m: %s] : dhcp ([i1: %d],[i2: %d],[i3: %d]) oui ([i4: %d],[i5: %d]) ua ([i6: %d],[i7: %d],[i8: %d]) derived [s: %s]([i9: %d]):[os:%s]	This shows an internal user message	
522309	Debug	Deriving role from user attributes. MAC=[mac:%s].	This shows an internal debug message	
522315	Debug	MAC=[mac:%s] ingress [ingres:%x] ([usr_dest:%s]), u_encr [u_encr:%d], m_encr [m_encr:%d], slotport [slot:%x] [port:%s], type: [type:%s], FW mode: [fw_mode:%u], AP IP: [apip:%s] mdie [mdie:%d] ft_complete [ft_complete:%d]	This shows an internal user debug message	
522316	Debug	Idle timeout should be driven by STM for MAC [mac: %s].	This shows an internal debug message.	
522317	Debug	MAC:[mac:%s]: Reusing UUID: [uuid:%s] This shows an internal debug message 522318@MAC:[mac:%s]: Copying GSM mac user.	This shows an internal debug message	
522320	Debug	{[ipuser:%s]} datapath entry deleted.	This shows an internal debug message	
522322	Debug	Auth GSM : USER publish Success for mac [m: %s] [uuid: %s] [rep_key: %d]	This shows an internal user debug message	
522324	Debug	Auth GSM : MAC USER publish Success for mac [m: %s] [rep_key: %d]	This shows an internal user debug message	
522326	Debug	Auth GSM : USER repkey change Success for mac [m: %s] [uuid: %s] [rep_key: %d]	This shows an internal user debug message	
522328	Debug	Auth GSM : MAC USER change repkey Success for mac [m: %s] [rep_key: %d]	This shows an internal user debug message	
522330	Debug	Auth GSM : STA change repkey Success for mac [m: %s] [rep_key: %d]	This shows an internal user debug message	
522331	Debug	AP-Bridge station ([mac:%s]) invalid ACL name:[aclnname:%s]	This shows an internal user debug message	
522333	Debug	MAC=[mac:%s] IP=[ipaddr:%s] INTER MOVE: HA-IP [ha:%s] HA-UUID [uuid:%s]	This shows an internal user debug message	
522334	Debug	Sending DHCP VLAN to Mobility: MAC=[mac:%s] dhcp vlan [dhcpvlan:%d] type [type:%d].	This shows an internal debug message	

522335	Debug	DA request received with attributes : User MAC [mac:%s], User IP-Address [uip:%s], User-Name [name:%s], Session-Id [id:%s], Station ID [sta_id:%s], reqcode=[reqcode:%d], rspcode=[rspcode:%d], nack=[nack:%d], error_cause=[cause:%s].	This shows an internal debug message	
522338	Debug	Received DHCP based UDR VLAN change ACK from Mobility: MAC=[mac:%s] dhcp vlan [dhcpvlan:%d].	This shows an internal debug message	
522341	Debug	Client [mac:%s] idle timeout [tmo:%d] profile [prof:%s]	This shows an internal debug message	
522342	Debug	[func:%s] ([line:%u]): rtts macuser [user:%m] not found		
522343	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] enabled=[state:%d] old tput=[old_tput:%d] new tput=[new_tput:%d] discard=[discard:%d] reest=[reest:%d] keepalive=[keepalive:%d]		
522344	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] enabled=[state:%d] initial tput=[tput:%d]		
522345	Debug	Delete [updownstream:%s] dynamic bandwidth contract group-id=[groupid:%u], contract=[contract:%s] (#[contracttype:%d]/[contractid:%d]).	This shows an internal debug message	
522346	Debug	Role Change by L2 Auth, get ipuser to update BWC: mac=[mac:%s], role=[role:%s]	This shows an internal debug message	
522349	Debug	MAC [mac:%s] IP [userip:%s]: non-DHCP pkt received, Option-12 hostname configured for accounting.	This shows an internal debug message	
522351	Debug	MAC=[mac:%s] Dldb Role: [r:%s] Server Name [name:%s] been put in GSM	Downloadable role been prepared to be shared with standby cluster node.	
522352	Debug	MAC authentication request sent for MPSK user - MAC [mac:%s].	This shows an internal debug message	
522353	Debug	MPSK passphrase received for MPSK user - MAC [mac:%s].	This shows an internal debug message	
522354	Debug	PSK assigned for MPSK user - MAC [mac:%s].	This shows an internal debug message	
524000	Debug	Skipping disable operation, opcode:0x[address:%x] not registered.	This shows internal debug messages.	
524001	Debug	cert id [certid:%d] tun id [tuneid:%d].	This shows internal debug messages.	
524002	Debug	Download was skipped	This shows internal debug messages.	
524003	Debug	Dot1x- Default profile cert id:[certid:%d].	This shows internal debug messages.	
524004	Debug	Dot1x- Download time ID :[certid:%d],[certname:%s],[caname:%s]	This shows internal debug messages.	
524011	Debug	Src ip:[src:%s],Dst ip:[dst:%s],offset= [offset:%d] flags:=[flags:%d] Fragmented Packet	This shows internal debug messages.	
524012	Debug	Fragment Length [fraglen:%d]	This shows internal debug messages.	
524013	Debug	Forwarding the Radius packet after stateful dot1x processing code=:[code:%d], smac=:[smac:%s],sport=:[sport:%d],dport[dport:%d]	This shows internal debug messages.	
524014	Debug	radius request timeout, unauthenticating station name:[name:%s], mac=:[mac:%s]	This shows internal debug messages.	
524015	Debug	Forwarding the Radius Response to AP:[ipstr:%s],[len:%d]	This shows internal debug messages.	
524016	Debug	radius response timeout, unauthenticating station name=:[name:%s],mac=:[mac:%s]	This shows internal debug messages.	
524017	Debug	User name:[name:%s] ,has moved from SAP mac:[mac:%s] to SAPmac:[smac:%s]	This shows internal debug messages.	
524018	Debug	Forwarding to the Radius Server[srvip:%s],len:[len:%d]	This shows internal debug messages.	
524029	Debug	FT([string:%s]): sap=[string1:%s] mdie=[mdie:%d], ft_cap=0x[ft_cap:%x] ucast 0x[ucast:%x]	This shows internal debug messages.	
524031	Debug	Continuing show at [i:%d] [instance:%lu]	This shows internal debug messages.	
524032	Debug	For kcache table [i:%x], got pcache [pcache:%lu] for mac [mac:%s] bssid [mac1:%s]	This shows internal debug messages.	
524033	Debug	Breaking the show at [i:%d] [pcache:%lu] ie for mac [mac:%s] bssid [bssid:%s]	This shows internal debug messages.	
524034	Debug	[string:%s]: begins=>	This shows internal debug messages.	
524035	Debug	[i:%2x] [j:%2x] [k:%2x] [l:%2x] [m:%2x] [n:%2x] [o:%2x] [p:%2x]	This shows internal debug messages.	
524036	Debug	[string:%s]: ends=>	This shows internal debug messages.	
524037	Debug	[string:%s]: [mac:%s] sending key1 11r ([ft:%d]) xsec([xsec:%d])	This shows internal debug messages.	
524038	Debug	[string:%s]: FT sending key1	This shows internal debug messages.	
524039	Debug	[string:%s]: MFP sending Key Desc Ver 3 in key1	This shows internal debug messages.	
524040	Debug	[string:%s]: rsn len ([len:%d])	This shows internal debug messages.	
524041	Debug	[string:%s] :FT mesg3 copied gtk, len=[len:%d] data len=[len1:%d]	This shows internal debug messages.	

524042	Debug	[string:%s]: FT mic=[string1:%s]	This shows internal debug messages.	
524045	Debug	FT ([func:%s]): sap=[bssid:%s] mdie=[mdie:%d] ft_cap=0x[cap:%x] ucast=0x[ucast:%x] mcast 0x[mcast:%x]	This shows internal debug messages.	
524047	Debug	USERNAME	This shows internal debug messages.	
524048	Debug	NAP_IP_ADDRESS	This shows internal debug messages.	
524049	Debug	CALLING_STATION_ID	This shows internal debug messages.	
524050	Debug	CALLED_STATION_ID	This shows internal debug messages.	
524051	Debug	EAP MESSAGE	This shows internal debug messages.	
524052	Debug	NAS_IDENTIFIER_ID	This shows internal debug messages.	
524053	Debug	NAS_IDENTIFIER_ID	This shows internal debug messages.	
524054	Debug	NAS_IP is set to 0.0.0.0, Using source ip as the NAS_IP	This shows internal debug messages.	
524055	Debug	Received Valid Radius Response	This shows internal debug messages.	
524069	Debug	FT [str:%s] input: pmk_r0=[str1:%s], pmk_r0_name=[str2:%s] r1kh_id=[id:%s]	This shows internal debug messages.	
524070	Debug	RSNIE buf([len:%zu])=[str:%s]	This shows internal debug messages.	
524071	Debug	FT [str:%s] Derived pmk_r1=[str1:%s], pmk_r1_name=[str2:%s]	This shows internal debug messages.	
524072	Debug	FT ([str:%s]): bssid=[bssid:%s]	This shows internal debug messages.	
524073	Debug	FT ([str:%s]): input pmk_r1 =[str1:%s]	This shows internal debug messages.	
524074	Debug	FT ([str:%s]): input pmk_r1_name =[str1:%s]	This shows internal debug messages.	
524075	Debug	FT ([str:%s]): snonce=[str1:%s]	This shows internal debug messages.	
524076	Debug	FT ([str:%s]): anonce=[str1:%s]	This shows internal debug messages.	
524077	Debug	FT ([str:%s]): Derived ptk [ptk:%s]	This shows internal debug messages.	
524078	Debug	FT ([str:%s]): Derived ptk_name [ptk:%s]	This shows internal debug messages.	
524079	Debug	FT ([str:%s]): essid:[essid:%s], bssid:[bssid:%m] ukey:0[ukey:%x], mkey:[mkey:%x], cnsa:[cnsa:%s], wpa3_non_cnsa_gcm256:[noncnsa:%s], sae:[sae:%s], psk:[psk:%s], tkip:[tkip:%s]	This shows internal debug messages.	
524080	Debug	FT: cannot allocate FT key info entry	This shows internal debug messages.	
524081	Debug	[str:%s]: kcache [cache:%pI4] for sta [sta:%s] added	This shows internal debug messages.	
524082	Debug	[str:%s]: Error adding pcache	This shows internal debug messages.	
524083	Debug	[str:%s]: pcache [pcahe:%p] for sta [sta:%s] added.	This shows internal debug messages.	
524084	Debug	FT: xxkey=[str:%s], mdid=[mdid:%d], ssid=[ssid:%s], r0kh_id=[id:%s]	This shows internal debug messages.	
524085	Debug	FT [str:%s]: pmk_r0:[pmk:%s], pmk_r0_name [name:%s]	This shows internal debug messages.	
524086	Debug	FT [str:%s]: ptk[ptk:%s]	This shows internal debug messages.	
524087	Debug	FT [str:%s]: input: sta [sta:%s], sap_mac[sap:%s]	This shows internal debug messages.	
524088	Debug	[str:%s]: kcache [cache:%p] found for sta [sta:%s]	This shows internal debug messages.	
524089	Debug	[str:%s]: Error adding kcache and r0_data	This shows internal debug messages.	
524090	Debug	[str:%s]: Copy new pmk_r1 = [pmk:%s], pmk_r1_name = [str1:%s]	This shows internal debug messages.	
524091	Debug	[str:%s]: Missing kcache entry!	This shows internal debug messages.	
524092	Debug	[str:%s]: kcache found	This shows internal debug messages.	
524093	Debug	FT([str:%s]) r0kh:[r0kh:%s], r0_name:[str1:%s]	This shows internal debug messages.	
524095	Debug	Missing kcache entry!	This shows internal debug messages.	
524096	Debug	PMKR0-Name mismatch! cached=[str:%s]	This shows internal debug messages.	
524097	Debug	Generated anonce:[str:%s]	This shows internal debug messages.	
524098	Debug	[str:%s]: Derived gtk=[str1:%s]	This shows internal debug messages.	
524099	Debug	[str:%s]: Encrypted gtk=[str1:%s]	This shows internal debug messages.	
524100	Debug	FT([str:%s]): Calculating MIC	This shows internal debug messages.	
524101	Debug	MIC buf(60)=[str:%s], mic_buf_len [len:%d]	This shows internal debug messages.	
524102	Debug	MIC buf([mic:%d])=[str:%s], mic_buf_len [len:%d]	This shows internal debug messages.	
524103	Debug	FTIE-MIC =[str:%s]	This shows internal debug messages.	
524104	Debug	FT:Failed to calculate MIC	This shows internal debug messages.	
524105	Debug	FT([str:%s]): buf_len([len:%zu]) = 2*ETH_ALEN + 1 + rsnie_len([rsnie:%zu]) + mdie_len([mdie:%zu]) + ftie_len([ftie:%zu]) + ric_len([ric:%zu]), buf [buf:%p]	This shows internal debug messages.	
524106	Debug	FT association request	This shows internal debug messages.	

524108	Debug	[str:%s]: Error adding kcache	This shows internal debug messages.	
524109	Debug	[str:%s]: missing sap entry for bssid [bssid:%s], encr 0x[encr:%x]	This shows internal debug messages.	
524110	Debug	Mismatch PMKR1-Name!	This shows internal debug messages.	
524111	Debug	[str:%s]: missing sap entry for bssid [bssid:%s]	This shows internal debug messages.	
524112	Debug	[func:%s]: kcache essid ([kcacheessid:%s]), essid ([essid:%s])	This shows internal debug messages.	
524113	Debug	auth done called from ncfg_dot1x_validatepmkid_enabled	This shows internal debug messages.	
524114	Debug	MAC auth failed, skipping dot1x.	This shows internal debug messages.	
524115	Debug	Auth done called from Authenticated state.	This shows internal debug messages.	
524116	Debug	DHCP UDR defined vlan. Got response from STM VLAN UPDATED.	This shows internal debug messages.	
524117	Debug	Auth done called from Key Challenge.	This shows internal debug messages.	
524118	Debug	[func:%s] cached entry [buf:%s].	This shows internal debug messages.	
524119	Debug	[func:%s] Failed to lookup user/dot1xctx.	This shows internal debug messages.	
524120	Debug	[func:%s] Failed to lookup user.	This shows internal debug messages.	
524121	Debug	Derived VLAN for the user is [vlan:%d].	This shows internal debug messages.	
524122	Debug	ACL/Key propagation failed, Msgtype:[msgtype:%d], keytype:[keytype:%d], mac:[mac:%s], bssid:[bssid:%s], error:[errstr:%s]([errid:%d]), station doesnt exist currently.	This shows internal debug messages.	
524123	Debug	ACL/Key propagation failed, Msgtype:[msgtype:%d], keytype:[keytype:%d], mac:[mac:%s], bssid:[bssid:%s], error:[errstr:%s]([errid:%d]), sending deauth to station.	This shows internal debug messages.	
524124	Debug	[func:%s](): MAC:[mac:%s], pmkid_present:[pmkid_present:%s], pmkid:[pmkid:%s]	This shows internal debug messages.	
524125	Debug	[func:%s](): FT-Bridge Client-MAC:[mac:%s] Recover from K-cache- VLAN:[vlan:%d] ROLE:[role:%s]	This shows internal debug messages.	
524129	Debug	[func:%s](): MAC:[mac:%s] GSM: Successfully published Key-cache object.	This shows internal debug messages.	
524131	Debug	[func:%s](): MAC:[mac:%s] GSM: Successfully deleted Key-cache object.	This shows internal debug messages.	
524134	Debug	[func:%s](): MAC:[mac:%s] BSS:[bssid:%s] GSM: Successfully published PMK-cache object.	This shows internal debug messages.	
524136	Debug	[func:%s](): MAC:[mac:%s] BSS:[bssid:%s] GSM: Successfully deleted PMK-cache object.	This shows internal debug messages.	
524139	Debug	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s] Update:[update:%c]	This shows internal debug messages.	
524140	Debug	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s] Update:[update:%c]	This shows internal debug messages.	
524141	Debug	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s]	This shows internal debug messages.	
524142	Debug	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s] Update:[update:%c]	This shows internal debug messages.	
524148	Debug	PMK aging: start-index [si:%d] end-index [ei:%d] (visited, deleted) kcache ([kv:%d], [kd:%d]) pcache ([pv:%d], [pd:%d])	This shows internal debug messages.	
524149	Debug	okc Key found in dt-cache for Client-MAC:[mac:%s].	This shows internal debug messages.	
524150	Debug	11r key found in dt-cache for Client-MAC:[mac:%s].	This shows internal debug messages.	
524153	Debug	[func:%s]():[line:%u]: MAC:[mac:%s] finished authentication, start process auth_done.	This shows internal debug messages.	
524154	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] dot1xctx_auth_type=[auth:%d] enabled=[state:%d] result=[result:%d]		
524155	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] RTTS_ACCEPT reest=[reest:%d] discard=[discard:%d] keepalive=[keepalive:%d]		
524156	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] RTTS_REJECT send stm denylist bkoff=[backoff:%d]		
524157	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] RTTS_RESULT not received		
524158	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] RADIUS ACCEPT result=[result:%d] discard=[discard:%d] reest=[reest:%d] keepalive=[keepalive:%d] bkoff=[bkoff:%d] earlylift=[earlylift:%d]		
524160	Debug	[func:%s] ([line:%u]): rtts user=[user:%m] Added VSA for throughput [tput:%d]		
525101	Debug	OWE: Station=[mac:%m] BSS=[bss:%m] PMKID Matched.	This indicates OWE client with matched PMKID.	
525102	Debug	OWE: Station=[mac:%m] BSS=[bss:%m] done with DH-Group=[grp:%u].	This indicates D-H is performed for an OWE client.	

525103	Debug	OWE: Station=[mac:%m] BSS=[bss:%m] failed with unsupported DH-Group=[grp:%u].	This indicates D-H can't be performed due to unsupported group for an OWE client.	
525104	Debug	OWE: Station=[mac:%m] BSS=[bss:%m] failed due to non-OWE BSS.	This indicates D-H can't be performed due to incorrect BSS.	
527000	Debug	[thread:%u] [func:%s] [line:%d] [msg:%s]	User debug messages for mDNS proxy (mdns)	
527003	Debug	[thread:%u] CPPM [func:%s] [line:%d] [msg:%s]	CPPM information update from mDNS proxy (mdns)	
527500	Debug	[func:%s] [line:%d] [msg:%s]	User debug messages for AirGroup	
541005	Debug	[func:%s]: set accounting session, client mac-[mac:%m], time-[time:%u],name-[name:%s].	AP update client from STM.	
541006	Debug	[func:%s]: Set auth state, Station [mac:%m], authenticated [true:%d].	Station authenticated state.	
541007	Debug	[func:%s]: persist client mac-[mac:%m], bssid-[bssid:%m], essid-[essid:%s].	AP sync persist client to STM.	
541008	Debug	[func:%s]: client mac-[mac:%m], bssid-[bssid:%m], essid-[essid:%s], session-[name:%s] [time:%u].	AP sync client to STM.	
541009	Debug	[func:%s]: machine auth token, mac-[mac:%m], bssid-[bssid:%m], ssid-[ssid:%s].	AP configure machine auth.	
541010	Debug	[func:%s]: apip-[ap_ip:%s], clientip-[client_ip:%s], mac-[mac:%m], bssid-[bssid:%m].	AP sent reauth.	
541011	Debug	[func:%s]: sta look up req to apip-[ap_ip:%s], mac-[mac:%m] timestamp-[time:%u]-[time_usec:%u].	AP sent/receive station request.	
541014	Debug	[func:%s]: sta lkup response to ap-[ap_ip:%s], mac-[mac:%m], cap-[cap:%s] timestamp-[time:%u]-[time_usec:%u].	AP sent/receive station response.	
541015	Debug	[func:%s]: send machine auth token for sta-[sta:%m].	Station update.	
541016	Debug	[func:%s]: Send reauth ctx for client-[mac:%m], timeout-[to:%d], authtime-[at:%d], auth age-[ag:%d], essid-[essid:%s].	Station update.	
541019	Debug	[func:%s]: session timeout, sta [mac:%m] , reauth-[session_time:%d], current-[current:%d].	Station update.	
541020	Debug	[func:%s]: sta [mac:%m] reauth disable in ssid-[ssid:%s].	Station update.	
541022	Debug	[func:%s]: send sta-[mac:%m] update to conductor-[conductor:%s], essid-[essid:%s].	Station update.	
541024	Debug	[func:%s],[line:%d]:get sync message for client [mac:%m], from [from_ap:%s], username [name:%s], hostname [hostname:%s]	station ip updated.	
541025	Debug	[func:%s]: check client [mac:%m] [ip:%s] on AP [ap_ip:%s], timeout [timeout:%d] auth time [time:%d].	Debug client reauth info.	
541027	Debug	Locate client response for [mac:%m], AP-ip: [ap_ip:%s].	AP locate client.	
541029	Debug	Receive stat publish for client - [mac:%m], from ap [ip:%s].	Receive stat publish msg.	
541030	Debug	[func:%s]: Set user role, Station [mac:%m] essid [essid:%s] role [name:%s] acl_flag[flag:%d] rule_index [index:%x].	Station user role update.	
541033	Debug	[func: %s]: L3 mobility updates user [mac:%m] [action:%s] [type:%s] with [peerip:%s] [vcip:%s].	Marking or clearing the client as foreign or remote.	
541037	Debug	[func:%s]: send accounting interval, sta [mac:%m] , account interval-[time:%d].	Station update.	
541038	Debug	[func:%s]: send class attribute, sta [mac:%m] , class attribute-[class:%s].	Station update.	
541039	Debug	[func:%s]: Set dhcp-opt, Station [mac:%m] essid [essid:%s] role [name:%s] rule_index [index:%x] vlan [vlan:%d] vlanhow[vlanhow:%s].	Station dhcp-option update.	
541040	Debug	[func:%s]: Set os string, client [mac:%m], os [os:%s].	Station os update.	
541041	Debug	[func:%s]: update vc for client [mac:%m].	Station update to vc.	
541042	Debug	[func:%s]: set accounting interval, sta [mac:%m] , account interval-[time:%d].	Station update.	
541043	Debug	[func:%s]: set class attribute, sta [mac:%m] , class attribute-[class:%s].	Station update.	
541044	Debug	[func:%s]: set reauth ctx for client-[mac:%m], timeout-[to:%d], authtime-[at:%d], auth age-[ag:%d], essid-[essid:%s].	Station update.	
541045	Debug	[func:%s]: Send accounting session, client mac-[mac:%m], name-[name:%s], time-[time:%u].	AP update client from STM.	
541053	Debug	[func:%s]: Send os string, client [mac:%m], os [os:%s].	Station os update.	
541054	Debug	[func:%s]: Send user role, Station [mac:%m] essid [essid:%s] role [name:%s] acl_flag [flag:%d] rule_index [index:%x].	Station user role update.	

541055	Debug	[func:%s]: Send dhcp-opt, Station [mac:%m] essid [essid:%s] role [num:%s] rule_index [index:%x] vlan [vlan:%d] vlanhow[vlanhow:%s].	Station dhcp-option update.	
541056	Debug	[func:%s]: Add auth state, Station [mac:%m], authenticated [true:%d].	Station authenticated state.	
541057	Debug	[func:%s]: Station [mac:%m], essid [ssid:%s], cp-enable [yes:%d].	Print cp user.	
541058	Debug	[func:%s]: Add calea state, Station [mac:%m], intercept [yes:%d].	Print calea state add.	
541059	Debug	[func:%s]: Set calea state, Station [mac:%m], intercept [yes:%d].	Print calea state add.	
541060	Debug	[func:%s]: Send accounting ctx, client mac-[mac:%m], status-[status:%u], inocts-[inocts:%u], giginocts-[giginocts:%u], outocts-[outocts:%u], gigoutocts-[gigoutocts:%u], inpkts-[inpkts:%u], outpkts-[outpkts:%u], sesstim-[sesstim:%u], sessid-[sessid:%s], cpradip-[cpradip:%s].	AP update client from STM.	
541061	Debug	[func:%s]: Set accounting ctx, client mac-[mac:%m], status-[status:%u], inocts-[inocts:%u], giginocts-[giginocts:%u], outocts-[outocts:%u], gigoutocts-[gigoutocts:%u], inpkts-[inpkts:%u], outpkts-[outpkts:%u], sesstim-[sesstim:%u], sessid-[sessid:%s], cpradip-[cpradip:%s].	AP update client in CLI.	
541062	Debug	[func:%s]: Send accounting request, client mac-[mac:%m], status-[status:%u].	Send sta accouting request to STM.	
541063	Debug	Locate client send to member for [mac:%m], AP-ip: [ap_ip:%s].	AP locate client.	
541064	Debug	Reclassify ap type for: [mac:%m], phyType: [phy:%d], rapType: [rap:%d].	Reclassify ap type.	
541065	Debug	Reclassify ap type conf lvl for: [mac:%m], phyType: [phy:%d], rapType: [rap:%d], confLvl: [cl:%d].	Reclassify ap type conf level.	
541066	Debug	Reclassify sta type for: [mac:%m], phyType: [phy:%d], rapType: [rap:%d].	Reclassify sta type.	
541073	Debug	[func:%s]: Set FACEBOOK token, client [mac:%m], token [token:%s].	Facebook client token update.	
541074	Debug	[func:%s]: Add FACEBOOK token, client [mac:%m], token [token:%s].	Facebook client token update.	
541075	Debug	[func:%s]: receive ppsk req for client [mac:%m].	PPSK request.	
541076	Debug	[func:%s]: reply ppsk [ppsk:%s].	PPSK reply.	
541077	Debug	[func:%s]: v6 address [mac:%m] [ip:%s].	IPV6 address update.	
541078	Debug	[func:%s]: Send ppsk ctx, client mac-[mac:%m], is_valid-[is_valid:%u], nusers-[nusers:%u], username-[username:%s].	AP update client from STM.	
541079	Debug	[func:%s]: set ppsk ctx, client mac-[mac:%m], is_valid-[is_valid:%u], nusers-[nusers:%u], username-[username:%s].	AP update client in CLI.	
541080	Debug	[msg:%s]	This shows an internal clarity auth debug log	
541083	Debug	[func:%s]: compare accounting session start time, client mac-[mac:%m], time-[time:%u],ext_time-[ext_time:%u],name-[name:%s].	Compare accounting session start time between local data and old ap data.	
541084	Debug	[func:%s]: reset client information when it roam back, client mac-[mac:%m].	Reset client information when it roam back.	
541094	Debug	[func:%s]: Send client name string, client [mac:%m], client name [clent_name:%s].	Station name update.	
541095	Debug	[func:%s]: Send client hotst name string, client [mac:%m], client host name [clent_host_name:%s].	Station clietn host name update.	
541096	Debug	[func:%s]: Set client name string, client [mac:%m], name [client_name:%s].	Station name update.	
541097	Debug	[func:%s]: Set client host name string, client [mac:%m], host name [client_host_name:%s].	Station host name update.	
541098	Debug	[func:%s]: Set download-role cache, client [mac:%m], role-name [name:%s].	Cache download-role name.	
541099	Debug	[func:%s]: Add download-role cache, client [mac:%m], role-name [name:%s].	download-role cache update.	
542000	Debug	[msg:%s]	Not Available	
542001	Debug	[msg:%s]		
542003	Debug	VM: Clearing state for [client:%s]	Not Available	
542004	Debug	VM: [fn: %s] [line: %d] Error in handling SIP message opcode [opcode: %d].	Not Available	
542005	Debug	VM: [fn: %s] [line: %d]: Error in handling RTCP message	Not Available	
542006	Debug	VM: [fn: %s] [line: %d]: The pid [pid: %u] of ethernet frame recvd not IP. Processing Stopped.	Not Available	
542007	Debug	VM: [fn: %s] [line: %d]: The Tx protocol [protocol: %u] is neither UDP nor TCP. Processing Stopped.	Not Available	
542008	Debug	VM: [fn: %s] [line: %d]: RTCP packet parsing error	Not Available	
542009	Debug	VM: [fn: %s] [line: %d]: SIP TCP MSG [From: %s] ---> [To: %s]	Not Available	

542010	Debug	VM: [fn: %s] [line: %d]: Invalid Parameters Passed	Not Available	
542011	Debug	VM: [fn: %s] [line: %d]: Message buffer received is Not valid. Buffer Pointer [ptr:%p] Buffer Length [len: %d]	Not Available	
542014	Debug	VM: [fn: %s] [line: %d]: protocol message length [length: %d] not sufficient for further parsing	Not Available	
542015	Debug	VM: [fn: %s] [line: %d]: RTCP packet recv not valid, may be malformed	Not Available	
542016	Debug	VM: [fn: %s] [line: %d]: STM didn't initialize voip hash tables yet	Not Available	
542017	Debug	VM: [fn: %s] [line: %d]: RTCP Source [src: %s] entry not found	Not Available	
542018	Debug	VM: [fn: %s] [line: %d]: H.323 TCP MSG [From: %s] ---> [To: %s]	Not Available	
542022	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d]: current active calls: [no: %d]	Display current Vocera active call number on a badge	
542023	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] [state: %s] [dir: %d]	Display call state and direction for a to-be-disconnected call	
542024	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] active call idx [idx: %d]	Display current active call index of a badge	
542025	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] call [idx: %d] event [evt: %s] on state [state: %s]	Display event and call state change on a call	
542026	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] call [idx: %d] from [st1: %s] to [st2: %s]	Display prior and current state of a call	
542028	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] Closing upgrading session	Display Vocera ALG removing upgrading session	
542029	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d]: Incoming message [msg: %s]	Display incoming messages (other than ACK and PING) for Vocera ALG	
542030	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] registering [name: %s]	Display Vocera Ping (Register) message with client name	
542031	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] button touched [btn: %d]	Display Vocera Button message	
542032	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d]: current active calls: [call: %d], party no [party: %d]	Display active call number and party number in CallStart message	
542033	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] partyid [name: %s]	Display Vocera PartyID	
542034	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] hold state [hold: %d], idx [idx: %d], call_count [call: %d]	Display Vocera Call Hold state, call idx and call count	
542036	Debug	VOCERA: [ip: %s] [fn: %s] [ln: %d] registered [name: %s]	Display Vocera Ack for Ping (Register) message	
542037	Debug	VM: [fn: %s] [line: %d]: The call can't be admitted for [client: %s] because of CAC	Not Available	
542039	Debug	VM: [fn: %s] [line: %d]: SIP Message 100 Trying couldn't be sent for [client: %s]	Not Available	
542040	Debug	VM: [fn: %s] [line: %d]: SIP Message 100 Trying sent for [client: %s]	Not Available	
542041	Debug	VM: [fn: %s] [line: %d]: ReTxing same INVITE for [client: %s]	Not Available	
542042	Debug	VM: [fn: %s] [line: %d]: [client: %s] sending Re-Invite	Not Available	
542043	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 100 Trying	Not Available	
542044	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing 100 Trying	Not Available	
542045	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 180 Ringing	Not Available	
542046	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing 180 Ringing	Not Available	
542047	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 183 Session Progress	Not Available	
542048	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing 183 Session Progress	Not Available	
542049	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> PRACK	Not Available	
542050	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing PRACK	Not Available	
542051	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> UPDATE	Not Available	
542052	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing UPDATE	Not Available	
542053	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 200 OK	Not Available	
542054	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing 200 OK	Not Available	
542056	Debug	VM: [fn: %s] [line: %d]: 200 OK for Invite for [client: %s]	Not Available	
542058	Debug	VM: [fn: %s] [line: %d]: 200OK for Cancel received for [client: %s]	Not Available	
542059	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 401 UnAuthorized	Not Available	
542060	Debug	VM: [fn: %s] [line: %d]: Not able to find the session for [client: %s] while processing 401 UnAuth	Not Available	
542061	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 487 Request Terminated	Not Available	
542062	Debug	VM: [fn: %s] [line: %d]: Not able to find the session for [client: %s] while processing 487 ReqTerm	Not Available	

542063	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> ACK	Not Available	
542065	Debug	VM: [fn: %s] [line: %d]: Sending message to SiByte	Not Available	
542066	Debug	VM: [fn: %s] [line: %d]: Unable to create session list for [client: %s]	Not Available	
542067	Debug	VM: [fn: %s] [line: %d]: Unable to create session for [client: %s]	Not Available	
542068	Debug	VM: [fn: %s] Message received for visitor client, forwarding back	Mobility, visitor client message handling	
542069	Debug	VM: Client [client: %s] is deregistering.	VoIP client has de-registered with PBX	
542070	Debug	VM: [fn: %s] [line: %d]: [client: %s] ReTxing same REGISTER	Not Available	
542071	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> INVITE	Not Available	
542072	Debug	VM: [fn: %s] [line: %d]: Dummy Session Removed for [client: %s] while processing ACK	Not Available	
542073	Debug	VM: [fn: %s] [line: %d]: SIP error response not sent for [client: %s]	Not Available	
542075	Debug	VM: [fn: %s] [line: %d]: SDP length is [sdplen: %d]	Not Available	
542076	Debug	VM: [fn: %s] [line: %d]: SIP message is malformed, remaining length [remlength: %d]	Not Available	
542077	Debug	VM: [fn: %s] [line: %d]: SIP Hdr [hdr: %d] not found in message control block	Not Available	
542078	Debug	VM: [fn: %s] [line: %d]: Session created and inserted successfully for call id [cid: %s], [client: %s]	Not Available	
542079	Debug	VM: [fn: %s] [line: %d]: Responding with [status: %d] to [client: %s]	Not Available	
542081	Debug	VM: [fn: %s] [line: %d]: Tx params changed	Not Available	
542083	Debug	VM: [fn: %s] [line: %d]: SDP Length is [sdplen: %d]	Not Available	
542084	Debug	VM: [fn: %s] [line: %d] [client: %s] ---> REGISTER	Not Available	
542085	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> CANCEL	Not Available	
542086	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing CANCEL	Not Available	
542087	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 4xx	Not Available	
542088	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 5xx	Not Available	
542089	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> 6xx	Not Available	
542090	Debug	VM: [fn: %s] [line: %d]: Session not found for [client: %s] while processing 4xx/5xx/6xx messages	Not Available	
542091	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> MISC	Not Available	
542092	Debug	VM: [fn: %s] [line: %d]: [client: %s] ---> BYE	Not Available	
542093	Debug	VM: CFG [fn: %s] [line: %d] NULL profile [name: %s]	Cannot get the configuration profile.	
542094	Debug	VM: [fn: %s] [line: %d]: Flushing inactive calls for [client: %s]	Not Available	
542096	Debug	VM: [fn: %s] [line: %d]: RTCP BYE	Not Available	
542097	Debug	VM: [fn: %s] [line: %d]: RTCP APP	Not Available	
542098	Debug	VM: [fn: %s] [line: %d]: RTCP XR	Not Available	
542099	Debug	VM: [fn: %s] [line: %d]: Associated SAP Not found for Client [mac: %s]	Not Available	
542100	Debug	VM: [fn: %s] [line: %d]: SIP SDP IP address is [ip: %s]	Not Available	
542101	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Event [evt: %s] not applicable on state [st: %s]	NOE FSM receives not-applicable event	
542103	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Call [vcall: %p], event [evt: %s], from state [st1: %s] to state [st2: %s]	NOE call state update	
542104	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: event [evt: %s], state [st: %s]	NOE event invokes on a call	
542107	Debug	NOE: [fn: %s] [line: %d]: Incorrect message length	NOE incorrect message length	
542109	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Keepalive interval set to [time: %d]	NOE set keepalive interval	
542111	Debug	NOE: DBGRTRN [ip: %s]: [pkt: %s]: exp_seq [exp: %d], sent_seq [sent: %d], from [from: %d], size [len: %d]	NOE debug logs for retransmissions	
542112	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Set contact to [name: %s]	NOE log for setting contact	
542114	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Set caller to [name: %s]	NOE log for setting caller	
542115	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Update peer to [name: %s]	NOE log for updating peer	
542118	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Call [vcall: %p]	NOE identify a call pointer	
542120	Debug	NOE: [ip: %s]: set role [r1: %s] to [r2: %s]	NOE set client role for supplementary service	
542121	Debug	NOE: [ip: %s]: client RESET, cleanup seq_list	NOE client resets and cleans up sequence queue	
542122	Debug	NOE: [ip: %s]: Accumulated dialed string [no: %s]	NOE log for accumulated dialed string	

542123	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: call [vcall: %p]: [from: %s] -> [to: %s]	NOE identify call parties for a call	
542124	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: [key: %s]	NOE function key is pressed	
542130	Debug	NOE: [ip: %s]: [fn: %s] [line: %d]: Keepalive, count [no: %d]	Debugging log for NOE keepalive count	
542132	Debug	VM: [fn: %s] [line: %d]: [client: %s] not associated	Not Available	
542133	Debug	SCCP: [fn: %s] [line: %d]: Message incomplete	Debugging log for SCCP message incomplete	
542134	Debug	SCCP: [fn: %s] [line: %d]: Cannot allocate message info buffer	Debugging log for SCCP message allocation failure	
542135	Debug	SCCP: [fn: %s] [line: %d]: Handle [msg: %s] message	Debugging log for handling SCCP message	
542136	Debug	SCCP: [fn: %s] [line: %d]: Client State: [vc: %s]-[contact: %s] [state: %s]	Debugging log for SCCP client state	
542137	Debug	SCCP: [fn: %s] [line: %d]: session doesn't exist	Debugging log for SCCP session	
542138	Debug	SCCP: [fn: %s] [line: %d]: session list doesn't exist	Debugging log for SCCP session list	
542139	Debug	SCCP: [fn: %s] [line: %d]: session list [state: %s] [ip: %s], id [id: %d]	Debugging log for SCCP session state	
542140	Debug	SCCP: [fn: %s] [line: %d]: Keepalive interval set to [time: %d]	Debugging log for SCCP keepalive interval	
542141	Debug	SCCP: [fn: %s] [line: %d]: Alarm message received for in-call client	Debugging log for SCCP alarm message for in-call client	
542142	Debug	SCCP: [fn: %s] [line: %d]: Unregister message received while session is active. Not clearing session	Debugging log for SCCP unregister message received while session is active	
542143	Debug	SCCP: [fn: %s] [line: %d]: Client [ip: %s] extension set [contact: %s]	Debugging log for SCCP extension set	
542144	Debug	SCCP: [fn: %s] [line: %d]: Cannot create session list	Debugging log for SCCP session list creation failure	
542145	Debug	SCCP: [fn: %s] [line: %d]: Cannot create session	Debugging log for SCCP session creation failure	
542146	Debug	SCCP: [fn: %s] [line: %d]: Call State: [ip: %s]-[ext: %s] {[from: %s]==>[to: %s]}	Debugging log for SCCP valid call state	
542147	Debug	SCCP: [fn: %s] [line: %d]: Call State: [ip: %s]-[ext: %s] {[from: %s]==>[to: %s]} {Invalid}	Debugging log for SCCP invalid call state	
542148	Debug	SCCP: [fn: %s] [line: %d]: Keepalive for [ip: %s]-[ext: %s], count [no: %d]	Debugging log for SCCP keepalive count	
542149	Debug	SCCP: [fn: %s] [line: %d]: Media info incomplete. Cannot open port	Debugging log for SCCP media info incomplete failure	
542150	Debug	SCCP: [fn: %s] [line: %d]: [ip: %s]-[ext: %s] [st: %s]	Debugging log for SCCP CAC state	
542151	Debug	SCCP: [fn: %s] [line: %d]: Cannot handle [msg_id: %d] message	Debugging log for unknown SCCP message	
542152	Debug	SCCP: [fn: %s] [line: %d]: session state [ip: %s] ports [state: %s]: [rip: %s]:[rport: %d] - [tip: %s]:[tport: %d]	Debugging log for detail SCCP session state	
542153	Debug	DIGITMAP: [fn: %s] profile [name: %s] not found	Cannot find the specified profile	Contact technical support
542154	Debug	DIGITMAP: [fn: %s] [line: %d]: Null param	Lack of pass-in parameters	Contact technical support
542155	Debug	DIGITMAP: [fn: %s] [line: %d]: Final action: [action: %s]	Display the final action after digitmap matching	
542156	Debug	DIGITMAP: [fn: %s] [line: %d]: No rule matched.	There is no matching rule.	
542157	Debug	DIGITMAP: [fn: %s] [line: %d]: Rule matched, action [act: %s]	Display the action of a matching rule.	
542158	Debug	DIGITMAP: [fn: %s]: Pattern compiled [str: %s]	Digitmap pattern compiled.	
542159	Debug	DIGITMAP: [fn: %s]: Input has plus: [input: %s], Rule has plus: [rule: %s]	Input string and rule do not match on plus sign.	
542160	Debug	DIGITMAP: [fn: %s]: profile [name: %s]	Digitmap is cleaned up.	
542161	Debug	DIGITMAP: [fn: %s]: seq=[no: %d] pattern=[pat: %s] action=[act: %s]	Print each digitmap string.	
542162	Debug	DIGITMAP: [fn: %s] [line: %d]: Mismatch: Input string=[str: %s] type=[no: %d]	Rule mismatch	
542163	Debug	DIGITMAP: [fn: %s] Original=[orig: %s] Updated=[update: %s]	Remove illegal character from input string.	
543004	Debug	[msg:%s]		
543005	Debug	[func:%s]: [msg:%s]		
543006	Debug	Station [mac:%m] received [type:%s] on vlan [v:%d]		
543007	Debug	Station [mac:%m] associated on vlan pool [pool:%s]		
543008	Debug	Station [mac:%m] [str:%s] derived vlan		
543009	Debug	Station [mac:%m] received DHCP OFFER with old XID, start afresh		
543010	Debug	Station [mac:%m] [str:%s] mac entry		
543011	Debug	Station [mac:%m] [str:%s] DHCP OFFER received for station		
543012	Debug	Station [mac:%m] DHCP OFFER received on new vlan [v:%d]		
543013	Debug	Station [mac:%m] no memory for [str:%s]		
543014	Debug	Station [mac:%m] DHCP OFFER received on same vlan [v:%d]		
543015	Debug	Station [mac:%m] [str:%s] on vlan [vl:%d]		
543016	Debug	Station [mac:%m] received DHCP OFFER with differnt XID [xid:%d]		
543017	Debug	Station [mac:%m] [str:%s] schedule delete timer		

543018	Debug	Station [mac:%m] re-schedule delete timer		
543019	Debug	Station [mac:%m] [str:%s] delete now		
543020	Debug	Station [mac:%m] [str:%s]		
543021	Debug	Station [mac:%m] [str:%s] can not allocate memroy in MQ of size [sz:%d]		
543022	Debug	Station [mac:%m] received MQ msg with type [t:%d] vlan [v:%d] packet length [l:%d]		
543023	Debug	Station [mac:%m] received mmoblity vlan change ack [ok:%d]		
543024	Debug	Station [mac:%m] DISCOVER with new xid received old XID [o:%d] new XID [n:%d]		
543025	Debug	Station [mac:%m] REQUEST received on vlan [v:%d] but new vlan is [n:%d], drop packet		
543026	Debug	Station [mac:%m] NAK received on different vlan [v:%d] station vlan [s:%d], drop packet		
543027	Debug	Station [mac:%m] send RELEASE on vlan [v:%d], station vlan [s:%d]		
543028	Debug	Station [mac:%m] datapath notification for vlan change to [v:%d]		
543029	Debug	Station [mac:%m] incorrect vlan update from datapath, vlan [v:%d] should have been [c:%d]		
543030	Debug	Station [mac:%m] [str:%s] send message queue msg to tx thread		
543031	Debug	Station [mac:%m] associated on a vlan pool which has at most one vlan		
544000	Debug	[func:%s] [line:%d] [msg:%s]	User debug messages for DPI MGR	
599800	Debug	[function:%s], [file:%s]:[line:%d]: [error:%s]	This is an internal user debugging log.	
509000	Emergency	FIPS Emergency: [msg:%s]	This is a FIPS emergency log in user module.	
500000	Error	Station [mac:%m], [ip:%s]: Mobile IP PROXY FSM received unexpected event [event:%s]: previous state: [cs:%s], current state: [ns:%s]	Proxy Mobile IP state machine for a particular user received an expected event	Contact technical support
500031	Error	Station [mac:%m], [ip:%s]: Received error from data path adding bridge entry, error code [sibyte_error:%d]	An unexpected error happened updating the port or tunnel for a station in the data path	Contact technical support
500033	Error	Station [mac:%m], [ip:%s]: Received error from data path adding home bridge entry, error code [sibyte_error:%d]	An unexpected error happened updating the home bridge entry for a station in the data path	Contact technical support
500038	Error	Station [mac:%m], [ip:%s]: Received error from data path updating bridge entry, error code [sibyte_error:%d]	An unexpected error happened updating the port or tunnel for a station in the data path	Contact technical support
500040	Error	Station [mac:%m], [ip:%s]: Received error from data path updating home bridge entry, error code [sibyte_error:%d]	An unexpected error happened updating the home bridge entry for a station in the data path	Contact technical support
500046	Error	[line:%d] Station [mac:%m], [ip:%s]: Received error from the data path deleting bridge entry for local station on vlan [vlan:%d] v6-vlan [v6_vlan:%d], error code [sibyte_error:%d]	An unexpected error happened deleting the bridge entry for a station in the data path	Contact technical support
500048	Error	[line:%d] Station [mac:%m], [ip:%s]: Received error while deleting home bridge entry for local station on vlan [vlan:%d] v6-vlan [v6_vlan:%d], error code [sibyte_error:%d]	An unexpected error happened deleting the home bridge entry for a station in the data path	Contact technical support
500050	Error	Station: [mac:%m], [ip:%s]: mobility state machine/type/event: [ty:%s] Previous State: [pst:%s] Current State: [cst:%s] at function [fn:%s] line [ln:%d]	Mobile client state machine dump in event mobility hit corner case	
500060	Error	[func:%s] [line:%d] Station [mac:%m], [ip:%s]: Mobileip failed to synchronize auth about user state, error [papi_error:%d]	Mobile IP failed to synchronize its state with the Authentication module	Contact technical support
500081	Error	Station [mac:%m], [ip:%pI4]: mismatches with home addr [sta_home_addr:%s] found in Registration Request/Discovery received from COA [coa:%s] at line [ln:%d]	Mobile client IP at HA does not match incoming registration request IP address from FA, it implies client IP is changed and HA was not aware. HA will delete this client	
500101	Error	Station [mac:%m], [ip:%s]: FA FSM receive event: [evt:%s] previous: [cur:%s], current: [nxt:%s] !!! NO STATE !!!	Visitor FA state machine reached bad state which state machine cannot handle	Contact technical support
500114	Error	Station [mac:%m], [ip:%s]: Failed to create or update auth state for new visitor [hwaddr:%m] [staip:%pI4], error [er:%d]	Mobility failed to update/create client state in auth	Contact technical support
500115	Error	Station [mac:%m], [ip:%s]: FAILED to create tunnel from local address [la:%pI4] to remote HA address [rha:%pI4]	Mobility failed to create L2-GRE tunnel between HA-FA	Contact technical support
500119	Error	Station [mac:%m], [ip:%s]: Received error while creating bridge entry for visitor, error [er:%d]	>Mobility failed to create bridge entry for visitor in data plane	Contact technical support

500129	Error	Station [mac:%m], [ip:%s]: Failed to create or update auth state for visitor [hwaddr:%m] [staip:%pI4] at line [ln:%d], error [er:%d]	Mobility is unable to update/create state in auth. This should not happen, contact technical support.	
500133	Error	Station [mac:%m], [ip:%s]: Error deleting bridge entry for visitor	Error deleting bridge entry for visitor in Data plane	Contact technical support
500135	Error	Station [mac:%m], [ip:%s]: Received error while deleting bridge entry for visitor, error [er:%d]	Error deleting bridge entry for visitor in Data plane	Contact technical support
500201	Error	Station [mac:%m], [ip:%s]: HA FSM recv event: [evt:%s] previous: [cur:%s], current: [nxt:%s] !!! NO STATE !!!	Binding HA state machine reached bad state which state machine cannot handle. This should not happen, contact technical support.	
500207	Error	Station [mac:%m], [ip:%s]: Failed to create auth state for binding [hwaddr:%m] [staip:%pI4], error [er:%d]	HA Mobility failed to update/create client state in authentication module	Contact technical support
500208	Error	Station [mac:%m], [ip:%s]: FAILED to create tunnel from local address [addr:%pI4] to remote COA address [coa:%pI4]	Mobility failed to create L2-GRE tunnel between HA-FA	Contact technical support
500212	Error	Station [mac:%m], [ip:%s]: Received error from sibyte for bridge add/update for binding on vlan [vl:%d], error [er:%d]	HA received error updating bridge entry for Binding in data path	Contact technical support
500216	Error	Station [mac:%m], [ip:%s]: Failed to update auth state for binding [hwaddr:%m] [ipaddr:%pI4], error [er:%d]	HA Mobility failed to update/create client state in auth	Contact technical support
500218	Error	Station [mac:%m], [ip:%s]: FAILED to create tunnel from local address [addr:%pI4] to remote COA address [coa:%pI4]	Mobility failed to create L2-GRE tunnel between HA-FA	Contact technical support
500226	Error	Station [mac:%m], [ip:%s]: Received error while deleting bridge entry for binding on vlan [vl:%d], error [er:%d]	HA mobility received error while deleting bridge entry in data path	Contact technical support
500228	Error	Station [mac:%m], [ip:%s]: Failed to delete auth state for binding [hwaddr:%m] [staip:%pI4], error [er:%d]	HA Mobility failed to delete client authentication state	Contact technical support
500403	Error	Station [mac:%m], [ip:%s]: action [act:%s] message type [mtype:%s] send to Auth failed at line [line:%d]	Mobility failed to send user create/update/delete message to authentication module	Contact technical support
500451	Error	Station [mac:%m], [ip:%s]: Cannot add bridge entry for binding	Mobility failed to add Bridge entry for Binding in data plane	Contact technical support
500454	Error	Station [mac:%m], [ip:%s]: Cannot add bridge entry for visitor line [ln:%d]	Mobility failed to add Bridge entry for visitor in data plane	Contact technical support
500457	Error	Station [mac:%m], [ip:%s]: Cannot add bridge entry for local station	Mobility failed to add Bridge entry for client	Contact technical support
500458	Error	Station [mac:%m], [ip:%s]: Cannot add home VLAN bridge entry for local station	Mobility failed to add Bridge entry on home vlan	Contact technical support
500459	Error	Station [mac:%m], [ip:%s]: Cannot delete datapath bridge entry for station on vlan [vl:%d] v6-vlan [v6_vlan:%d]	Mobility failed to delete data plane Bridge entry	Contact technical support
500523	Error	Tunnel [addr:%pI4] for VRRP [vrrp:%pI4]: Can't add tunnel entry, maximum tunnel limit reached	Can not add any more tunnel, max limit reached	
500524	Error	Failed to add active domain [dom:%s], HAT/Tunnel count exceeds [ent:%d]	Failed to add active domain	
500525	Error	HAT [addr:%pI4] Failed to add hat entry, HAT/Tunnel count exceeds [ent:%d]	Failed to add hat entry	
501051	Error	Station [sta:%m]: Dynamic BSS tunnel could not be setup for bssid [bss:%m]		
501053	Error	Station [sta:%m]: STA UP sent to wrong UAC for essid [ess:%s]		
501074	Error	wifi_deauth_sta: bad data, dropping. mac: [mac:%m] bssid: [bssid:%m]		
507023	Error	[msg:%s]	This log indicates that we encountered an internal system error	Contact your support provider
509003	Error	FIPS Error: [msg:%s]	This is a FIPS error log in user module.	
520002	Error	Authentication server request Timeout, username=[username:%s] userip=[userip:%s] usermac=[usermac:%s] servername= [servername:%s] server-group=[group:%s] serverip=[serverip:%s] bssid=[bssid:%s] apname=[apname:%s]	This shows request timeout for authentication server.	
520003	Error	Accounting server request Timeout, username=[username:%s] userip=[userip:%s] usermac=[usermac:%s] servername= [servername:%s] server-group=[group:%s] serverip=[serverip:%s] bssid=[bssid:%s] apname=[apname:%s]	This shows request timeout for accounting server.	
520010	Error	[func:%s] ([line:%u]): rtts user=[user:%m] Failed to add VSA for throughput [tput:%d]		
520013	Error	[msg:%s]	This shows an internal clarity auth error log	
522040	Error	Error setting role for user [ipuser:%s]-[mac:%s]-[username:%s] role [ro:%s] err [error:%s].	This shows an internal error message	
522041	Error	MAC=[mac:%s] IP=[ip:%s] Derived unknown VPN role '[r:%s]' from server rules. Server=[s:%s], authentication=[auth:%s]	System derived an unknown role from server derivation rules. User will be assigned default role for authentication	Please check if all the derived roles are configured in configuration file.

522067	Error	Role for user [user:%s]-[mac:%s]-[name:%s] set to 'logon' since configured role '[role:%s]' not found.	This shows an internal debug message	
522135	Error	Internal Error : while retriving AAA profile for IP: [ipaddr:%s], MAC: [macaddr:%s].	This shows an internal debug message	
522159	Error	Event [ev:%s] not handled in role Derivation for user [mac:%s].	This shows an internal debug message	
522248	Error	User age timer add failed for user MAC [mac: %s].	This shows an error happened during timer creation	
522273	Error	WW roam failed for [mac:%s] err [e:%d]	This shows an error happened for a user during wireless-wired roaming	
522274	Error	Mgmt User Authentication failed. username=[username:%s] userip=[userip:%s] servername=[servername:%s] serverip=[serverip:%s]	This shows mgmt user authentication failure	
522276	Error	Authentication Server Out Of Service while serving request. servername=[servername:%s] serverip=[serverip:%s] username=[username:%s] userip=[userip:%s] usermac=[usermac:%s] bssid=[bssid:%s] apname=[apname:%s]	This shows user authentication failure	
522279	Error	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] Cannot be assigned downloadable role, role with same name exists in config	User cannot be assigned role derived from CPPM VSA as role with same name already present in configuration	
522280	Error	MAC=[mac:%s] [dormant:%s] Dldb Role: [r:%s] Cannot be assigned downloadable role, role is in error state	User cannot be assigned role derived from CPPM VSA as the role is in an error state	
522288	Error	Auth GSM : MAC_USER publish failed for mac [m: %s] result [r: %s]	This shows an internal user error message	
522293	Error	Auth GSM : MAC_USER lookup failed for mac [m: %s] result [r: %s]	This shows an internal user error message	
522294	Error	Auth GSM : MAC_USER notify failed for mac [m: %s] vlan [v: %d] result [r: %s]	This shows an internal user error message	
522300	Error	Auth GSM : DEV_ID_CACHE publish failed for mac [m: %s] dev-id [s: %s]([ig: %d]) result [r: %s]	This shows an internal user error message	
522302	Error	Auth GSM : USER publish failed for mac [m: %s] uuid [u: %s] repkey [rep:%d] result [r: %s]	This shows an internal user error message	
522306	Error	Auth GSM : DEV_ID_CACHE ager failed for mac [m: %s] result [r: %d]	This shows an internal user error message	
522310	Error	[string:%s]	This shows an internal error message	
522312	Error	MAC=[mac:%s] [Dormant:%s] Dldb Role: [r:%s] Cannot be assigned downloadable role, role has been cleaned up	User cannot be assigned role derived from CPPM VSA as the role is in cleaned-up state	
522313	Error	MAC=[mac:%s] ingress [ingres:%x] ([usr_dest:%s]), u_encr [u_encr:%d], m_encr [m_encr:%d], slotport [slot:%x] [port:%s], type: [type:%s], FW mode: [fw_mode:%u], AP IP: [apip:%s] is invalid	This shows an internal user error message	
522314	Error	Role=[role: %s] deleted on conductor, setting L2 role to [new_role: %s] for user=[mac: %s]	This shows an internal error message	
522319	Error	Auth GSM : MAC_USER lookup failed for mac [m: %s] result [r: %s]	This shows an internal user error message	
522321	Error	Auth GSM : USER publish failed for mac [m: %s] [uuid: %s] [rep_key: %d] result [r: %s]	This shows an internal user error message	
522323	Error	Auth GSM : MAC USER publish failed for mac [m: %s] [rep_key: %d] result [r: %s]	This shows an internal user error message	
522325	Error	Auth GSM : USER repkey change failed for mac [m: %s] [uuid: %s] [rep_key: %d] result [r: %s]	This shows an internal user error message	
522327	Error	Auth GSM : MAC USER change repkey failed for mac [m: %s] [rep_key: %d] result [r: %s]	This shows an internal user error message	
522329	Error	Auth GSM : STA change repkey failed for mac [m: %s] [rep_key: %d] result [r: %s]	This shows an internal user error message	
522332	Error	MAC=[mac:%s] Dldb Role cannot be assigned cached downloadable role, role not available	User cannot be assigned role derived from CPPM VSA as the cached-role is not available	
522339	Error	MAC=[mac:%s] Dldb Role: [r:%s] Invalid downloadable role, role name length invalid	User cannot be assigned role derived from CPPM VSA as role name is too long	
522350	Error	MAC=[mac:%s] Dormant Dldb Role: [r:%s] CPPM server [name:%s] not found	Downloadable role cannot be downloaded from CPPM server as server configuration not found.	
522355	Error	Aruba-MPSK-Passphrase VSA not received for MPSK user - MAC [mac:%s]	This shows an internal user error message	
522356	Error	Aruba-MPSK-Passphrase VSA decryption failed for MPSK user - MAC [mac:%s]	This shows an internal user error message	
522357	Error	Aruba-MPSK-Passphrase length is invalid for MPSK user - MAC [mac:%s]	This shows an internal user error message	
524005	Error	Invalid action :[file:%s],[func:%s],[line:%d],[action:%d]	This shows internal debug messages.	
524006	Error	[file:%s], [func:%s],[line:%d],cur=0x[cur:%x],end=0x[end:%x]	This shows internal debug messages.	

524007	Error	[file:%s], [func:%s],[line:%d], realloc size invalid, tot=:[tot:%d],certlen=:[len:%d]	This shows internal debug messages.	
524008	Error	[file:%s], [func:%s],[line:%d], offset should be zero but is =[offset:%d]	This shows internal debug messages.	
524009	Error	[file:%s], [func:%s],[line:%d] Sanity check for first/Only cert chunk failed. Ignoring cert chunk.	This shows internal debug messages.	
524010	Error	[file:%s], [func:%s],[line:%d] malloc size:=[total:%d] failed	This shows internal debug messages.	
524019	Error	Invalid MPPE recv-key length:[len:%d]	This shows internal debug messages.	
524020	Error	Unknown protocol/Opcode [proto:%2X] [opcode:%2X] from the Datapath	This shows internal debug messages.	
524021	Error	[string:%s]	This shows internal debug messages.	
524022	Error	Radius Shared secret is NULL, NASIP = [nasip:%s], Radius Server [srvip:%s]	This shows internal debug messages.	
524023	Error	Error decoding LEAP key (code=[code:%d])	This shows internal debug messages.	
524024	Error	Error decoding MPPE recv-key (code = [code:%d])	This shows internal debug messages.	
524025	Error	Could not create the stateful config entry, dropping the request. NASIP=:[nasip:%s],[srvip:%s]	This shows internal debug messages.	
524026	Error	Dropping the radius request to=:[srvip:%s]	This shows internal debug messages.	
524027	Error	Error decoding MPPE send-key (code = [code:%d])	This shows internal debug messages.	
524028	Error	Invalid MPPE send-key length:[len:%d]	This shows internal debug messages.	
524030	Error	Invalid Radius Code [radcode:%d]	This shows internal debug messages.	
524043	Error	[string:%s]: FT mic=[string1:%s]	This shows internal debug messages.	
524044	Error	AES-GCM key size should be either [key1:%d] or [key2:%d]	This shows internal debug messages.	
524046	Error	Station UP failed for station [str:%s] [str1:%s]	This shows internal debug messages.	
524056	Error	Invalid radius code	This shows internal debug messages.	
524057	Error	Dropping the radius packet for stateful dot1x processing	This shows internal debug messages.	
524058	Error	No Valid NAS IP dropping the request	This shows internal debug messages.	
524059	Error	NAS IP address didn't match the NASIP attribute	This shows internal debug messages.	
524060	Error	No Valid Calling Station ID dropping the request	This shows internal debug messages.	
524061	Error	Could not create a new user entry	This shows internal debug messages.	
524062	Error	Failed to add to the radius request list	This shows internal debug messages.	
524063	Error	Dropping radius response to AP	This shows internal debug messages.	
524064	Error	No matching request fot the response..dropping the pkt	This shows internal debug messages.	
524065	Error	User was deleted before the response came in	This shows internal debug messages.	
524066	Error	No dot1xctx for this response	This shows internal debug messages.	
524067	Error	Failed to process EAP packet from backend	This shows internal debug messages.	
524068	Error	AES-GCM key setting is allowed only for Tunnel mode VAP's	This shows internal debug messages.	
524094	Error	[func:%s](): System Error - No enugh buffer space, expected:[exp:%zu] octets, buffer-size:[bs:%zu] octets	This indicates No enough buffer space error in the system.	
524127	Error	[func:%s]():[line:%u]: MAC:[mac:%s] GSM: Failed to activate Key-cache object. Error:[error:%s]	This shows internal debug messages.	
524128	Error	[func:%s](): MAC:[mac:%s] GSM: Failed to publish Key-cache object. Error:[error:%s]	This shows internal debug messages.	
524130	Error	[func:%s](): MAC:[mac:%s] GSM: Failed to delete Key-cache object. Error:[error:%s]	This shows internal debug messages.	
524132	Error	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s] GSM: Failed to activate PMK-cache object. Error:[error:%s]	This shows internal debug messages.	
524135	Error	[func:%s](): MAC:[mac:%s] BSS:[bssid:%s] GSM: Failed to delete PMK-cache object. Error:[error:%s]	This shows internal debug messages.	
524137	Error	[func:%s]():[line:%u]: MAC:[mac:%s] GSM: Failed to get key-cache object.	This shows internal debug messages.	
524138	Error	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s] GSM: Successfully deleted PMK-cache object.	This shows internal debug messages.	
524143	Error	Failed to decode vendor attributes	This shows internal debug messages.	
524144	Error	[func:%s]():[line:%u]: Failed to delete oldest keycache entries. Error:[error:%s]	This shows internal debug messages.	
524145	Error	[func:%s]():[line:%u]: Failed to delete oldest pmkcache entries. Error:[error:%s]	This shows internal debug messages.	
524146	Error	[func:%s]():[line:%u]: MAC:[mac:%s] Failed to set GSM ager node. Error:[error:%u]	This shows internal debug messages.	
524147	Error	[func:%s]():[line:%u]: MAC:[mac:%s] BSS:[bssid:%s] Failed to set GSM ager node. Error:[error:%u]	This shows internal debug messages.	

524151	Error	[func:%s]():[line:%u]: MAC:[mac:%s] Failed to delete GSM ager node. Error:[error:%u]	This shows internal debug messages.	
524152	Error	[func:%s]():[line:%u]: MAC:[mac:%s] Failed to delete GSM ager node. Error:[error:%u]	This shows internal debug messages.	
524159	Error	[func:%s] ([line:%u]): rtts user=[user:%m] Failed to add VSA for throughput [tput:%d]		
524161	Error	[func:%s](): PTK-Length=[len:%zu] is invalid	Invalid PTK-Length is used while derive FT-PTK	
525007	Error	[func:%s]([line:%d]): Data Inconsistence Error.(mac=[mac:%m] bssid=[bssid:%m] [field1:%s]=[value1:%u] [field2:%s]=[value2:%u])	This indicates inconsist data to be processed	
525105	Error	OWE: Failed to acquire Diffie-Hellman Group Helper for Station=[mac:%m] BSS=[bss:%m] DH-Group=[grp:%u].	This indicates system can't acquire D-H group helper for an OWE client.	
527505	Error	[func:%s] [line:%d] [msg:%s]	User debug error messages for AirGroup	
541012	Error	[func:%s]: [line:%d]: find client-[mac:%m] fail.	Station sync.	
541017	Error	[func:%s]: parse tlv ret-[ret:%d] mac-[mac:%m] fail.	Station sync.	
541018	Error	[func:%s],[line:%d]: could not find client-[mac:%m].	AP is looking up station.	
541021	Error	sta [mac:%m] - fail to find wlan profile for ssid-[ssid:%s].	Station sync.	
541028	Error	[func:%s],[line:%d]: could not get stm ip for client-[client:%m], essid-[essid:%s].	AP send portal auth acl to STM.	
541046	Error	[func:%s]: Unexpected sta-[mac:%m] lkup resp from [ip:%s],	Unexpected sta lkup resp.	
541081	Error	[msg:%s]	This shows an internal clarity auth error log	
542095	Error	VM: [fn: %s] [line: %d]: Memory allocation failure	System failed to allocate memory at the specified location	Use "show memory", "show memory stm" and "show process" commands to monitor memory usage. Contact customer support if problem persists.
542164	Error	[msg:%s]	User related error messages logged in UCM.	
543000	Error	[msg:%s]	Unexpected condition occurred in the dhcpdproxy process	
543001	Error	[func:%s]: [msg:%s]	Unexpected condition occurred in the dhcpdproxy process	
500004	Info	Station [mac:%m], [ip:%s]: Created mobility state for new station	Created mobility state for the station. This state will be kept as long as the station will be active on this switch or roaming. This state holds the station mobility state.	
500006	Info	Station [mac:%m], [ip:%s]: No Mobility timeout, Mobility (only) station state will be deleted	When a station cannot be provided with mobility service, we add a temporary bridge entry in the data path for this station so that it can get service without mobility. This message means that this entry will be deleted. The mobility status of this station will be evaluated again on the frame we receive from it and it may either get mobility service if the situation was corrected of another temporary bridge entry.	
500007	Info	Station [mac:%m], [ip:%s]: Mobility stale entry timeout, station state will be deleted	When a station enter stale state (due to 802.11 Disassociation, HA went down etc) a configurable timer is started which deletes the client upon its expiry. This is an intermediate state used to hold client until we hear from it again.	
500008	Info	Station [mac:%m], [ip:%s]: De-Auth timeout, STM will de-auth client to force renew its DHCP IP	When a station uses Stale IP address (that may happen due to network topology change e.g. HA went down and FA does not have access to client Home network or a AP failover happened client's IP address is no longer valid in new environment) it goes to "No mobility service state" where it gets add a temporary bridge entry in the data path. As soon as mobility detects station is using stale IP it starts De-auth timer and before its expiry if client didn't recovered on its own(get new IP) it is De-authenticated to force renew its IP address that fits in new environment.	
500009	Info	Station [mac:%m], [ip:%s]: MIP message timeout, current state [cs:%s], mobility will terminate stale state of the user	When mobility state machine does not receive ack from auth module; this timer fires which terminates mobility service of user in an effort to start a brand new state machine	

500013	Info	Station [mac:%m], [ip:%s]: MIP message timeout triggered, current state [cs:%s], mobility will terminate stale state of the user	When mobility state machine does not receive ack from auth module; Proxy Timeout is triggered on auth user delete (idle-timeout) which terminates mobility service of user in an effort to start a brand new state machine	
500020	Info	Station [mac:%m], [ip:%s]: No association information was received	No association information was received by Mobile IP prior to processing a mobility event	Contact technical support
500021	Info	Station [mac:%m]: Unexpected Disassociation message from assoc bssid [bssid:%m] current bssid [bssid2:%m] line [ln:%d]	Received a de-association message from station management but the bssid does not correspond to the last known location for this station.	
500052	Info	Visitor: [mac:%m], [ip:%s]: Sibyte Session Table Update to Destination Tunnel-id [tunn:%d] failed	Visitor session table update failed, This should not happen, please contact technical support	
500070	Info	Station [mac:%m], [ip:%s]: Cannot find a local home vlan for station, check VLAN assignment and HAT line [ln:%d]	No VLAN can be found matching the IP address that the station is currently using. This may be because the station was previously in another network or because the Home Agent Table for the mobility domain is not properly configured.	
500072	Info	Station [mac:%m], [ip:%s]: local VLAN not matching HAT	The station IP address seems to belong to any VLAN or match any HAT entry. This may mean that the HAT for the mobility domain is misconfigured or that the station previously joined another network.	
500073	Info	Station [mac:%m], [ip:%s]: HA discovery did not find a remote session: THIS will be the home switch	When a new station associates to a switch, we perform HA discovery to find out if this station has an ongoing session on any of the switches that matches the station IP in the HAT. This means that no remote switch had a session, so this switch will become the home switch for the station	
500074	Info	Station [mac:%m], [ip:%s]: HA discovery failed ===> [reason:%s]	The station IP Address does not match any entry in the HAT or any VLAN. The station will not get service until it renews its IP address	
500077	Info	Station [mac:%m], [ip:%s]: Cannot find Home Agent; Mobility domain is misconfigured or station has an unexpected IP address	When a station associates with a switch and we have no prior mobility state for this station, we look at the station IP address to locate its HA. The lookup is performed in the active HAT (Home Agent Table), which is the aggregation of all the HATs of the active mobility domains on a switch. This message means that no matching entry was found in the HAT for this station. This maybe because the station has recently joined another network and is requesting an address from that network in DHCP. Or if this address is part of the Enterprise WLAN, it may mean that a subnet is missing from the HAT configuration.	
500078	Info	Station [mac:%m], [ip:%s]: Associated on a new ESSID [ness:%s], previous ESSID [pess:%s] at line number [ln:%d]	Mobile client ESSID is changed, moblity services will be terminated	
500082	Info	Station [mac:%m], [ip:%s]: State current [cs:%s] Previous [ps:%s] Roaming [rs:%s] roamed to No Mobility ESS [essid:%s], service will be terminated or updated based on roaming from mobile to non-mobile ESS and vice versa	Mobile client is associated to ESSID on which mobile ip service is Disabled	
500103	Info	Station [mac:%m], [ip:%s]: Received a registration reply with lifetime 0	FA received registration reply with lifetime of 0 seconds for visitor. This should not happen, contact technical support.	
500108	Info	Station [mac:%m], [ip:%s]: Received HA discovery replies from all potential HA; Aborting discovery; will assigning a HA	FA is unable to locate HA who owns this client. FA now will try to assign HA by itself.	
500110	Info	Station [mac:%m], [ip:%s]: Cannot find a Home Agent address in Home Agent Table (HAT)	Possibly a misconfiguration of mobility domian/HAT, mobility is unable to locate candidate HA(s) for this client.	
500126	Info	Station [mac:%m], [ip:%s]: Error sending Registration Revocation Acknowledgement for visitor	FA is unable to send registration revocation ack to HA. Check HA-FA network conectivity. This should not happen, please contact technical support	
500157	Info	Visitor: [mac:%m], [ip:%s] Previous: [ps:%s] Current State: [cs:%s] Proxy MN: [prxip:%s] Home agent: [ha:%s] HomeVlan: [hv:%d] Current Vlan: [cv:%d] event: [evt:%s] at line [ln:%d]	FA state machine information dump to track visitor moves.	

500159	Info	Visitor: [mac:%m], [ip:%s]: Failed to assign HA	FA is unable to assign HA for this visitor. Probably due to misconfiguration or network connectivity issues. This should not happen, please contact techincal support.	
500163	Info	Race noticed for visitor: [mac:%m], [ip:%s] Previous: [ps:%d] Current State: [cs:%d] Proxy MN: [prxip:%s] Home agent: [ha:%s] HomeVlan: [hv:%d] Current Vlan: [cv:%d] at [fn:%s] [ln:%d]	FA state machine detected race condition for particular visitor	
500167	Info	Race noticed for visitor: [mac:%m] at [fn:%s] [ln:%d]	FA state machine detected race condition for particular visitor	
500252	Info	Station [mac:%m], [ip:%s]: Binding will be revoked due to VRRP ID [vrid:%d] failover	VRRP fail over happened, all binding will be revoked and deleted. Client(s) might experience connecitivty loss until new HA is selected.	
500253	Info	Binding: [mac:%m], [ip:%s]: Previous: [ps:%s] Current State: [cs:%s] Previous COA: [pfa:%s] Current COA: [ccoa:%s] HomeVlan: [hv:%d] Current FA Vlan: [cv:%d] event: [evt:%s] at line [ln:%d]	HA state machine information dump to track binding moves.	
500401	Info	Station [mac:%m], [ip:%s]: Receive User delete from Auth, no state for this user	Mobility received delete user from Auth, mobile client will be deleted	
500510	Info	HAT [addr:%pI4]: delete datapath hat entry	Mobility delete Hat entry in datapath	
500521	Info	HAT [addr:%pI4]: add datapath hat entry	Mobility add Hat entry in datapath	
500522	Info	bulk add datapath hat entry	Mobility bulk add Hat entry in datapath	
500991	Info	Station [mac:%m], [ip:%s]: Manual delete trigerred; Current State [cs:%s], Previous state [ps:%s] del pending [dp:%x] events per second [eps:%d]	Mobile client stale entry delete trigger manually; mobility services for this client will be Terminated	
500992	Info	Station [mac:%m]: Assoc event triggered; Current State [cs:%s], Previous State [ps:%s], HA discovery triggered [ha:%d] event [es:%s] at line [ln:%d]	Mobile client associated and an event was triggered	
500993	Info	Station [mac:%m]: Assoc event ignored; Current State [cs:%s], Previous State [ps:%s], HA discovery triggered [ha:%d] at line [ln:%d]	Mobile client associated and event was ignored	
501035	Info	Station [sta:%m]: DA [da:%m] not found trying to disassociate to BSSID [bss:%m] on AP [name:%s]		
501137	Info	Source: [sa:%m] Disabled aggregation on AP [ip:%P]-[bssid:%m]-[name:%s]; WEP or TKIP encryption in use		
501138	Info	VPOOL: [sa:%m] Assign Vlan [vlan:%d] on BSSID [bssid:%s] (remain=[remain:%d], reason=[res:%s])	This message indicates that a VLAN was assigned to a client from the Pool	
501139	Info	VPOOL: [sa:%m] Release Vlan [vlan:%d] for BSSID [bssid:%s] (remain=[remain:%d], reason=[res:%s])	This message indicates that a VLAN was released to VLAN pool for future reuse	
501210	Info	XML_API: add user, mac [mac:%m], ip [ip:%s], name [name:%s], role [role:%s], session_timeout [st:%d]	This log indicates that we are receiving xml api.	
501211	Info	XML_API: internal user auth, mac [mac:%m]	This log indicates that we are receiving xml api.	
505000	Info	[string:%s]	This shows an information message in Cert Mgr in user logs.	
509006	Info	FIPS Info: [msg:%s]	This is a FIPS info log in user module.	
522005	Info	MAC=[mac:%s] IP=[ip:%s] User entry deleted: reason=[r:%s] clusterflag [cf:%d]	L3 user entry deleted	
522006	Info	MAC=[mac:%s] IP=[ip:%s] User entry added: reason=[r:%s]	L3 user entry created	
522007	Info	MAC=[mac:%s] IP=[ip:%s] Session time set to [tout:%d] seconds from server attribute	Session time derived from server attribute	
522012	Info	MAC=[mac:%s] IP=[ip:%s] IP UP: outerIP=[ip2:%s] tunnels=[n:%d]	L3 entry created for tunnelled user	
522013	Info	MAC=[mac:%s] IP=[ip:%s] IP DN: outerIP=[ip2:%s] tunnels=[n:%d]	L3 entry deleted for tunnelled user	
522015	Info	MAC=[mac:%s] IP=[ip:%s] Remove Bridge Entry	User Bridge Entry was removed	
522016	Info	MAC=[mac:%s] IP=[ip:%s] Derived role '[r:%s]' from Aruba VSA	User was assigned a role derived from Vendor Specific Attributes returned by authentication server	
522017	Info	MAC=[mac:%s] IP=[ip:%s] Derived role '[r:%s]' from server rules: server-group=[sg:%s], authentication=[auth:%s]	User role was derived from server derivation rules and attributes returned by authentication server	
522019	Info	MAC=[mac:%s] IP=[ip:%s] Derived role '[r:%s]' at pos [pos:%d] from user rules	System derived a role from user derivation rules	
522020	Info	MAC=[mac:%s] IP=[ip:%s] Derived unknown role '[r:%s]' from user rules	System derived an unknown role from user derivation rules. User will be assigned default role for AAA profile	
522021	Info	MAC=[mac:%s] Derived VLAN '[v:%d]' from Aruba VSA	User VLAN was derived from Vendor Specific Attributes returned by authentication server	

522022	Info	MAC=[mac:%s] Derived VLAN [v:%d] from Tunnel attributes	User VLAN was derived from Tunnel attributes returned by authentication server	
522023	Info	MAC=[mac:%s] Derived VLAN [v:%d] from server rules: server-group=[sg:%s]	User VLAN was derived from server derivation rules and attributes returned by authentication server	
522024	Info	MAC=[mac:%s] Derived VLAN [v:%d] from user rules	System derived a VLAN from user derivation rules	
522025	Info	MAC=[mac:%s] IP=[ip:%s] MAC spoof from MAC=[m:%s]	System detected MAC spoofing. Frame was dropped	
522026	Info	MAC=[mac:%s] IP=[ip:%s] User miss: ingress=[i:%x], VLAN=[v:%d] flags=[f:%x]	System detected first IP frame the user. L3 entry will be created	
522029	Info	MAC=[mac:%s] Station authenticate: method=[m:%s], role=[r1:%s]/[r2:%s]/[r3:%s]/[r4:%s], VLAN=[v1:%d]/[v2:%d], Derivation=[d1:%d]/[d2:%d], Value Pair=[p:%d]	Station completed successful authentication and was admitted into the system	
522030	Info	MAC=[mac:%s] Station deauthenticated: BSSID=[b:%s], ESSID=[e:%s]	Station was De-authenticated	
522033	Info	MAC=[mac:%s] IP=[ip:%s] SIP authenticate: Set role to '[r:%s]'	User was authenticated and assigned new role after completing SIP registration with PBX	
522034	Info	MAC=[mac:%s] IP=[ip:%s] Fast age: role=[r:%s]	Fast ageout triggered because multiple IP detected for a MAC. System will send ICMP echo messages to detect inactive stations without waiting for expiry of inactivity period.	
522035	Info	MAC=[mac:%s] Station UP: BSSID=[b:%s] ESSID=[e:%s] VLAN=[v:%d] AP-name=[n:%s] u-encr-alg=[ue:%x] m-encr-alg=[me:%x] at [t:%s]	System detected a new wireless station	
522036	Info	MAC=[mac:%s] Station DN: BSSID=[b:%s] ESSID=[e:%s] VLAN=[v:%d] AP-name=[n:%s] reason=[rsn:%d] at [t:%s]	System is reporting departure of a wireless station	
522037	Info	MAC=[mac:%s] IP=[ip:%s] Assign VLAN [v:%d], Default=[d:%d] Current=[c:%d] BSSID=[b:%s]	User VLAN was changed	
522044	Info	MAC=[mac:%s] Station authenticate(start): method=[m:%s], role=[r1:%s]/[r2:%s]/[r3:%s]/[r4:%s], VLAN=[v1:%d]/[v2:%d], Derivation=[d1:%d]/[d2:%d], Value Pair=[p:%d], flags=[fl:%x]	Station authentication is in progress	
522045	Info	[string:%s]	Internal message to track user state	
522047	Info	Skipping certificate common name check for username=[user:%s] MAC=[mac:%s]	Based on configuration settings, the check for the certificate common name against a AAA server was skipped.	
522049	Info	MAC=[mac:%s],IP=[ip:%s] User role updated, existing Role=[r1:%s]/[r2:%s], new Role=[r3:%s]/[r4:%s], reason=[r5:%s]	Internal message to track role update for a user. For "RAP New user with no l3 auth or authenticated station", the role was updated for a new RAP user that has not been L3 authenticated. For "User not authenticated for inheriting attributes", the role was updated for an un-authenticated user through the station inheritance scheme.	
522050	Info	MAC=[mac:%s],IP=[ip:%s] User data downloaded to datapath, new Role=[r3:%s]/[r4:%d], bw Contract=[r5:%d]/[r6:%d], reason=[r7:%s], Downloaded value for idle-timeout=[r8:%d]	Internal message to track Role update for a User.	
522051	Info	MAC=[mac:%s] Clear Bridge Entry	User Bridge Entry was cleared	
522103	Info	[type:%s]: Station=[mac:%m] BSS=[bss:%m] PMKID does not match.	This shows WPA3 client has mis-matched PMKID	
522106	Info	MAC=[mac:%s] IP=[ipaddr:%s] MOBILITY AUTH UPDATE: no mac user found, creating it	This shows an internal debug message	
522157	Info	Update [type:%s] bridge-mode user: username=[name:%s] MAC=[mac:%s] IP=[ip:%s] AP=[apname:%s] aclnum=[acl:%d].	This shows informtion about updatinng a bridge-mode user	
522190	Info	MAC=[mac:%s] IP=[ipaddr:%s]: MAC auth [macauth:%s]: entry-type=[entrytype:%s], bssid=[bssid:%s]	This shows an internal debug message	
522219	Info	MAC=[mac:%s] IP=[ipaddr:%s] INTRA MOVE: no mac user found.	This shows an internal debug message	
522220	Info	MAC=[mac:%s] IP=[ipaddr:%s] INTRA MOVE: default_vlan=[defvlan:%d],port=[port:%d],flag=[flag:%x],tunid=[tunid:%d],apname=[apname:%s] , User mac [usermac:%s] flags [flags:%x] homeagent [homeagent:%d] tunacl [tunacl:%p] mac-mismatch [macmismatch:%d].	This shows an internal debug message	
522221	Info	MAC=[mac:%s] IP=[ipaddr:%s] INTER MOVE: no mac user found.	This shows an internal debug message	

522222	Info	MAC=[mac:%s] IP=[ipaddr:%s] INTER MOVE: default_vlan=[defvlan:%d],port=[portid:%d],flag=[flag:%x],tunid=[tunid:%x],apname=[apname:%s], User mac [usermac:%s] flags [flags:%x] homeagent [ha:%d] user tunid [usertunid:%x] mac-mismatch [macmismatch:%d].	This shows an internal debug message	
522227	Info	Cannot move non-existent user [mac:%s]:[ipstr:%s] on [ha:%s] Agent.	This shows an internal debug message	
522228	Info	Cannot delete non-existent user [mac:%s]:[ipstr:%s] on [ha:%s] Agent.	This shows an internal debug message	
522250	Info	ARP-packet: MAC=[mac:%s] Sender-IP=[ip:%s] Sender-MAC=[smac:%s] IP spoof with exsting MAC=[exist:%s], Drop It.	System detected MAC spoofing. Frame was dropped	
522251	Info	ARP-packet: Detected ARP attack MAC=[mac:%s] IP=[ip:%s] Sender-MAC=[smac:%s] from [from:%s], Denylist It.	System detected ARP attack. Put station in denylist	
522252	Info	ARP-packet: MAC=[mac:%s] IP=[ip:%s] Sender-MAC=[smac:%s] spoofing, Drop It.	System detected MAC spoofing. Frame was dropped	
522278	Info	MAC=[mac:%s] IP=[ip:%s] Dldb Role: [r:%s] Derived downloadable role from Aruba CPPM VSA	User was assigned a role derived from CPPM Vendor Specific Attributes returned by authentication server	
522311	Info	MAC=[mac:%s] Station ACTIVATE: BSSID=[b:%s] ESSID=[e:%s] VLAN=[v:%d] AP-name=[n:%s]	System activating a standby wireless station	
522347	Info	Auth GSM : MAC_USER publish failed for mac [m: %s] result [r: %s]	This shows an internal user info message	
522348	Info	Auth GSM : USER publish failed for mac [m: %s] uuid [u: %s] repkey [rep:%d] result [r: %s]	This shows an internal user info message	
522358	Info	Replace ip [ipuser:%s] with [user:%s] for MAC [mac:%s]. Reason: [string:%s] limit reached.	This shows an internal user info message	
522359	Info	Received user_miss from SOS for a bridge mode user MAC=[mac:%m] IP=[ip:%s], drop packet	This shows an internal user error message	
522360	Info	Received Invalid rap_user_miss with IP=[ip:%s], fw_mode=[fwmode:%d] from BSSID=[bssid:%m] in RAP=[apname:%s] for a bridge mode user MAC=[mac:%m], Ignore it	This shows an unsupported user error message	
527004	Info	[thread:%u] [func:%s] [line:%d] [msg:%s]	User debug messages for mDNS proxy (mdns)	
527501	Info	[func:%s] [line:%d] [msg:%s]	User debug information messages for AirGroup	
541001	Info	Add client [mac:%s] to denylist, reason is [reason:%s].	add a client to blacklist.	
541002	Info	Remove client [mac:%s] from denylist, reason is [reason:%s].	remove a client from blacklist.	
541031	Info	Learning client username: mac-[mac:%m] usr-[username:%s] acct-[acctname:%s].	learning client usrname.	
541032	Info	[func: %s]: allocate accounting session id, user-[mac:%m] id-[id:%u].	learning client usrname.	
541034	Info	[func: %s]: set user idle timeout, user-[mac:%m] timeout-[to:%u].	Set user idle timeout.	
541035	Info	[func: %s]: receive os msg, mac-[mac:%m], detail-[us:%s].	Receive os msg.	
541036	Info	[func:%s]: send idle timeout, sta [mac:%m] , idle time-[time:%d].	Station update.	
541047	Info	Recv sta l2 roam msg for sta-[mac:%m], pap-[ip:%s], essid-[ssid:%s] timestamp-[time:%u]-[time_usec:%u]	Receive sta l2 roam.	
541048	Info	Send move req to [pap:%s], for sta-[mac:%m], essid-[essid:%s] timestamp-[time:%u]-[time_usec:%u]	Send sta move req.	
541049	Info	Receive move req for sta-[mac:%m], essid-[essid:%s], from-[ap:%s] timestamp-[time:%u]-[time_usec:%u]	Send sta move req.	
541050	Info	Send move response for sta-[mac:%m], to ap-[ip:%s], timestamp-[time:%u]-[time_usec:%u]	Send sta move resp.	
541051	Info	Recv sta move resp for sta-[mac:%m], from [ip:%s], timestamp-[time:%u]-[time_usec:%u]	Receive sta move resp.	
541052	Info	Sta [mac:%m] move timeout, retry cnt [retry:%d]	Sta move timeout	
541067	Info	Rfc3576 update client role for: [mac:%m], [role:%s], idx-[idx:%u], acl-[acl:%u].	Update user role.	
541068	Info	Receive XML API lookup for: [mac:%m], [ip:%s].	Receive XML API	
541069	Info	Receive XML API usr_del for: [mac:%m], [ip:%s].	Receive XML API usr_del	
541070	Info	Receive XML API usr_denylist for: [mac:%m], [ip:%s].	Receive XML API usr_blacklist	
541071	Info	Receive XML API usr_query for: [mac:%m], [ip:%s].	Receive XML API usr_query	
541072	Info	Receive XML API usr_auth for: [mac:%m], [ip:%s].	Receive XML API usr_auth	
541085	Info	[func:%s]: Add user-[user:%s] in Auth Survivability cache for client-[mac:%m].	Add new user entry in cache.	

541086	Info	[func:%s]: Update user-[user:%s] in Auth Survivability cache for client-[mac:%m].	Updating existing user entry in cache.	
541087	Info	[func:%s]: Delete user-[user:%s] in Auth Survivability cace for timeout.	Delete existing user entry in cache.	
541088	Info	[func:%s]: Send user-[user:%s] for Auth Survivability to AP-[ip:%s].	Sync cached user for Auth Sruvivability to new AP.	
541089	Info	[func:%s]: Send user-[user:%s] for Auth Survivability to AP-[ip:%s]. aruba_vlan-[vlan:%hu] aruba_named_vlan-[named_vlan:%s] aruba_no_dhcp_fingerprint-[finger_print:%hhu] aruba_role-[role:%s] tunnel_type-[tunnel_type:%hhu] tunnel_medium_type-[tunnel_media_type:%hhu] tunnel_private_group_id-[tunnel_private_groupid:%s] pw_user_name-[pw_user_name:%s] pw_session_timeout-[session_timeout:%u]	Sync cached user for Auth Sruvivability to new AP.	
541090	Info	[func:%s]: Receive synced user-[user:%s] for Auth Survivability from AP-[ip:%s].	Receive user for Auth Sruvivability from old AP.	
541091	Info	[func:%s]: Receive synced user-[user:%s] for Auth Survivability from AP-[ip:%s]. aruba_vlan-[vlan:%hu] aruba_named_vlan-[named_vlan:%s] aruba_no_dhcp_fingerprint-[finger_print:%hhu] aruba_role-[role:%s] tunnel_type-[tunnel_type:%hhu] tunnel_medium_type-[tunnel_media_type:%hhu] tunnel_private_group_id-[tunnel_private_groupid:%s] pw_user_name-[pw_user_name:%s] pw_session_timeout-[session_timeout:%u]	Receive cached user attributes for Auth Sruvivability from old AP.	
541092	Info	[func:%s]: Add user-[user:%s] in Auth Survivability cache for client-[mac:%m]. aruba_vlan-[vlan:%hu] aruba_named_vlan-[named_vlan:%s] aruba_no_dhcp_fingerprint-[finger_print:%hhu] aruba_role-[role:%s] tunnel_type-[tunnel_type:%hhu] tunnel_medium_type-[tunnel_media_type:%hhu] tunnel_private_group_id-[tunnel_private_groupid:%s] pw_user_name-[pw_user_name:%s] pw_session_timeout-[session_timeout:%d]	Add new user entry in cache.	
541093	Info	[func:%s]: Update user-[user:%s] in Auth Survivability cache for client-[mac:%m]. aruba_vlan-[vlan:%hu] aruba_named_vlan-[named_vlan:%s] aruba_no_dhcp_fingerprint-[finger_print:%hhu] aruba_role-[role:%s] tunnel_type-[tunnel_type:%hhu] tunnel_medium_type-[tunnel_media_type:%hhu] tunnel_private_group_id-[tunnel_private_groupid:%s] pw_user_name-[pw_user_name:%s] pw_session_timeout-[session_timeout:%d]	Updating existing user entry in cache.	
542012	Info	VM: CDR started for client [name: %s], protocol [alg: %s]	Call data record created for a new call	
542013	Info	VM: CDR generated for client IP:[ip: %s] Name:[name: %s] ALG:[alg: %s] Dir:[dir: %s] Peer Party:[peer: %s] Status:[status: %s] Dur:[time: %d] Orig time:[orig: %s] R-value:[r: %d] Reason:[reason: %s] Codec:[codec: %s] Band:[band: %s] Setup Time:[setup: %d] Re-Assoc:[reassoc: %d] Initial-BSSID:[initbss: %s] Initial-ESSID:[initess: %s] Initial-AP Name:[initap: %s]	Call data record ended for a call	
542020	Info	VM: CDR AP Event: Timestamp:[time: %s] BSSID:[bss: %s] Event:[evt: %s]	AP Event kept with CDR	
542021	Info	VM: CDR AP Stat: Timestamp:[time: %s] BSSID:[bss: %s] RSSI:[rssi: %d] Tx:[tx: %d] Tx_Drop:[tx_d: %d] Tx_Data:[tx_data: %d] Tx_Data_Retry:[tx_data_retry: %d] Tx_Data_Bytes:[tx_data_byte: %ld] Tx_Data_Time:[tx_data_time: %ld] Rx:[rx: %d] Rx_Retry:[rx_r: %d]	AP Stat kept with CDR	
542038	Info	VM: Client [ip_addr: %s] de-authenticated due to extra call	Client was de-authenticated as extra call could not be admitted because call capacity has been reached	Increase the call capacity by adding more AP and/or increasing call capacity limit in CAC profile. Disable "disconnect extra call" if configured in CAC profile
542057	Info	VM: VoIP call terminated for client [ip_addr: %s]	Voice call to/from the client has ended	
542064	Info	VM: VoIP call started for client [client: %s]	Voice call to or from client started	
542074	Info	VM: Client [ip_addr: %s] is registered	VoIP client has registered with PBX	

542082	Info	VM: Unexpected end of SIP message	This message is logged when system encounters a truncated SIP message	
542102	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Illegal event [evt: %s] on state [st: %s]	NOE FSM receives illegal event	
542105	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: call FSM failed	NOE call FSM failed	
542106	Info	NOE: [fn: %s] [line: %d]: cannot locate or create vc	NOE failed to locate or create vc	
542108	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Too many unack keepalives	NOE client exceeds unacknowledged keepalive threshold	
542110	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: NULL seq_qlist	NOE sequence queue not initialized	
542113	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Cannot get valid call	NOE failed to get a valid call	
542116	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Null call_list pointer	NOE log for NULL call list pointer	
542117	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Multiple calls [num: %d] in call_list	NOE log for multiple calls when there should be only one call	
542119	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Failed to malloc a call	NOE failed to create a call	
542125	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: RTCP local IP [lip: %s] not equal to vc IP	NOE RTCP local IP mismatch	
542126	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: RTCP local port [lport: %d] not equal to media rx port [rxport: %d] plus 1	NOE RTCP local port mismatch	
542127	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: RTCP remote IP [rip: %s] not equal to media tx IP [txip: %s]	NOE RTCP remote IP mismatch	
542128	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: RTCP remote port [rport: %d] not equal to media tx port [txport: %d] plus 1	NOE RTCP remote port mismatch	
542129	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: empty call_list	NOE log for empty call list	
542131	Info	NOE: [ip: %s]: [fn: %s] [line: %d]: Keepalive failure	Info log for NOE keepalive failure	
543002	Info	[msg:%s]		
543003	Info	[func:%s]: [msg:%s]		
544001	Info	[func:%s] [line:%d] [msg:%s]	User debug messages for DPI MGR	
500002	Notice	Station [mac:%m], [ip:%s]: received [nevent:%d] mobility events within 1 sec, threshold exceeded	Mobile IP handles all the frames from a station until it gets assigned a mobility state. This message means that we have exceeded the number of received frames threshold before assigning a mobility state. This threshold is configurable with "ip mobile proxy event-threshold" cli command. This means that either there is an unexpected problem with mobility state for this station or that this station generates a lot of upstream frames at a high rate shortly after association. Since client exceeded threshold it will be penalized for 60 seconds during which mobility will not process any event from client. During this period client will experience connectivity issues.	
500010	Notice	Station [mac:%m], [ip:%s]: Mobility trail, on switch [switchip:%pI4], VLAN [vl:%d], AP [apname:%s], [essid:%s]/[bssid:%s]/[phy:%s]	This is the Mobility trail message, it is generated every time a station moves to a new BSSID. This allows to track a specific station movement in the network over time	
500011	Notice	Station [mac:%m], [ip:%s]: added to Mobility BlackList table on [hafa:%s]		
500012	Notice	Station [mac:%m], [ip:%s]: deleted from Mobility BlackList table on [hafa:%s]	The station marked Blacklisted by ESI server will be deleted	
500518	Notice	Station [mac:%m] : Update Mobility Mcast-Group table, bssid [bssid:%m], home vlan:[home_vlan:%d], Lkup Tunnel:[lkup_tun_id:%x], Dest Tunnel:[dst_tun_id:%x], action [action:%s] [dbg_str:%s]	Updating (add/del) MMG DB entry when client moves	
500519	Notice	Station [mac:%m] : Mobility Mcast-Group table [action:%s] FAILED, bssid [bssid:%m], home vlan:[home_vlan:%d], Lkup Tunnel:[lkup_tun_id:%x], Dest Tunnel:[dst_tun_id:%x], error:[ret:%d] [dbg_str:%s]	Updating (add/del) MMG DB entry when client moves failed	
501001	Notice	Station [sta:%m]: Trying to associate to BSSID [bss:%m] on AP [name:%s] before authentication		
501002	Notice	Station [sta:%m]: ESSID length error trying to associate to BSSID [bss:%m] on AP [name:%s], length [len:%d]		
501003	Notice	Station [sta:%m]: Supported rates length trying to associate to BSSID [bss:%m] on AP [name:%s], length [len:%d], actual [alen:%zu]		
501004	Notice	Station [sta:%m]: WPA too Many Ucast ([num:%d]) trying to associate to BSSID [bss:%m] on AP [name:%s]		

501005	Notice	Station [sta:%m]: WPA2 too Many Ucast ([num:%d]) trying to associate to BSSID [bss:%m] on AP [name:%s]		
501010	Notice	Station [sta:%m]: Ucast ([ucast:%d]) cannot be non WPA trying to associate to BSSID [bss:%m] on AP [name:%s]		
501011	Notice	Station [sta:%m]: Ucast ([ucast:%d]) cannot be non AES trying to associate to BSSID [bss:%m] on AP [name:%s]		
501020	Notice	Station [sta:%m]: WPA too Many auth ([num:%d]) trying to associate to BSSID [bss:%m] on AP [name:%s]		
501021	Notice	Station [sta:%m]: WPA2 too Many auth ([num:%d]) trying to associate to BSSID [bss:%m] on AP [name:%s]		
501025	Notice	Station [sta:%m]: WPA2 too Many PMKID ([num:%d]) trying to associate to BSSID [bss:%m] on AP [name:%s]		
501037	Notice	Station [sta:%m]: no association found trying to disassociate to BSSID [bss:%m] on AP [name:%s]		
501044	Notice	Station [sta:%m]: No authentication found trying to de-authenticate to BSSID [bss:%m] on AP [name:%s]	Station is already removed from station manager when receiving the de-authentication from the station	
501080	Notice	Deauth to sta: [mac:%m]: Ageout AP [ip:%P]-[bssid:%m]-[name:%s] [reason:%s]		
501081	Notice	Deauth to sta: [mac:%m]: Ageout AP [ip:%P]-[bssid:%m]-[name:%s] [reason:%d]		
501084	Notice	Probe request: [mac:%m]: Dropped AP [ip:%P]-[bssid:%m]-[name:%s] for STA DoS protection		
501087	Notice	Probe request: [mac:%m]: Dropped AP [ip:%P]-[bssid:%m]-[name:%s] for STA DoS protection SSID [essid:%s]		
501088	Notice	Probe request: [mac:%m]: Dropped AP [ip:%P]-[bssid:%m]-[name:%s] for Rates Mismatch STA 0x[rates:%x] AP 0x[tx_rates:%x] SSID [essid:%s]		
501089	Notice	Probe request: [mac:%m]: Dropped AP [ip:%P]-[bssid:%m]-[name:%s] for Load Balancing SSID [essid:%s]		
501093	Notice	Auth success: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s]		
501094	Notice	Auth failure: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [resp:%s]		
501095	Notice	Assoc request @ [tstr:%s]: [mac:%m] (SN [sn:%d]): AP [ip:%P]-[bssid:%m]-[name:%s]	Observed station sent association request to AP.	
501098	Notice	Deauth to sta: [mac:%m]: Moved out from AP [ip:%P]-[bssid:%m]-[name:%s] to new AP		
501099	Notice	Deauth to sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [resp:%s]		
501100	Notice	Assoc success @ [tstr:%s]: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s]		
501101	Notice	Assoc failure: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [resp:%s]		
501102	Notice	Disassoc from sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [reason_code:%s]		
501105	Notice	Deauth from sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [reason_code:%s]		
501106	Notice	Deauth to sta: [mac:%m]: Ageout AP [ip:%P]-[bssid:%m]-[name:%s] [func:%s]		
501107	Notice	Deauth to sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] AP going down		
501108	Notice	Deauth to sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Configuration Change		
501109	Notice	Auth request: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] auth_alg [auth_alg:%d]		
501110	Notice	Auth failure: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [resp:%d]		
501111	Notice	Deauth to sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [resp:%d]		
501112	Notice	Assoc failure: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [resp:%d]		
501113	Notice	Disassoc from sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [reason_code:%d]		
501114	Notice	Deauth from sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Reason [reason_code:%d]		
501117	Notice	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s]		
501126	Notice	Addts resp: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] accept flow - [flow:%s]		

501129	Notice	Delts: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Flow - [flow:%s]		
501132	Notice	[ip:%P]:[mac:%m] - kick off idle VoIP STA		
501133	Notice	[func:%s]:[line:%d] Extra call admitted [mac:%m]-[ip:%P]		
501134	Notice	STA [mac:%m]: HT Capabilities element too short ([len:%d]); ignoring		
501136	Notice	Source: [sa:%m] Failed AP [ip:%P]-[bssid:%m]-[name:%s] Legacy stations not allowed.		
501153	Notice	STA [mac:%m]: required MFP but SSID [bssid:%s] not capable; ignoring		
501154	Notice	STA [mac:%m]: not MFP capable but SSID [bssid:%s] requires MFP; reject		
501155	Notice	STA [mac:%m]: sent illegal MFP params [bssid:%s] ; reject		
501156	Notice	STA [mac:%m]: MFPC 0 but MFPR 1 [bssid:%s] ; reject		
501159	Notice	STA [mac:%m]: VHT Capabilities element too short ([len:%d]); ignoring		
501189	Notice	No available vlan in sta_vlan_id. Cannot take [mac:%m] association request	Station manager does not have available configured vlan to accept association request	
501190	Notice	Vlan assignment algorithm not set. Cannot take [mac:%m] association request	Vlan assignment algorithm is not specified in virtual-ap profile	
501191	Notice	STM fails to assign a vlan to sta [mac:%m] on association request	Station manager fails to assign a vlan to a station on association request	
501199	Notice	User authenticated, mac-[mac:%m], username-[name:%s], IP-[ip:%pI4], method-[method:%s], role-[role:%s]	This log indicates that a user has been authenticated	
501201	Notice	[func:%s][line:%d]: mac-[mac:%m], role-[role:%s], intercept-[on:%d]	This log indicates that a user has been caleaOn	
501216	Notice	[func: %s] [line:%d]: user entry created for [ip:%s]-[mac:%m]	This log indicates that client is online.	
501217	Notice	[func: %s] [line:%d]: user entry deleted for [ip:%s]-[mac:%m]	This log indicates that client is offline.	
501218	Notice	[msg:%s]		
501220	Notice	Denylist for [reason:%s] skipped to rate limit the deauth for device [mac:%m] of type [device_type:%s]		
501223	Notice	STA [mac:%m]: HE Capabilities element too short ([len:%d]); ignoring		
501224	Notice	STA [mac:%m]: HE 6GHz Band Capabilities element too short ([len:%d]); ignoring		
501225	Notice	STA [mac:%m]: HE 6GHz Band Capabilities element is missing; rejecting assoc-req in 6GHz band. AP: [ip:%P] [bssid:%m] [name:%s]		
509005	Notice	FIPS Notice: [msg:%s]	This is a FIPS notice log in user module.	
522008	Notice	User Authentication Successful: username=[name:%s] MAC=[mac:%s] IP=[ip:%s] role=[r:%s] VLAN=[vlan:%d] AP=[ap:%s] SSID=[ssid:%s] AAA profile=[aaa:%s] auth method=[am:%s] auth server=[as:%s]	User authenticated	
522009	Notice	MAC=[mac:%s] IP=[ip:%s] CIM Remediation failed: user role reset to [role:%s]	User role was reset due to remediation failure	
522010	Notice	MAC=[mac:%s] IP=[ip:%s] User de-authenticated: name=[n:%s], cause=[c:%s]	User deauthenticated	
522031	Notice	MAC=[mac:%s] IP=[ip:%s] RFC 3576 Disconnect user: role=[r:%s]	System received a RFC 3576 disconnect message. All user entries matching MAC, IP and name in the message will be removed	
522032	Notice	MAC=[mac:%s] IP=[ip:%s] RFC 3576 CoA: Change role from '[r1:%s]' to '[r2:%s]	System received a RFC 3576 Change-of-Authorization message. All user entries matching MAC, IP and name in the message will user role updated	
522038	Notice	username=[user:%s] MAC=[mac:%s] IP=[ip:%s] Result=[r:%s] method=[m:%s] server=[sg:%s]	User authentication was completed using the specified method and server	
522039	Notice	MAC=[mac:%s] IP=[ip:%s] Denylist user: reason=[r:%s]	User was denylisted for violation of a firewall rule	
522375	Notice	Dot1x User authenticated with new username [newname:%s] old username [oldname:%s], delete existing PMKs		
527005	Notice	[thread:%u] [func:%s] [line:%d] [msg:%s]	User debug messages for mDNS proxy (mdns)	
527502	Notice	[func:%s] [line:%d] [msg:%s]	User debug notice messages for AirGroup	
542002	Notice	[func:%s]:[line:%d] Extra call admitted [mac:%m]-[ip:%pI4]		
544002	Notice	[func:%s] [line:%d] [msg:%s]	User debug messages for DPI MGR	
500022	Warning	Station [mac:%m], [ip:%pI4]: IP address change [nip:%pI4] detected, mobility service will be aborted	Mobile client IP address is changed henceforth its mobility services will be terminated	
500053	Warning	Race noticed for Station: [mac:%m], [ip:%s]: HomeVlan: [hv:%d] Current Vlan: [cv:%d] roaming status: [rs:%d] Proxy state: [ps:%d] at [fn:%s] [ln:%d]	Proxy State machine detected race for particular mobile client	

500071	Warning	Station [mac:%m], [ip:%s]: local VLAN not matching HAT	The station IP address seems to belong to a different VLAN that the one matching its IP address in the HAT. This probably means that the HAT for the mobility domain is misconfigured.	
500100	Warning	Station [mac:%m], [ip:%s]: Maximum number of visitors is reached, station will be rejected. Please increase the limit (ip mobile foreign-agent max-visitors) if more visitors are to be allowed.	FA has rechaed maximum number of configurable visitor. Please increase the limit if more visitors need to be entertained	
500243	Warning	Station [mac:%m], [ip:%s]: Maximum number of bindings is reached, station will be rejected. Please increase the limit (ip mobile home-agent max-bindings) if more visitor bindings are to be allowed.	HA reached configurable Max number of binding. Please increase the limit in order to accomodate new bindings.	
500256	Warning	Race noticed for binding: [mac:%m], [ip:%s]: Previous: [ps:%d] Current State: [cs:%d] Previous COA: [pfa:%s] Current COA: [ccoa:%s] HomeVlan: [hv:%d] Current FA Vlan: [cv:%d] at [fn:%s][ln:%d]	HA state machine detected Race condition for particular binding	
500501	Warning	HAT [addr:%pI4] Failed to add datapath hat entry	Mobility failed to add Hat entry in datapath	
500502	Warning	HAT [addr:%pI4]: Failed to delete datapath hat entry	Mobility failed to delete Hat entry in datapath	
500503	Warning	Station [mac:%m], [vlan:%d], [ip:%s]: Failed to start ha discovery in datapath	Mobility failed to start ha discovery in datapath	
500507	Warning	Station [mac:%m]: Received invalid ha discovery packet	Received invalid ha discovery packet from datapath	
500508	Warning	HAT failed to add datapath hat entry in bulk	Mobility failed to add Hat entry in bulk	
501026	Warning	Station [sta:%m]: too many vlan ([num:%d]) trying to associate to BSSID [bss:%m] on AP [name:%s]		
501027	Warning	Station [sta:%m]: authentication payload shorter than min, length [len:%d], expected [elen:%zu] trying to associate to BSSID [bss:%m] on AP [name:%s]		
501030	Warning	Station [sta:%m]: Packet too short, length [len:%d], expected [elen:%zu] trying to disassociate to BSSID [bss:%m] on AP [name:%s]	An 802.11 Disassociation frame was received that was too short. It will be ignored.	
501040	Warning	Station [sta:%m]: Packet too short, length [len:%d], expected [elen:%zu] trying to de-authenticate to BSSID [bss:%m] on AP [name:%s]		
501060	Warning	Station [sta:%m]: Ignored Association response to BSSID [bss:%m] on AP [name:%s]		
501061	Warning	Station [sta:%m]: Ignored Re-Association response to BSSID [bss:%m] on AP [name:%s]		
501062	Warning	Station [sta:%m]: Ignored ATIM to BSSID [bss:%m] on AP [name:%s]		
501064	Warning	Station [sta:%m]: Ignored unknown management frame subtype [stype:%x]h to BSSID [bss:%m] on AP [name:%s]		
501067	Warning	Source: [sa:%m] Failed AP [ip:%P]-[bssid:%m]-[name:%s] Rates Mismatch STA 0x[rates:%x] AP 0x[tx_rates:%x]		
501068	Warning	Source: [sa:%m] Failed AP [ip:%P]-[bssid:%m]-[name:%s] Multicast Encryption Mismatch		
501069	Warning	Source: [sa:%m] Failed AP [ip:%P]-[bssid:%m]-[name:%s] Unicast Encryption Mismatch		
501070	Warning	STA [mac:%m] not found in sta_hash_table		
501071	Warning	wifi_update_sta_vlan: STA [mac:%m] not found		
501072	Warning	wifi_update_sta_vlan: STA [mac:%m] not associated with SAP [bssid:%m]		
501073	Warning	STA [mac:%m] not found in sta_hash_table		
501075	Warning	wifi_counter_measures_enable: STA [mac:%m] not found		
501076	Warning	wifi_bss_counter_measures_enable: STA [mac:%m] not found		
501077	Warning	wifi_update_sta_vlan: AP [bssid:%m] STA [mac:%m]: VAP Not found. ageout		
501078	Warning	wifi_update_sta_vlan: AP [bssid:%m] STA [mac:%m]: VLAN [vlan_id:%d] not found. ageout		
501079	Warning	handle_sta_stat_req: Unknown STA [mac:%m]		
501083	Warning	Probe request: [mac:%m]: Invalid Station MAC address from AP [ip:%P]-[bssid:%m]-[name:%s]		
501086	Warning	Probe request: [mac:%m]: Invalid Station MAC address from AP [ip:%P]-[bssid:%m]-[name:%s] SSID [essid:%s]		

501091	Warning	Auth request: [mac:%m]: Invalid Station MAC address from AP [ip:%P]-[bssid:%m]-[name:%s]		
501092	Warning	Auth request: [mac:%m]: Dropped AP [ip:%P]-[bssid:%m]-[name:%s] for STA DoS protection		
501096	Warning	Assoc request: [mac:%m]: Invalid Station MAC address from AP [ip:%P]-[bssid:%m]-[name:%s]		
501097	Warning	Assoc request: [mac:%m]: Dropped AP [ip:%P]-[bssid:%m]-[name:%s] for STA DoS protection		
501103	Warning	Denylist add: [mac:%m]: Reason: [reason:%s]		
501104	Warning	Disassoc from sta: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Disassoc Flood DoS Attack Detected		
501115	Warning	Denylist del: [mac:%m]: by administrator		
501116	Warning	Denylist del: [mac:%m]: timeout		
501118	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. STA Not Found		
501119	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. STA Not Associated		
501120	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. SIP client not on-call		
501121	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. Invalid TCLAS count/type ([num_tclas:%d]/[type:%d])		
501122	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. TCLAS/SDP mismatch ([tbuf:%s]/[sdpbuf:%s])		
501123	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. TSPEC does't match codec characteristics ([rv:%d])		
501124	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. Voice Capacities Reached		
501125	Warning	Addts req: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] refused. Flow Setup Failed		
501127	Warning	Delts: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] STA Not found		
501128	Warning	Delts: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] STA Not Associated		
501130	Warning	Delts: [mac:%m]: AP [ip:%P]-[bssid:%m]-[name:%s] Flow Not Found		
501131	Warning	[func:%s]:[line:%d] STA [mac:%m] not found		
501135	Warning	Source: [sa:%m] Failed AP [ip:%P]-[bssid:%m]-[name:%s] WEP and TKIP encryption not valid with high throughput		
501141	Warning	Denylist client: [mac:%m] removed during repopulation from db. Reason: [reason:%s]	This log indicates that a client denylist entry was removed during repopulation from db.	
501209	Warning	Remove stale user [mac:%m], driver age out	This log indicates that we are remove stale user entry.	
506203	Warning	Unsupport device-name:[devname:%s] for station:[mac:%m] received from Clearpass. Ignore it!	This indicates Device-Name for a station received from ClearPass NetWatch is not supported.	
506900	Warning	[func:%s](MAC/IP=[macstr:%s]/[ipstr:%s]): PAPI_Alloc() Failed while communicating to MAPC.	This indicates an error in PAPI_Alloc()	
506901	Warning	[func:%s](MAC/IP=[macstr:%s]/[ipstr:%s]): PAPI_Send() Failed while communicating to MAPC.	This indicates an error in PAPI_Send()	
506904	Warning	[func:%s](MAC=[macstr:%s]): PAPI_Alloc() Failed while communicating to MAPC.	This indicates an error in PAPI_Alloc()	
506905	Warning	[func:%s](MAC=[macstr:%s]): PAPI_Send() Failed while communicating to MAPC.	This indicates an error in PAPI_Send()	
509004	Warning	FIPS Warning: [msg:%s]	This is a FIPS warning log in user module.	
520014	Warning	[msg:%s]	This shows an internal clarity auth warning log	
522018	Warning	MAC=[mac:%s] IP=[ip:%s] Derived unknown role '[r:%s]' from server rules: server-group=[sg:%s], authentication=[auth:%s]	System derived an unknown role from server derivation rules. User will be assigned default role for authentication	
522027	Warning	MAC=[mac:%s] IP=[ip:%s] IP Spoof from MAC=[m:%s] role=[ur:%s]/[sr:%s]	System detected IP spoofing. Frame was dropped	
522028	Warning	MAC=[mac:%s] Assigned VLAN [v1:%d] is not configured, using default VLAN [v2:%d]		

522042	Warning	Failed to send a SNMP trap. trap-type=[trap:%s] usermac=[usermac:%m] username=[username:%s] userip=[userip:%s]	This shows failure in sending SNMP trap	
522043	Warning	Configured Session limit reached for client IP=[ip:%s]	Configured Session limit has been reached for the client	Turn off the client till existing sessions have been cleared. Contact tecnical support if problem persists after turning the client back on
522046	Warning	[string:%s]	User state between mobility and auth is out of sync; datapath detected IPIP loop. Preventive action is being taken to fix user state. Please notify TAC immediately	
522052	Warning	[string:%s]	Potential out of sync of user information between AUTH / SOS	
522105	Warning	User state between auth-mobileip is NOT in sync. User details: MAC=[mac:%s] IP=[ipaddr:%s] homeagent [home:%d] roaming [roam:%d] tunid [tunid:%x] tunacl [tunacl:%d] apname [apname:%s] MM flags [mmflags:%x] Born [born:%s].	This shows an internal debug message	
522125	Warning	Could not create/find bandwidth-contract for user, return code ([user_bwm:%d]).	This shows that controller ran out of per-user bandwidth contracts	
522223	Warning	Failed to create dynamic role [role:%s] for user [mac:%s]:[ipstr:%s] with tunnel id [tunid:%d].	This shows an internal debug message	
522233	Warning	MAC-address is changed from [omac:%m] to [nmac:%m] for IP:[ip:%s].	This shows mac-address for an ip-user is changed.	
522267	Warning	MAC=[mac:%s] IP=[ip:%s] Derived unknown role '[r:%s]' from VSA, authentication=[auth:%s]	System derived an unknown role from vendor specific attributes. User will be assigned default role for authentication	
522275	Warning	User Authentication failed. username=[username:%s] userip=[userip:%s] usermac=[usermac:%s] authmethod=[method:%s] servername=[servername:%s] serverip=[serverip:%s] apname=[apname:%s] bssid=[bssid:%s]	This shows user authentication failure	
522340	Warning	Client [mac:%s] name updated to [name:%s]	User name of client updated with client's hostname, found in DHCP option 12	
522373	Warning	Stateful1x in progress for user. Dropping bridge miss rcvd. MAC=[mac:%m] ingress [ingress:%x] VLAN=[v:%d]	This shows a user warning message	

522374	Warning	Stateful1x started for existing user. Purging old user. MAC=[mac:%m] Authenticator MAC=[authmac:%m] IP=[authip:%s] This shows a user warning message 524107@FTIE MIC Failed in FT association request for Station [mac:%m] BSS:[bssid:%m] mic_control:[mc:%u] This shows FTIE-MIC verification failure for FT ReAssoc. 524126@[func:%s](): FT-Bridge Client-MAC:[mac:%s] Could not find in K-Cache. This shows internal debug messages. 524133@[func:%s](): MAC:[mac:%s] BSS:[bssid:%s] GSM: Failed to publish PMK-cache object. Error:[error:%s] This shows internal debug messages. 524162@[func:%s](): MAC:[mac:%m] BSS:[bssid:%m] ESSID:[essid:%s] Failed to derive PMK-R0 This shows problem in deriving PMKR0 for initial FT-Association. 525000@[func:%s]([line:%d]): PAPI_Send(mac=[mac:%m] to=[dest:%s]:[port:%d] oper-type=[type:$%d]) Failed, error:[err:%s] This indicates failed to send PAPI message. 525001@[func:%s]([line:%d]): PAPI_Alloc(mac=[mac:%m] to=[dest:%s]:[port:%d] oper-type=[type:$%d]) Failed, error:[err:%s] This indicates failed to send PAPI message. 525002@[func:%s]([line:%d]): PAPI_Send(mac=[mac:%m] seqNum=[seqnum:%d] to=[port:%d] oper-type=[type:$%d]) Failed, error:[err:%s] This indicates failed to send PAPI message. 525003@[func:%s]([line:%d]): PAPI_Alloc(mac=[mac:%m] seqNum=[seqnum:%d] to=[port:%d] oper-type=[type:$%d]) Failed, error:[err:%s] This indicates failed to allocate PAPI buffer. 525004@[func:%s]([line:%d]): Unsupported group [group:%d]. (mac=[mac:%m] seqNum=[seqnum:%d]) This indicates unsupported group in the SAE requests 525005@[func:%s]([line:%d]): Resource allocation failed.(mac=[mac:%m] seqNum=[seqnum:%d]) This indicates failed to allocate the resource 525006@[func:%s]([line:%d]): Crypto operation failed.(mac=[mac:%m] seqNum=[seqnum:%d] group=[group:%d]) This indicates failed to do crypto operation 525100@OWE: Station=[mac:%m] BSS=[bss:%m] with DH-Group=[grp:%u] failed to update PMK at authmgr. This indicates failure while updating PMK-Info for an OWE client. 527001@Update [data:%s] Hostname and IP address update from mDNS proxy (mdns) Service information		

ID	Type	Message	Description	Action			
413001	413001	Alert	FIPS Alert: [msg:%s]	This is a FIPS alert log in wireless module.			
413002	413002	Critical	FIPS Critical: [msg:%s]	This is a FIPS critical log in wireless module.			
400101	400100	Debug	AP [name:%s]: LED state [state:%x]				
400110	400101	Debug	AP [name:%s]: Unidentified rate [val1:%x] [val2:%x]				
400131	400110	Debug	AP [name:%s]: Delete AP state for bssid [bss:%m]; Deauth [deauth:%d] Clear [clear:%d]				
400132	400131	Debug	AP [name:%s]: SAPCP Received SAPCP Probe - [band:%s]- [bssis:%m]				
400133	400132	Debug	AP [name:%s]: SAPCP Sending SAPCP Probe Response				
400134	400133	Debug	AP [name:%s]: SAPCP Probe from unknown bssid [bss:%m], dropping				
400161	400134	Debug	AP [name:%s]: SAPCP: Unknown sap				
400162	400161	Debug	AP [name:%s]: Registering AP: IP [apip:%P], BSS [bss:%m], [phy:%s] band, [T:%s] mode, max clients [MC:%d], [CV:%d%] virtual APs				
400166	400162	Debug	AP [name:%s]: Registering AP, new virtual ap for ESSID [ess:%s], deny broadcast [db:%d]				
400191	400166	Debug	[msg:%s]				
404014	400191	Debug	BSSID [bssid:%m]: STA [sta:%m] AID [aid:%d]: Duplicate AID on STA [osta:%m]				
404050	404014	Debug	AM: [msg:%s]	To be filled out			
404051	404050	Debug	AM [bssid:%s]: ARM Channel [channel:%d] Physical_Error_Rate [per:%d] MAC_Error_Rate [mer:%d] Frame_Retry_Rate [frr:%d] arm_error_rate_threshold [arm_error_rate_threshold:%d] arm_error_rate_wait_time [arm_error_rate_wait_time:%d]	The channel's error rate exceeds the error rate threshold, and it lasted more than the error rate wait time.			
404053	404051	Debug	AM: ARM Channel [channel:%d] Current Noise Level [noise:%d] ARM Noise threshold [arm_noise_threshold:%d] ARM Noise wait time [arm_noise_wait_time:%d]	This log indicates that radio changed the channel due to High Noise detection on the current channel.			
404054	404053	Debug	AM: ARM Channel [channel:%d] Current Channel Quality Level [ch_quality:%d] ARM Channel Quality threshold [arm_channel_quality_threshold:%d] ARM Channel Quality wait time [arm_channel_quality_wait_time:%d]	This log indicates that radio changed the channel when the channel quality is below the channel quality threshold.			
404055	404054	Debug	AM: ARM Defer scan [channel:%d][sec_offset:%s] because of DFS non-occupancy	Avoid scanning when in DFS non-occupancy duration			
404056	404055	Debug	AM: ARM channel [channel:%d] CCA stats ibss [ibss:%d] ibss_thresh [ibss_thresh:%d] intf [intf:%d] intf_thresh [intf_thresh:%d] load_aware_scan_rej_consec [load_aware_scan_rej_consec:%d] bcn_fails [bcn_fails:%d] bcn_fails_thresh [bcn_fails_thresh:%d] dynamic_bw_check [dynamic_bw_check:%d]	This log indicates the channel cca stats.			
408004	404056	Debug	AM: clear dynamic bandwidth observation window reason [reason:%s], before clear: load_aware_scan_rej_consec [load_aware_scan_rej_consec:%d] bcn_fails [bcn_fails:%d] dynamic_bw_check [dynamic_bw_check:%d]	This log indicates that ARM clear dynamic bandwidth observation window			
408005	408004	Debug	[msg:%s]				
409004	408005	Debug	[func:%s]: [msg:%s]				
409005	409004	Debug	[msg:%s]				
410004	409005	Debug	[func:%s], [msg:%s]				
410005	410004	Debug	[msg:%s]				
411000	410005	Debug	[func:%s], [msg:%s]				
412166	411000	Debug	[msg:%s]	Wireless BSSID debug messages for mDNS proxy (mdns)			
413007	412166	Debug	[msg:%s]				
499800	413007	Debug	FIPS Debug: [function:%s], [file:%s]:[line:%d]: [msg:%s]	This is a FIPS debugging log in wireless module.			
413000	499800	Debug	[function:%s], [file:%s]:[line:%d]: [error:%s]	This is an internal wireless debugging log.			
400143	413000	Emergency	FIPS Emergency: [msg:%s]	This is a FIPS emergency log in wireless module.			
408000	400143	Error	AP [name:%s]: ESSID mismatch index [ndx:%d]. expected [e1:%s] got [e2:%s]	An internal error has occurred.	Contact Aruba tech-support.		
408001	400144	Error	AP [name:%s]: Station [sta:%m] not found while clearing association	An internal error has occurred.	Contact Aruba tech-support.		
409000	408000	Error	Unexpected (fw_visibility process) runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the fw_visibility process. Report to technical support.			
409001	408001	Error	Unexpected (fw_visibility process) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the fw_visibility process. Report to technical support.			
410000	409000	Error	Unexpected Spectrum process runtime error at [func:%s], [line:%d]	Unexpected condition occurred in Spectrum process. Report to technical support.			
410001	409001	Error	Unexpected Spectrum process runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in Spectrum process. Report to technical support.			
413003	410000	Error	Unexpected proc (Misc Process) runtime error at [func:%s], [line:%d]	Unexpected condition occurred in the Misc process (misc-proc). Report to technical support.			
400189	410001	Error	Unexpected proc (Misc Process) runtime error at [func:%s], [line:%d], [data:%s]	Unexpected condition occurred in the Misc process (misc-proc). Report to technical support.			
400193	413003	Error	FIPS Error: [msg:%s]	This is a FIPS error log in wireless module.			

408002	400189	Info	Station EDCA parameters configured: AC=[ac:%s] params=[af:%d] [cmin:%d] [cmax:%d] [t:%d] [acm:%d]				
408003	400193	Info	VPOOL: STA [mac:%m] at AP [ip:%P]-[bssid:%m]-[name: %s] assigned vlan [vid:%d]	This message indicates VLAN assigned to a new station			
409002	403000	Info	SSID change detected by Probe:[ap_name:%s] for AP:[ap_bssid:%s]: New-SSID:[new_ssid:%s] Old-SSID:[old_ssid:%s]	To be filled out			
409003	408002	Info	[msg:%s]				
410002	408003	Info	[func:%s]: [msg:%s]				
410003	409002	Info	[msg:%s]				
413006	409003	Info	[func:%s], [msg:%s]				
400102	410002	Info	[msg:%s]				
400160	410003	Info	[func:%s], [msg:%s]				
400168	413006	Info	FIPS Info: [msg:%s]	This is a FIPS info log in wireless module.			
400185	400102	Notice	AP [name:%s]: probe request: dropped entry in ip table for [ip:%P]				
400186	400160	Notice	AP [name:%s]: Starting to configure AP at [ap:%P]				
400187	400168	Notice	Added AP [bssid:%m]-[name:%s]				
400188	400175	Notice	AP Radio Attributes Changed - BSSID [bssid:%m] Name [name:%s] IP [ip:%P] Channel [channel:%s] Band [band:%s] HT-mode [ht_mode:%s] Bandwidth [bandwidth:%s] Tx Power [tx_power:%s]				
400190	400185	Notice	[func:%s]:[bssid:%m] High Capacity Threshold Enabled				
400192	400186	Notice	[func:%s]:[bssid:%m] High Capacity Threshold Disabled				
404083	400187	Notice	[func:%s]:[bssid:%m] Call Handoff Reservation Enabled				
404400	400188	Notice	[func:%s]:[bssid:%m] Call Handoff Reservation Disabled				
404401	400190	Notice	AP EDCA parameters configured: AC=[ac:%s] params=[af:%d] [cmin:%d] [cmax:%d] [t:%d] [acm:%d]				
404402	400192	Notice	STA [mac: %m] at AP [ip:%P]-[bssid:%m]-[name: %s] 5GHz capable.				
404403	404083	Notice	AM: Tag ([MAC:%s]) detected on channel [channel:%d], battery = [battery:%d], tx-power = [tx_pwr:%d] and notification is sent to [to:%s]	Tag chirp packet is detected and sent to rtls servers.			
412192	404400	Notice	AM:SM: Spectrum: new Wi-Fi device found = [addr:%s] SSID = [ssid:%s] BSSID [bssid_str:%s] DEVICE ID [did:%d]	This log indicates a new Wi-Fi device is detected by the spectrum radio			
413005	404401	Notice	AM:SM: Spectrum: deleting Wi-Fi device = [addr:%s] SSID = [ssid:%s] BSSID [bssid_str:%s] DEVICE ID [did:%d]	This log indicates a previously detected Wi-Fi device is being deleted due to inactivity			
400130	404402	Notice	AM:SM: Spectrum: new non-Wi-Fi device found = DEVICE ID [did:%u] Type [dytpe:%s] Signal [sig:%u] Freq [freq:%u]KHz Bandwidth [bw:%u]KHz	This log indicates a new non-Wi-Fi device is detected by the spectrum radio			
400135	404403	Notice	AM:SM: Spectrum: deleting non-Wi-Fi device = DEVICE ID [did:%d] Type [dtype:%s]	This log indicates a previously detected non-Wi-Fi device is being deleted due to inactivity			
400140	412192	Notice	STA [mac: %m] at AP [ip:%P]-[bssid:%m]-[name: %s] 5GHz capable.				
400141	413005	Notice	FIPS Notice: [msg:%s]	This is a FIPS notice log in wireless module.			
400146	400130	Warning	AP [name:%s]: SAPCP payload shorter than minimum bssid [bss:%m]; minimuum length [len:%d], actual [alen:%d]				
400150	400135	Warning	AP [name:%s]: SAPCP: Unknown frame type [type:%d]				
400165	400140	Warning	AP [name:%s]: No virtual AP defined				
400167	400141	Warning	AP [name:%s]: VLAN [vlan:%d] not found				
400169	400142	Warning	AP [name:%s]: Remote AP support not licensed; dropping request				
400171	400146	Warning	AP [name:%s]: number of VLANs limit exceeded [nvlan:%d]				
400172	400150	Warning	AP [name:%s]: GRE tunnel setup failed for bssid [bss:%m]				
400173	400165	Warning	AP [name:%s]: Too many virtual APs [nvap:%d] configured.				
400174	400167	Warning	wifi_mgmt_del_sap: sap_list for [bssid:%m]-[ip:%P] not found				
400176	400169	Warning	AP - [bssid:%m], max_clients [max_clients:%d] too big				
400177	400171	Warning	wifi_sap_down:unknown SAP IP [ip:%P] BSS [bssid:%m]				
400178	400172	Warning	wifi_load_balance:unknown SAP IP [ip:%P] BSS [bssid:%m]				
400179	400173	Warning	wifi_update_sta_vlan: AP [bssid:%m] not found				
400180	400174	Warning	wifi_update_sta_vlan: Too Many VLANs on [bssid:%m]				
400181	400176	Warning	wifi_bss_counter_measures_enable: AP [bssid:%m] not found				
400182	400177	Warning	wifi_handle_vlan_message: AP [bssid:%m]: Too Many VLANs				
400183	400178	Warning	Association Flood DoS attack detected - AP [bssid:%m]				
400184	400179	Warning	handle_ap_message_response: BSS [bssid:%m] not found				
400194	400180	Warning	handle_ap_message_response: BSS [bssid:%m] nothing outstanding				
402000	400181	Warning	handle_clear_ap_state: Unknown AP [bssid:%m]				
402001	400182	Warning	stat_update: IP Addr Mismatch SAP [bssid:%m] Wrong IP [ip:%P]				
402003	400183	Warning	[func:%s]:Unknown SAP [bssid:%m]				
402004	400184	Warning	[func:%s]:Unknown SAP [bssid:%m] Mode [fw_mode:%d]				

402005	400194	Warning	Dropping association request from [sta:%m]: too many STM_STA_MESSAGE outstanding				
403001	402000	Warning	AP [name:%s] radio [rnum:%d]: No valid channels; entering air monitor mode.	The regulatory domain profile contains no channels that can be used on this radio. The radio will run as an air monitor.			
404021	402001	Warning	AP [name:%s] radio [rnum:%d]: Unable to assign virtual AP "[vap_name:%s]"				
404046	402003	Warning	AP [name:%s] radio [rnum:%d]: No gain set; using internal antenna.				
404052	402004	Warning	AP [name:%s] radio [rnum:%d]: Too many VAPs in config ([nvaps:%d]); maximum is [maxvaps:%d].				
404061	402005	Warning	AP [name:%s] radio [rnum:%d]: 802.11b protection disabled; may cause interoperability issues				
404062	403001	Warning	Cannot set rap_type to [type:%d] for AP:[bssid:%s]	To be filled out			
404063	404021	Warning	AM [bssid:%s]: Unexpected channel [channel:%d] change by AM for RFprotect Sensor radio	This log indicates that radio changed the channel for RFprotect Sensor radio			
404064	404046	Warning	AM [bssid:%s]: Low RSSI [rssi:%d] detected for STA [mac_str:%s] BSS [bssid_str:%s] ESS [essid:%s] Deauthing STA	Handoff assist feature has detected a station below the configured signal threshold and is deauthing the station			
404065	404052	Warning	AM [bssid:%s]: [message:%s]	To be filled out			
404066	404061	Warning	AM [bssid:%s]: ARM Band Request - GC [g_covered_channels:%d] AC [a_covered_channels:%d]	To be filled out			
404067	404062	Warning	AM [bssid:%s]: ARM Band Request - AC [a_covered_channels:%d] GC [g_covered_channels:%d]	To be filled out			
404068	404063	Warning	AM [bssid:%s]: ARM Channel Band Trigger new [channel:%d]-[arm_ii_arm_ccii:%d]/[arm_nii_arm_nccii:%d] old [ap_amc_channel:%d]-[arm_ccii_arm_ii:%d]/[arm_nccii_arm_nii:%d] new_rra [min_amc_channel:%d]/[new_tx_power:%d]	This log indicates that radio changed the channel when ARM band change.			
404069	404064	Warning	AM [bssid:%s]: ARM Radar Detected Trigger Current Channel [ap_amc_channel:%d] new_rra [min_amc_channel:%d]/[new_tx_power:%d]	This log indicates that radio changed the chanel when the radar is detected without converting to APM mode			
404070	404065	Warning	AM [bssid:%s]: ARM Error Threshold Trigger Current Channel [ap_amc_channel:%d] new_rra [min_amc_channel:%d]/[new_tx_power:%d]	This log indicates that radio changed the channel due to Error detection on the current channel.			
404071	404066	Warning	AM [bssid:%s]: ARM Invalid Channel Trigger Current Channel [ap_amc_channel:%d] new_rra [min_amc_channel:%d]/[new_tx_power:%d]	This log indicates that radio changed the channel due to that the current channel is invalid.			
404072	404067	Warning	AM [bssid:%s]: ARM Active Rogue Trigger new [rogue_channel:%d] old [ap_channel:%d] new_rra [channel:%d]/[new_tx_power:%d] TCI [arm_tci:%d]	This log indicates that radio changed the channel due to active rogue AP.			
404073	404068	Warning	AM [bssid:%s]: ARM Noise Threshold Trigger Current Channel [ap_channel:%d] new_rra [zero_ci_channel:%d]/[new_tx_power:%d]	This log indicates that radio changed the channel due to High Noise detection on current channel			
404074	404069	Warning	AM [bssid:%s]: ARM Channel Interference Trigger new [min_amc_channel:%d]-[arm_nii_arm_nccii:%d] old [ap_amc_channel:%d]-[arm_nccii_arm_nii:%d] new_rra [channel:%d]/[new_tx_power:%d] TCI [arm_tci:%d] Dyn Free ch idx [dfch:%d]	This log indicates that radio changed the channel due to Interference detection on the current channel.			
404075	404070	Warning	AM [bssid:%s]: ARM Empty Channel Trigger new [empty_amc_channel:%d]-[empty_amc_arm_ii:%d]/[empty_amc_arm_nii:%d] old [ap_amc_channel:%d]-[ap_amc_arm_ii:%d]/[ap_amc_arm_nii:%d] new_rra [channel:%d]/[new_tx_power:%d]	This log indicates that radio moved to the channel without other APs.			
404076	404071	Warning	AM [bssid:%s]: ARM Empty Co Channel Trigger new [empty_amc_channel:%d]-[empty_amc_arm_ii:%d]/[empty_amc_arm_nii:%d] old [ap_amc_channel:%d]-[ap_amc_arm_ii:%d]/[ap_amc_arm_nii:%d] new_rra [channel:%d]/[new_tx_power:%d]	This log indicates that radio changed the channel for Empty Co Channel Trigger.			
404077	404072	Warning	AM [bssid:%s]: ARM - too much power decreasing... cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d]/[arm_max_tx_power:%d]	This log indicates that radio changed the power when the current power is over the ARM maximum limits			
404085	404073	Warning	AM [bssid:%s]: ARM - too little power increasing... cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d]/[arm_min_tx_power:%d]	This log indicates that radio changed the power when the current power is under the ARM minmum limits			
404086	404074	Warning	AM [bssid:%s]: ARM - increasing power cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d]/[current_tx_power_1:%d]	This log indicates that radio increased the power on the current channel			
404087	404075	Warning	AM [bssid:%s]: ARM - decreasing power cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d]/[current_tx_power_2:%d]	This log indicates that radio decreased the power on the current channel			
404088	404076	Warning	AM [bssid:%s]: Radar detected on interface [interface:%s], channel [channel:%d], typeid [typeid:%d]	This log indicates that radio changed the channel due to Radar detection on the current channel			
404089	404077	Warning	AM [bssid:%s]: ARM Channel Quality Threshold Trigger Current Channel [ap_channel:%d] new_rra [zero_ci_channel:%d]/[new_tx_power:%d]	This log indicates that the radio changed the channel due to Channel Quality dropping below the threshold on the current channel.			

404090	404085	Warning	AM [bssid:%s]: ARM HT Channel Interference Trigger new [min_amc_channel:%d][min_amc_channel_sec:%s]/[arm_pii:%d] old [ap_amc_channel:%d][ap_amc_channel_sec:%s]/[old_arm_pii:%d] new_rra [channel:%d][secondary:%s]/[new_tx_power:%d] TCI [arm_tci:%d] Dyn Free ch idx [dfch:%d]	This log indicates that radio changed the channel due to Interference detection on the current HT channel.			
404092	404086	Warning	AM [bssid:%s]: ARM HT Noise Threshold Trigger Current Channel [ap_channel:%d][ap_sec_channel:%s] new_rra [zero_ci_channel:%d][zero_ci_channel_sec:%s]/[new_tx_power:%d]	This log indicates that radio changed the channel due to High Noise detection on current HT channel.			
404093	404087	Warning	AM [bssid:%s]: ARM Invalid HT Channel Trigger Current Channel old [ap_amc_channel:%d][ap_amc_sec_channel:%s] new [min_amc_channel:%d][min_sec_channel:%s]/[new_tx_power:%d]	This log indicates that radio changed the channel when the current channel is invalid on the HT channel.			
404094	404088	Warning	AM [bssid:%s]: ARM HT Radar Detected Trigger Current Channel old [ap_amc_channel:%d][ap_amc_sec_channel:%s] new [min_amc_channel:%d][min_sec_channel:%s]/[new_tx_power:%d]	This log indicates that radio changed the chanel when the radar is detected without converting to APM mode on the HT channel.			
404095	404089	Warning	AM [bssid:%s]: ARM HT Error Threshold Trigger Current Channel old [ap_amc_channel:%d][ap_amc_sec_channel:%s] new [min_amc_channel:%d][min_sec_channel:%s]/[new_tx_power:%d]	This log indicates that radio changed the channel due to Error detection on the current channel on the HT channel.			
404096	404090	Warning	AM [bssid:%s]: ARM HT Channel Quality Threshold Trigger Current Channel [ap_channel:%d][ap_sec_channel:%s] new_rra [zero_ci_channel:%d][zero_ci_channel_sec:%s]/[new_tx_power:%d]	This log indicates that the radio changed the channel due to Channel Quality dropping below the threshold on the current HT channel.			
404097	404092	Warning	AM [bssid:%s]: ARM HT Channel Band Trigger new [channel:%d][sec_channel:%s]/[arm_ii_arm_ccii:%d]/[arm_nii_arm_nccii:%d] old [ap_amc_channel:%d][ap_amc_channel_sec:%s]/[arm_ccii_arm_ii:%d]/[arm_nccii_arm_nii:%d] new_rra [min_amc_channel_pri:%d][min_amc_channel_sec:%s]/[new_tx_power:%d]	This log indicates that ARM change the channel when band change on the HT channel.			
404098	404093	Warning	AM [bssid:%s]: ARM HT Empty Channel Trigger new [empty_amc_channel:%d][empty_amc_channel_sec:%s]/[empty_amc_arm_ii:%d]/[empty_amc_arm_nii:%d] old [ap_amc_channel:%d][ap_amc_channel_sec:%s]/[ap_amc_arm_ii:%d]/[ap_amc_arm_nii:%d] new_rra [channel:%d][channel_sec:%s]/[new_tx_power:%d]	This log indicates that radio moved to the channel without other APs on the HT channel.			
404099	404094	Warning	AM [bssid:%s]: ARM HT Empty Co Channel Trigger new [empty_amc_channel:%d][empty_amc_channel_sec:%s]/[empty_amc_arm_ii:%d]/[empty_amc_arm_nii:%d] old [ap_amc_channel:%d][ap_amc_channel_sec:%s]/[ap_amc_arm_ii:%d]/[ap_amc_arm_nii:%d] new_rra [channel:%d][channel_sec:%s]/[new_tx_power:%d]	This log indicates that radio changed the channel for Empty Co Channel Trigger on the HT channel.			
404100	404095	Warning	AM [bssid:%s]: ARM - HT too much power decreasing... cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d][sec_channel:%s]/[arm_max_tx_power:%d]	This log indicates that radio changed the power when the current power is over the ARM maximum limit of the HT channel.			
404102	404096	Warning	AM [bssid:%s]: ARM - HT too little power increasing... cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d][sec_channel:%s]/[arm_min_tx_power:%d]	This log indicates that radio changed the power when the current power is under the ARM minmum limit of the HT channel			
404103	404097	Warning	AM [bssid:%s]: ARM - HT increasing power cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d][sec_channel:%s]/[current_tx_power_1:%d]	This log indicates that radio increased the power on the HT channel			
404104	404098	Warning	AM [bssid:%s]: ARM - HT decreasing power cov-index [arm_ci:%d]/[arm_nci:%d] tx-power [current_tx_power:%d] new_rra [current_channel:%d][sec_channel:%s]/[current_tx_power_2:%d]	This log indicates that radio decreased the power on the HT channel			
404105	404099	Warning	AM [bssid:%s]: Tx Hang: Driver reset radio to 20 MHz mode [current_channel:%d][current_sec_channel:%s]	This channel change indicates that the bandwidth was downgraded to 20MHz due to Tx Hang detection on the current channel			
404106	404100	Warning	AM [bssid:%s]: Tx Hang cleared: Set radio back to 40 MHz mode [current_channel:%d][current_sec_channel:%s]	This channel change indicates that the bandwidth recovered to 40MHz due to Tx Hang was Cleared on the current channel			
404107	404102	Warning	AM [bssid:%s]: ARM - Radar event cleared on channel [radar_channel:%d]	This log indicates that the previous channel was recovered due to Radar clearance.			
404108	404103	Warning	AM [bssid:%s]: ARM No alternate channel available after radar detection converting to APM mode Current Channel [ap_amc_channel:%d][current_sec_channel:%s] Current TxPower [tx_power:%d]	Radio was turned into APM mode due to no more channels available after Radar was detected on all of them.			
404404	404104	Warning	AM [bssid:%s]: ARM Radar event cleared. Converting APM back to AP on Channel [ap_amc_channel:%d][current_sec_channel:%s] Current TxPower [tx_power:%d]	This log indicates that the radar event cleared, the radio converting APM back to AP.			
404405	404105	Warning	AM [bssid:%s]: ARM Dynamic Channel Trigger [channel:%d][sec_channel:%s] old [ap_amc_channel:%d][ap_amc_channel_sec:%s]	This log indicates that the radio move to another channel if dynamic_bw signature detected			

404406	404106	Warning	AM [bssid:%s]: ARM HT Channel CCA Interference Trigger new [min_amc_channel:%d][min_amc_channel_sec:%s] old [ap_amc_channel:%d][ap_amc_channel_sec:%s]	This log indicates that radio changed the channel when encounter the channel interference on the HT channel.			
410006	404107	Warning	AM [bssid:%s]: Invalid NBR Measurement type [mtype:%d] from source [source_bssid:%s] channel [channel:%d] band [band:%d]	This log indicates invalid measurement received from Neighboring AP			
410007	404108	Warning	AM [bssid:%s]: ARM - Noise event cleared on channel [noise_channel:%d]	This log indicates Noise Clear Event on the Solver's Channel			
413004	404404	Warning	AM [bssid:%s]: AP to APM : Too much coverage on channel [channel:%d] coverage [arm_ci:%d] tx-power [current_tx_power:%d]	Radio is converted into APM mode due to mode-aware and too much coverage on the current channel.			
	404405	Warning	AM [bssid:%s]: Coverage hole: APM converting to AP on channel [channel:%d] coverage [amc_covera	Radio turned back to AP mode since a coverage hole was discovered on the current channel.			
	404406	Warning	AM [bssid:%s]:SM: Unexpected channel [channel:%d] change by AM for Spectrum Monitor radio	Changing the channel for a Radio which has spectrum monitoring turned on.			
	410006	Warning	[msg:%s]				
	410007	Warning	[func:%s], [msg:%s]				
	413004	Warning	FIPS Warning: [msg:%s]	This is a FIPS warning log in wireless module.			