

# RUCKUS SmartZone 300 and Virtual SmartZone High Scale Alarm and Event Reference Guide, 5.2.1

Supporting SmartZone 5.2.1

# Copyright, Trademark and Proprietary Rights Information

© 2020 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

*These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.*

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

---

<b>Preface</b> .....	<b>23</b>
Document Conventions.....	23
Notes, Cautions, and Safety Warnings.....	23
Command Syntax Conventions.....	23
Document Feedback.....	24
RUCKUS Product Documentation Resources.....	24
Online Training Resources.....	24
Contacting RUCKUS Customer Services and Support.....	25
What Support Do I Need?.....	25
Open a Case.....	25
Self-Service Resources.....	25
<b>About This Guide</b> .....	<b>27</b>
Introduction.....	27
What's New in This Document.....	28
Terminology.....	28
<b>Alarm and Event Management</b> .....	<b>33</b>
Overview.....	33
Alarm and Event Management.....	33
Event Categories.....	33
Event Attributes.....	34
Generation of Alarm and Event.....	34
<b>Alarm Types</b> .....	<b>37</b>
Introduction.....	37
Accounting Alarms.....	37
Accounting server not reachable.....	38
Accounting failed over to secondary.....	38
Accounting fallback to primary.....	38
AP accounting message mandatory parameter missing.....	39
AP accounting message decode failed.....	40
AP account message drop while no accounting start message.....	40
Unauthorized CoA/DM message dropped.....	41
AP Authentication Alarms.....	41
RADIUS server unreachable.....	41
LDAP server unreachable.....	42
AD server unreachable.....	42
WeChat ESP authentication server unreachable.....	43
WeChat ESP authentication server unresolvable.....	43
WeChat ESP DNAT server unreachable.....	43
WeChat ESP DNAT server unresolvable.....	44
AP Communication Alarms.....	44
AP rejected.....	45
AP configuration update failed.....	45
AP swap model mismatched.....	45
AP pre-provision model mismatched.....	46
AP firmware update failed.....	46

AP WLAN oversubscribed.....	47
AP join zone failed.....	47
AP image signing failed.....	47
AP LBS Alarms.....	48
No LS responses.....	49
LS authentication failure.....	49
AP failed to connect to LS.....	49
AP State Change Alarms.....	50
AP rebooted by system.....	50
AP disconnected.....	51
AP deleted.....	51
AP cable modem interface down.....	51
AP DHCP service failure.....	52
AP NAT failure.....	52
AP DHCP/NAT DWPDP Ethernet port configuration override.....	52
SZ DHCP/NAT DWPDP Ethernet port configuration override.....	53
SIM removal.....	53
AP System Anomaly.....	54
Authentication Alarms.....	54
Authentication server not reachable.....	54
Authentication failed over to secondary.....	55
Authentication fallback to primary.....	55
AD/LDAP connectivity failure.....	55
Bind fails with AD/LDAP.....	56
Bind success with LDAP, but unable to find clear text password for the user.....	56
RADIUS fails to connect to AD NPS server.....	57
RADIUS fails to authenticate with AD NPS server.....	57
Fails to establish TLS tunnel with AD/LDAP.....	58
Control and Data Plane Interface Alarms.....	58
GtpManager (DP) disconnected.....	59
Cloud Alarms.....	59
Cloud Analytics Service has been Enabled.....	59
Cloud Analytics Service has been Disabled.....	59
Cloud Analytics Disconnected.....	60
Cluster Alarms.....	60
New node failed to join.....	61
Node removal failed.....	61
Node out of service.....	62
Cluster in maintenance state.....	62
Cluster backup failed.....	63
Cluster restore failed.....	63
Cluster upgrade failed.....	64
Cluster application stopped.....	64
Node bond interface down.....	65
Node physical interface down.....	65
Cluster node rebooted.....	66
Cluster node shut down.....	66
Node IP Changed.....	67
Disk usage exceed threshold.....	67
Cluster out of service.....	67

Cluster upload AP firmware failed.....	68
Cluster add AP firmware failed.....	68
Unsync NTP time.....	69
Cluster upload KSP file failed.....	69
Configuration backup failed.....	69
Configuration restore failed.....	70
AP certificate updated.....	70
Upgrade SS table failed.....	70
Cluster redundancy sync configuration failed.....	71
Cluster redundancy restoring configuration failed.....	71
Not all APs rehome after timeout.....	71
Over switch max capacity.....	72
AP is connected to Standby Cluster Over The Expiration Date.....	72
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy.....	72
External DP Connected to Standby Cluster after Rehome Timeout.....	73
Certificate is about to Expire.....	73
Certificate is already Expired.....	73
Configuration Alarms.....	74
Zone configuration preparation failed.....	74
AP configuration generation failed.....	74
End-of-life AP model detected.....	75
VLAN configuration mismatch on non DHCP/NAT WLAN.....	75
VLAN configuration mismatch on DHCP/NAT WLAN.....	75
Data Plane Alarms.....	76
Data plane configuration update failed.....	76
Data plane disconnected.....	77
Data plane physical interface down.....	77
Data plane rebooted.....	78
Data plane packet pool is under low water mark.....	78
Data plane packet pool is under critical low water mark.....	78
Data plane core dead.....	79
Data plane process restarted.....	79
Data plane license is not enough.....	79
Data plane upgrade failed.....	80
Data plane of data center side fails to connect to the CALEA server.....	81
Data plane fails to connects to the other data plane.....	81
Data plane DHCP IP pool usage rate is 100 percent.....	81
Data Streaming Alarms.....	82
Connecting Failure to a Data Streaming Profile.....	82
Gn/S2a Interface Alarms.....	82
GGSN restarted.....	83
GGSN not reachable.....	83
GGSN not resolved.....	83
PDNGW could not be resolved.....	84
PDNGW version not supported.....	84
Associated PDNGW down.....	85
Create session response failed.....	85
Decode failed.....	86
Modify bearer response failed.....	86
Delete session response failed.....	86

Delete bearer request failed.....	87
Update bearer request failed.....	87
CGF server not configured.....	88
GR Interface Alarms.....	88
Destination not reachable.....	88
App server down.....	89
App server inactive.....	89
Association establishment failed.....	90
Association down.....	90
Outbound routing failure.....	91
Did allocation failure.....	91
IPMI Alarms.....	91
ipmiVoltage.....	93
ipmiThempBB.....	94
ipmiThempFP.....	94
ipmiThempIOH.....	95
ipmiThempMemP.....	95
ipmiThempPS.....	96
ipmiThempP.....	96
ipmiThempHSBP.....	96
ipmiFan.....	97
ipmiPower.....	97
ipmiCurrent.....	98
ipmiFanStatus.....	98
ipmiPsStatus.....	98
ipmiDrvStatus.....	99
Licensing Alarms.....	99
TTG session critical threshold.....	100
TTG session license exhausted.....	100
License going to expire.....	100
Insufficient license capacity.....	101
Data plane DHCP IP license insufficient.....	101
Data plane NAT session license insufficient.....	101
Insufficient license capacity .....	102
PMIPv6 Alarms.....	102
Config update failed.....	102
DHCP connection lost.....	103
SCI Alarms.....	103
Connect to SCI failure.....	104
SCI has been disabled.....	104
SCI and FTP have been disabled.....	104
Session Alarms.....	105
Binding failed.....	105
System Alarms.....	105
No LS responses.....	106
LS authentication failure.....	106
{produce.short.name} failed to connect to LS.....	107
Syslog server unreachable.....	107
CSV export FTP maximum retry.....	108
CSV export disk threshold exceeded.....	108

CSV export disk max capacity reached.....	108
Process restart.....	109
Service unavailable.....	109
Keepalive failure.....	109
Resource unavailable.....	110
HIP failed over.....	110
Unconfirmed program detection.....	111
Diameter initialization error.....	111
Diameter peer transport failure.....	112
Diameter CER error.....	112
Diameter peer add error.....	113
Diameter peer remove successful.....	113
Diameter realm entry error.....	114
Diameter failover to alternate peer.....	114
Diameter fail back to peer.....	115
Diameter CEA unknown peer.....	115
Diameter no common application.....	116
Process initiated.....	116
PMIPv6 unavailable.....	117
Memory allocation failed.....	117
The last one data plane is disconnected zone affinity profile alarm.....	117
Switch.....	118
Power supply failure.....	118
Fan failure.....	119
Module insertion.....	119
Module removal.....	119
Temperature above threshold warning.....	120
Stack member unit failure.....	120
PoE power allocation failure.....	121
DHCP_Snooping: DHCP offer dropped message.....	121
Port put into error disable state.....	121
Switch offline.....	122
Switch duplicated.....	122
Reject certificate signing request.....	122
Pending certificate signing request.....	123
Switch CPU major threshold exceed .....	123
Switch CPU critical threshold exceed .....	123
Switch memory major threshold exceed .....	124
Switch memory critical threshold exceed .....	124
Switch custom major threshold exceed .....	124
Switch custom critical threshold exceed .....	125
Switch Firmware Upgrade Failed.....	125
Switch Configuration Update Failed.....	125
Threshold Alarms.....	125
CPU threshold exceeded.....	126
Memory threshold exceeded.....	126
Disk usage threshold exceeded.....	127
The drop of client count threshold exceeded.....	127
License threshold exceeded.....	128
HDD Health Degradation.....	128

Rate limit for TOR surpassed.....	128
The number of users exceeded its limit.....	129
The number of devices exceeded its limit.....	129
Over AP maximum capacity.....	130
Over Device maximum capacity.....	130
Tunnel Alarms - Access Point.....	130
AP softGRE gateway not reachable.....	130
AP is disconnected from secure gateway.....	131
AP secure gateway association failure.....	131
<b>Events Types.....</b>	<b>133</b>
3rd Party Access Point Events.....	133
3rd party AP connected.....	134
Accounting Events.....	134
Accounting session disabled.....	134
Accounting server not reachable.....	135
Accounting failed over to secondary.....	135
Accounting fallback to primary.....	136
AP accounting message mandatory parameter missing.....	136
Unknown realm.....	136
AP accounting message decode failed.....	137
AP accounting retransmission message dropped.....	137
AP accounting response while invalid config.....	138
AP account message drop while no accounting start message.....	138
Unauthorized COA/DM message dropped.....	138
AP Authentication Events.....	139
Radius server reachable.....	140
Radius server unreachable.....	140
LDAP server reachable.....	140
LDAP server unreachable.....	141
AD server reachable.....	141
AD server unreachable.....	141
Wechat ESP authentication server reachable.....	142
WeChat ESP authentication server unreachable.....	142
WeChat ESP authentication server resolvable.....	142
WeChat ESP authentication server unresolvable.....	143
WeChat ESP DNAT server reachable.....	143
WeChat ESP DNAT server unreachable.....	143
WeChat ESP DNAT server resolvable.....	144
WeChat ESP DNAT server unresolvable.....	144
Authentication Attempts.....	144
Authentication Unsuccessful.....	145
Authentication Re-attempt.....	145
Authentication 8021.....	145
AP Local Session Timeout.....	145
AP Remote Session Timeout.....	146
AP Interactive Session Termination.....	146
AP Communication Events.....	146
AP discovery succeeded.....	147
AP managed.....	148
AP rejected.....	148



AP firmware updated.....	148
AP firmware update failed.....	149
Updating AP firmware.....	149
Updating AP configuration.....	149
AP configuration updated.....	150
AP configuration update failed.....	150
AP pre-provision model mismatched.....	150
AP swap model mismatched.....	151
AP WLAN oversubscribed.....	151
AP join zone failed.....	151
AP illegal to change country code.....	152
AP configuration get failed.....	152
Rogue AP.....	152
Rogue AP disappeared.....	152
Classified Rogue AP.....	153
AP image signing failed.....	153
Jamming attack.....	153
Rogue client.....	154
Key gen fail.....	154
Key dis fail.....	154
Key dis fail GTK.....	155
wpaendec fail.....	155
IPsecsec fail.....	155
Fw manual initiation.....	156
AP Management TSF data.....	156
AP TSF failure.....	156
AP Self tests.....	157
Firmware initiation update.....	157
SSH initiation.....	157
SSH termination.....	158
SSH failure.....	158
TLS initiation.....	158
TLS termination.....	158
TLS failure.....	159
IP sec initiation.....	159
IP sec termination.....	159
IP sec failure.....	160
AP LBS Events.....	160
No LS responses.....	160
LS authentication failure.....	161
AP connected to LS.....	161
AP failed to connect to LS.....	161
AP started location service.....	161
AP stopped location service.....	162
AP received passive calibration request.....	162
AP received passive footfall request.....	162
AP received unrecognized request.....	163
AP Mesh Events.....	163
EMAP downlink connected to MAP.....	163
EMAP downlink disconnected from MAP.....	164

EMAP uplink connected to MAP.....	164
EMAP uplink disconnected from MAP.....	164
MAP disconnected.....	165
MAP downlink connected.....	165
MAP downlink connected to EMAP.....	165
MAP downlink disconnected from EMAP.....	166
RAP downlink connected to MAP.....	166
MAP uplink connected to EMAP.....	166
MAP uplink disconnected from EMAP.....	166
MAP uplink connected to RAP.....	167
MAP uplink connected to MAP.....	167
Mesh state updated to MAP.....	167
Mesh state updated to MAP no channel.....	168
Mesh state updated to RAP.....	168
Mesh state update to RAP no channel.....	168
MAP downlink connected to MAP.....	169
MAP downlink disconnected from MAP.....	169
RAP downlink disconnected from MAP.....	169
AP State Change Events.....	170
AP rebooted by user.....	170
AP rebooted by system.....	171
AP disconnected.....	171
AP IP address updated.....	171
AP reset to factory default.....	172
AP channel updated.....	172
AP country code updated.....	172
AP channel updated because dynamic frequency selection (DFS) detected a radar.....	172
AP change control plane.....	173
AP connected.....	173
AP deleted.....	173
AP heartbeat lost.....	174
AP tagged as critical.....	174
AP cable modem interface down.....	174
AP brownout.....	175
AP cable modem power-cycled by user.....	175
AP smart monitor turn off WLAN.....	175
AP client load balancing limit reached.....	175
AP client load balancing limit recovered.....	176
AP WLAN state changed.....	176
AP capacity reached.....	176
AP capacity recovered.....	177
AP cable modem interface up.....	177
AP cable modem soft-rebooted by user.....	177
AP cable modem set to factory default by user.....	178
AP health high latency flag.....	178
AP health low capacity flag.....	178
AP health high connection failure flag.....	179
AP health high client count flag.....	179
AP health high latency clear.....	179
AP health low capacity clear.....	180

AP health high connection failure clear.....	180
AP health high client count clear.....	180
Primary DHCP AP is down.....	181
Primary DHCP AP is up.....	181
Secondary DHCP AP is down.....	181
Secondary DHCP AP is up.....	182
Primary or secondary DHCP AP detects 90% of the configured total IPs.....	182
Both primary and secondary DHCP server APs are down.....	182
AP NAT gateway IP failover detected for particular VLAN pool.....	182
AP NAT gateway IP fall back detected for particular VLAN pool.....	183
NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool.....	183
NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up.....	184
AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down.....	184
AP health high airtime utilization flag.....	184
AP health high airtime utilization clear.....	185
AP cluster failover.....	185
AP cluster rehome.....	185
AP switchover cluster failed.....	186
AP MAC OUI violation.....	186
Backhaul switched to primary.....	186
Backhaul switched to secondary.....	187
LTE network connectivity lost.....	187
Ethernet network connectivity lost.....	187
LTE DHCP timeout.....	187
Ethernet link down.....	188
Ethernet link up.....	188
SIM switch.....	188
Remote host blacklisted.....	189
SIM removal.....	189
LTE network registration status.....	189
LTE connection status.....	189
LTE good rssi status.....	190
LTE weak rssi status.....	190
AP client load balancing limit reached.....	190
AP client load balancing limit recovered.....	191
AP System Anomaly.....	191
AP USB Events.....	191
AP USB software package downloaded.....	191
AP USB software package download failed.....	192
Authentication Events.....	192
Authentication server not reachable.....	193
Unknown realm.....	193
Authentication succeeded.....	193
Authentication failed.....	194
Pseudonym authentication succeeded.....	194
Pseudonym authentication failed.....	194
Fast re-authentication succeeded.....	195
Fast re-authentication failed.....	195

Authentication failed over to secondary.....	196
Authentication fallback to primary.....	196
AD/LDAP connected successfully.....	196
AD/LDAP connectivity failure.....	197
Bind fails with AD/LDAP.....	197
Bind success with LDAP, but unable to find clear text password for the user.....	197
RADIUS fails to connect to AD NPS server.....	198
RADIUS fails to authenticate with AD NPS server.....	198
Successfully established the TLS tunnel with AD/LDAP.....	198
Fails to establish TLS tunnel with AD/LDAP.....	199
TLS Establishment Failed between SZ and external AAA Server.....	199
Authorization Events.....	200
DM received from AAA.....	200
DM NACK sent to AAA.....	200
DM sent to NAS.....	201
DM NACK received from NAS.....	201
CoA received from AAA.....	201
CoA NACK sent to AAA.....	202
CoA sent NAS.....	202
CoA NAK received NAS.....	202
CoA authorize only access reject.....	203
CoA RWSG MWSG notification failure.....	203
Control and Data Plane Interface.....	203
DP connected.....	204
GtpManager (DP) disconnected.....	204
Session updated at DP.....	204
Session update at DP failed.....	205
Session deleted at DP.....	205
Session delete at DP failed.....	205
C2d configuration failed.....	206
Client Events.....	206
Client authentication failed.....	207
Client joined.....	208
Client failed to join.....	208
Client disconnected.....	208
Client connection timed out.....	209
Client authorization successfully.....	209
Client authorization failed.....	210
Client session expired.....	210
Client roaming.....	210
Client logged out.....	211
3rd party client join .....	211
3rd party client inactivity timeout .....	212
3rd party client authorization .....	212
3rd party client authorization failure .....	212
3rd party client session expiration .....	213
3rd party client roaming .....	213
3rd party client session logout .....	214
Client roaming disconnected.....	214
Client blocked .....	214

Client grace period .....	215
Onboarding registration succeeded .....	215
Onboarding registration failed .....	215
Remediation succeeded .....	216
Remediation failed .....	216
Force DHCP disconnected .....	216
WDS device joined .....	217
WDS device left.....	217
Client is blocked because of barring UE rule.....	217
Client is unblocked by barring UE rule.....	218
Start CALEA mirroring client.....	218
Stop CALEA mirroring client.....	218
Client information updated.....	218
Wired client joined.....	219
Wired client failed to join.....	219
Wired client disconnected.....	219
Wired client authorization successfully.....	220
Wired client session expired.....	220
Application identified.....	220
Application denied.....	221
URL filtering server unreachable.....	221
URL filtering server reachable.....	221
Packet spoofing detected.....	222
Packet spoofing detected.....	222
Packet spoofing detected.....	222
Packet spoofing detected.....	223
Cloud Events.....	223
Cloud Services Enabled.....	223
Cloud Services Disabled.....	223
Cloud Analytics Enabled.....	224
Cloud Analytics Disabled.....	224
Cloud Services Token Refreshed.....	224
Cloud Analytics Token Renewed.....	225
Cloud Analytics Service has been Enabled.....	225
Cloud Analytics service has been disabled.....	225
Cloud Analytics Disconnected.....	225
Cluster Events.....	226
Cluster created successfully.....	227
New node joined successfully.....	227
New node failed to join.....	227
Node removal completed.....	228
Node removal failed.....	228
Node out of service.....	228
Cluster in maintenance state.....	229
Cluster back in service.....	229
Cluster backup completed.....	229
Cluster backup failed.....	229
Cluster restore completed.....	230
Cluster restore failed.....	230
Cluster node upgrade completed.....	230

Entire cluster upgraded successfully.....	231
Cluster upgrade failed.....	231
Cluster application stopped.....	231
Cluster application started.....	232
Cluster backup started.....	232
Cluster upgrade started.....	232
Cluster leader changed.....	233
Node bond interface down.....	233
Node bond interface up.....	233
Node IP address changed.....	234
Node physical interface down.....	234
Node physical interface up.....	234
Cluster node rebooted.....	234
NTP time synchronized.....	235
Cluster node shutdown.....	235
Cluster upload started.....	235
Cluster upload completed.....	236
Cluster upload failed.....	236
SSH tunnel switched.....	236
Cluster remove node started.....	237
Node back in service.....	237
Disk usage exceed threshold.....	237
Cluster out of service.....	237
Initiated moving APs in node to a new cluster.....	238
Cluster upload vSZ-D firmware started.....	238
Cluster upload vSZ-D firmware completed.....	238
Cluster upload vSZ-D firmware failed.....	239
Cluster upload AP firmware started.....	239
Cluster upload AP firmware completed.....	239
Cluster upload AP firmware failed.....	240
Cluster add AP firmware started.....	240
Cluster add AP firmware completed.....	240
Cluster add AP firmware failed.....	240
Cluster name is changed.....	241
Unsync NTP Time.....	241
Cluster upload KSP file started.....	241
Cluster upload KSP file completed.....	242
Cluster upload KSP file failed.....	242
NTP unreachable server.....	242
Configuration backup started.....	243
Configuration backup succeeded.....	243
Configuration backup failed.....	243
Configuration restore succeeded.....	243
Configuration restore failed.....	244
AP Certificate Expired.....	244
AP Certificate Updated.....	244
Configuration restore started.....	245
Upgrade SSTable failed.....	245
Reindex elastic search finished.....	245
Initiated APs contact APR.....	246

All nodes back in service.....	246
Not management service ready.....	246
Management service ready.....	246
Configuration sync failed.....	247
Node IPv6 address added.....	247
AP is connected to standby cluster over the expiration date.....	247
Node IPv6 address deleted.....	248
Sync Configuration started for Cluster Redundancy.....	248
Sync Configuration Success for Cluster Redundancy.....	248
Standby Cluster Failed to Restore a Configuration for Cluster Redundancy.....	248
Standby Cluster Restores a Configuration for Cluster Redundancy.....	249
Standby Cluster Restored a Configuration Success for Cluster Redundancy.....	249
Standby Cluster Back to Monitoring Mode for Cluster Redundancy.....	249
AP Connected to Standby Cluster after Rehome Timeout.....	250
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy.....	250
External DP Connected to Standby Cluster after Rehome Timeout.....	250
Certificate is about to Expire.....	250
Certificate is already Expired.....	251
Result of Renew Certificate.....	251
Configuration Events.....	251
Configuration updated.....	252
Configuration update failed.....	252
Configuration receive failed.....	252
Incorrect flat file configuration.....	253
Zone configuration preparation failed.....	253
AP configuration generation failed.....	253
End-of-life AP model detected.....	254
VLAN configuration mismatch on non-DHCP/NAT WLAN.....	254
VLAN configuration mismatch on DHCP/NAT WLAN.....	254
Generation failed during CCM GPB generation .....	255
Preparation failed during AP knowledge generation.....	255
Generation failed during AP knowledge generation.....	255
End-of-life AP model detected during AP knowledge generation.....	256
Notification failed during AP knowledge generation.....	256
Datablade Events.....	256
DP integrity test failed.....	257
DP CLI enable failed.....	257
DP re-authentication.....	258
DP password min length updated.....	258
DP password changed.....	258
DP enable password changed.....	258
DP https authentication failed.....	259
DP certificate uploaded.....	259
DP Scg FQDN updated.....	259
DP initial upgrade.....	260
DP discontinuous time change NTP server DP Ntp time sync.....	260
DP user login.....	260
DP user login failed.....	260
DP user logout.....	261
DP account locked.....	261

DP session idle updated.....	261
DP session idle terminated.....	262
DP SSH tunnel failed.....	262
DP https connection failed.....	262
DP IPsec tunnel create failed.....	262
Data Plane Events.....	263
Data plane discovered.....	263
Data plane discovery failed.....	264
Data plane configuration updated.....	264
Data plane configuration update failed.....	264
Data plane rebooted.....	265
Data plane heartbeat lost.....	265
Data plane IP address updated.....	265
Data plane updated to a new control plane.....	265
Data plane status update failed.....	266
Data plane statistics update failed.....	266
Data plane connected.....	266
Data plane disconnected.....	267
Data plane physical interface down.....	267
Data plane physical interface up.....	267
Data plane packet pool is under low water mark.....	267
Data plane packet pool is under critical low water mark.....	268
Data plane packet pool is above high water mark.....	268
Data plane core dead.....	268
Data plane process restarted.....	269
Data plane discovery succeeded.....	269
Data plane managed.....	269
Data plane deleted.....	270
Data plane license is not enough.....	270
Data plane upgrade started.....	270
Data plane upgrading.....	271
Data plane upgrade succeeded.....	271
Data plane upgrade failed.....	271
Data plane of data center side successfully connects to the CALEA server.....	272
Data plane of data center side fails to connect to the CALEA server.....	272
Data Plane of data center side disconnects to CALEA server.....	272
Data plane successfully connects to the other data plane.....	273
Data plane fails to connect to the other data plane.....	273
Data plane disconnects to the other data plane.....	273
Start CALEA mirroring client in data plane.....	274
Stop CALEA mirroring client in data plane.....	274
Data plane DHCP IP pool usage rate is 100 percent.....	274
Data plane DHCP IP pool usage rate is 80 percent.....	275
Data plane NAT session capacity usage rate is 80 percent.....	275
Data plane NAT session capacity usage rate is 100 percent.....	276
Data plane DHCP IP capacity usage rate is 80 percent.....	276
Data plane DHCP IP capacity usage rate is 100 percent.....	276
Data plane backup success.....	277
Data plane backup failed.....	277
Data plane restore success.....	277



Data plane restore failed.....	278
dpIpmiPsStatus.....	278
dpIpmiThempIOH.....	278
dpIpmiThempMemP.....	278
dpIpmiPsStatus.....	279
dpIpmiREVoltage.....	279
dpIpmiREThempIOH.....	279
dpIpmiREThempMemP.....	280
dpIpmiRePsStatus.....	280
dpSSDHealthDegrade.....	280
Remote Administration Start.....	280
Remote Administration Stop.....	281
Data Streaming Event.....	281
Connected to Data a Streaming Endpoint.....	281
Disconnected to Data a Streaming Endpoint.....	281
Connected to Data a Streaming Endpoint Failure.....	282
DHCP Events.....	282
DHCP inform received.....	282
DHCP dcln received.....	283
GA Interface Events.....	283
Connection to CGF failed.....	283
CGF keepalive not responded .....	283
CDR transfer succeeded.....	284
CDR generation failed.....	284
CDR transfer failed.....	284
Gn/S2a Interface Events.....	285
GGSN restarted.....	285
GGSN not reachable.....	286
Echo response not received.....	286
GGSN not resolved.....	286
PDP context established.....	287
PDP create failed.....	287
PDP update by HLR succeeded.....	287
PDP update by HLR failed.....	288
PDP update by roaming succeeded.....	288
PDP update by roaming failed.....	288
PDP update by GGSN succeeded.....	289
PDP update by GGSN failed.....	289
PDP delete by TTG succeeded.....	289
PDP delete by TTG failed.....	290
PDP delete by GGSN succeeded.....	290
PDP delete by GGSN failed.....	290
IP assigned.....	291
IP not assigned.....	291
Unknown UE.....	292
PDP update success COA.....	292
PDP update fail COA.....	292
PDNGW could not be resolved.....	293
PDNGW version not supported.....	293
Associated PDNGW down.....	293

Create session response failed.....	294
Decode failed.....	294
Modify bearer response failed.....	295
Delete session response failed.....	295
Delete bearer request failed.....	295
Update bearer request failed.....	296
CGF server not configured.....	296
Gr Interface Event.....	296
Destination not reachable.....	297
Destination available.....	297
App server down.....	298
App server inactive.....	298
App server active.....	298
Association establishment failed.....	299
Association down.....	299
Association up.....	299
Send auth info success.....	300
Auth info sending failed.....	300
GPRS location update succeeded.....	300
GPRS location update failed.....	300
Insert sub data success.....	301
Insert sub data failed.....	301
Outbound routing failure.....	301
Did allocation failure.....	302
Restore data success.....	302
Restore data failed.....	302
IPMI Events.....	303
ipmiVoltage.....	303
ipmiThempBB.....	304
ipmiThempFP.....	304
ipmiThempIOH.....	304
ipmiThempMemP.....	305
ipmiThempPS.....	305
ipmiThempP.....	305
ipmiThempHSBP.....	306
ipmiFan.....	306
ipmiPower.....	306
ipmiCurrent.....	307
ipmiFanStatus.....	307
ipmiPsStatus.....	307
ipmiDrvStatus.....	308
ipmiREVotage.....	308
ipmiREThempBB.....	308
ipmiREThempFP.....	308
ipmiREThempIOH.....	309
ipmiREThempMemP.....	309
ipmiREThempPS.....	309
ipmiREThempP.....	310
ipmiREThempHSBP.....	310
ipmiREFan.....	310

ipmiREPower.....	311
ipmiRECurrent.....	311
ipmiREFanStatus.....	311
ipmiREPsStatus.....	311
ipmiREDrvStatus.....	312
Licensing Interface Events.....	312
TTG session warning threshold.....	313
TTG session major threshold.....	313
TTG session critical threshold.....	313
TTG session license exhausted.....	314
License sync succeeded.....	314
License sync failed.....	314
License import succeeded.....	315
License import failed.....	315
License data changed.....	315
License going to expire.....	315
Insufficient license capacity.....	316
Data plane DHCP IP license insufficient.....	316
Data plane NAT session license insufficient.....	316
AP number limit exceeded.....	317
Insufficient license capacity.....	317
Insufficient license capacity.....	317
Location Delivery Events.....	318
Unavailable location info requested.....	318
Incapable location info requested.....	318
Unsupported location delivery request.....	319
PMIPv6 Events.....	319
Config update failed.....	319
LMA ICMP reachable.....	320
LMA server unreachable.....	320
DHCP connected.....	320
DHCP connection lost.....	321
Session Events.....	321
Session timeout.....	321
Delete all sessions.....	322
Binding succeeded.....	322
Binding failed.....	323
Binding time expired.....	323
Binding revoked.....	323
Binding released.....	324
STA Interface Events.....	324
STA successful authentication.....	324
STA session termination {produce.short.name} initiated success.....	325
STA session termination AAA initiated success.....	325
STA session termination AAA initiated failed.....	325
STA re-authorization successful.....	326
System Events.....	326
No LS responses.....	327
LS authentication failure.....	327
{produce.short.name} connected to LS.....	328

{produce.short.name} failed to connect to LS.....	328
{produce.short.name} received passive request.....	328
{produce.short.name} sent controller information report.....	329
{produce.short.name} received management request.....	329
{produce.short.name} sent AP info by venue report.....	329
{produce.short.name} sent query venues report.....	329
{produce.short.name} sent associated client report.....	330
{produce.short.name} forwarded calibration request to AP.....	330
{produce.short.name} forwarded footfall request to AP.....	330
{produce.short.name} received unrecognized request.....	331
Syslog server reachable.....	331
Syslog server unreachable.....	331
Syslog server switched.....	332
System service failure.....	332
Generate AP config for plane load rebalance succeeded.....	332
Generate AP config for plane load rebalance failed.....	333
FTP transfer.....	333
FTP transfer error.....	333
CSV export FTP transfer.....	333
CSV export FTP transfer error.....	334
CSV export FTP transfer maximum retry.....	334
CSV export disk threshold exceeded.....	334
CSV export disk max capacity reached.....	335
CSV export disk threshold back to normal.....	335
File upload.....	335
Email sent successfully.....	336
Email sent failed.....	336
SMS sent successfully.....	336
SMS sent failed.....	337
Process restart.....	337
Service unavailable.....	337
Keepalive failure.....	338
Resource unavailable.....	338
HIP started.....	338
HIP stopped.....	339
Standby HIP restarted.....	339
HIP cache cleaned.....	339
All data planes in the zone affinity profile are disconnected.....	340
CALEA UE Matched.....	340
Diameter peer transport failure.....	340
Diameter CER error.....	341
Diameter CER success.....	341
Diameter invalid version.....	342
Diameter peer add successful.....	342
ZD AP migrating.....	343
ZD AP migrated.....	343
ZD AP rejected.....	343
ZD AP migration failed.....	344
Database error.....	344
Recover cassandra error.....	344

Process initiated.....	345
PMIPv6 unavailable.....	345
Memory allocation failed.....	345
Process stopped.....	346
SZ Login Fail.....	346
SZ Login.....	346
SZ Logout.....	346
Password expiration.....	347
Admin account lockout.....	347
Admin session expired.....	347
Disable inactive admins.....	348
Two factor auth failed.....	348
Unconfirmed program detection.....	348
Admin account lockout after failed attempts.....	349
Discontinuous time change.....	349
Mesh network connectivity lost.....	349
Failure of Key Generation.....	350
Failure of IPsec.....	350
Failure Certificate.....	350
IPsec KE is Up.....	350
IPsec IKE is Down.....	351
Discontinuous Time Change.....	351
Switch Events.....	351
Switch critical message.....	352
Switch alert message.....	352
Switch warning message.....	353
Switch CPU warning threshold exceed.....	353
Switch CPU major threshold exceed.....	353
Switch CPU critical threshold exceed.....	353
Switch memory warning threshold exceed.....	354
Switch memory major threshold exceed.....	354
Switch memory critical threshold exceed.....	354
Switch custom warning threshold exceed.....	355
Switch custom major threshold exceed.....	355
Switch custom critical threshold exceed.....	355
GetCACert Request.....	355
Certificate signing request.....	356
Accept certificate signing request.....	356
Reject certificate signing request.....	356
Pending certificate signing request.....	357
Switch is Offline for 15 Minutes.....	357
Over Switch Max Capacity.....	357
Switch Duplicated.....	357
Switch Firmware Upgrade.....	358
Switch Firmware Upgrade Failed.....	358
Switch Configuration Update.....	358
Switch Configuration Update Failed.....	359
Switch Reboot.....	359
Switch Delete.....	359
Switch Disconnected from the Controller.....	359

Switch is Connected to the Controller.....	360
Switch Discovered by the Controller.....	360
Threshold Events.....	360
CPU threshold exceeded.....	361
Memory threshold exceeded.....	361
Disk usage threshold exceeded.....	361
CPU threshold back to normal.....	362
Memory threshold back to normal.....	362
Disk threshold back to normal.....	362
License threshold exceeded.....	363
The drop of client count threshold exceeded.....	363
Rate limit threshold surpassed.....	363
Rate limit threshold restored.....	364
Rate limit for TOR surpassed.....	364
The number of users exceed its limit.....	364
The number of devices exceeded its limit.....	365
Over AP maximum capacity.....	365
Over Device Maximum Capacity.....	365
Device Capacity Threshold Back to Normal.....	366
Tunnel Events - Access Point (AP).....	366
Data plane accepted a tunnel request.....	366
Data plane rejected a tunnel request.....	367
Data plane terminated a tunnel.....	367
AP created a tunnel.....	367
AP tunnel disconnected.....	367
AP softGRE tunnel fails over primary to secondary.....	368
AP softGRE tunnel fails over secondary to primary.....	368
AP softGRE gateway reachable.....	368
AP softGRE gateway not reachable.....	369
Data plane set up a tunnel.....	369
AP secure gateway association success.....	369
AP is disconnected from secure gateway.....	370
AP secure gateway association failure.....	370
Tunnel Events - Data Plane.....	370
DP sGRE GW unreachable.....	371
DP sGRE keep alive timeout.....	371
DP sGRE GW inactive.....	371
DP DHCPRelay no response.....	372
DP DHCPRelay failover.....	372
DP sGRE new tunnel.....	372
DP sGRE del tunnel.....	373
DP sGRE keepalive recovery.....	373
DP DHCPRelay response recovery.....	373
DP sGRE GW reachable.....	373
DP sGRE GW active.....	374
DP sGRE GW failover.....	374
DP switchover.....	374
AP Ethernet Phy Error Count.....	375
AP Ethernet PHY Down Shift.....	375

# Preface

- Document Conventions..... 23
- Command Syntax Conventions..... 23
- Document Feedback..... 24
- RUCKUS Product Documentation Resources..... 24
- Online Training Resources..... 24
- Contacting RUCKUS Customer Services and Support..... 25

## Document Conventions

The following table lists the text conventions that are used throughout this guide.

**TABLE 1** Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

## Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

### NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

### ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



### CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



### DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.

## Preface

Document Feedback

Convention	Description
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.  Default responses to system prompts are enclosed in square brackets.
{ x   y   z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x   y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member</i> [ <i>member</i> ...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at [#Ruckus-Docs@commscope.com](mailto:#Ruckus-Docs@commscope.com).

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

## RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckuswireless.com>.

## Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://training.ruckuswireless.com>.



# Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckuswireless.com> and select **Support**.

## What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

## Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

## Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at [https://support.ruckuswireless.com/case\\_management](https://support.ruckuswireless.com/case_management).



# About This Guide

---

- Introduction.....27
- What's New in This Document.....28
- Terminology.....28

## Introduction

This *SmartZone Alarm and Event Reference Guide* describes the various types of alarms and events that SmartZone 300 (SZ300) and Virtual SmartZone-High-Scale (vSZ-H) (collectively referred to as “the controller” throughout this guide) generates. For each alarm and event this guide provides the code, type, attributes, and description.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting RUCKUS devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

### NOTE

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the RUCKUS Support Web site at <https://support.ruckuswireless.com/contact-us>.

# What's New in This Document

The following are the new events in 5.2.1 release.

Revision Number	Summary of Changes
A	<ul style="list-style-type: none"> <li>• Alarm code 823 - Node IP Address Changed</li> <li>• Alarm code 890 - Certificate is about to expire</li> <li>• Alarm code 891 - Certificate is already expired</li> <li>• Alarm code 4503 - Cloud Analytics service has been enabled</li> <li>• Alarm code 4504 - Cloud Analytics service has been disabled</li> <li>• Alarm code 4504 - Cloud Analytics disconnected</li> <li>• Event code 353 - AP Ethernet Phy Error Count</li> <li>• Event code 354 - AP Ethernet PHY Down Shift</li> <li>• Event code 890 - Certificate is about to expire</li> <li>• Event code 891 - Certificate is already expired</li> <li>• Event code 892 - Result of renew certificate</li> <li>• Event code 2901 - active cluster unable to connect to other active clusters for cluster redundancy.</li> <li>• Event code 2901 - Data Plane IP miPs Status</li> <li>• Event code 2902 - Data Plane IP miThemp BB</li> <li>• Event code 2904 - Data Plane IP miThemp IOH</li> <li>• Event code 2905 - Data Plane IP miThemp MemP</li> <li>• Event code 2913 - Data Plane IP miPs Status</li> <li>• Event code 2926 - Data Plane IpmiRE Voltage</li> <li>• Event code 2929 - Data Plane IP mi RE Voltage</li> <li>• Event code 2930 - Data Plane IP miRE Themp MemP</li> <li>• Event code 2938 - Data Plane IP miREPs Status</li> <li>• Event code 2961 - Data Plane SSDHealth Degrade</li> <li>• Event code 4505 - Cloud Analytics Disconnected</li> <li>• Event code 99100 - Failure of Key Generation</li> <li>• Event code 99101 - Failure of IPsec</li> <li>• Event code 99102 - Failure of Certificate</li> <li>• Event code 99103 - IPsec Key is Up</li> <li>• Event code 99104 - IPsec Key is Down</li> <li>• Event code 22071 - Switch Delete</li> <li>• Event code 22081 - Switch Disconnected from the Controller</li> <li>• Event code 22082 - Switch is Connected to the Controller</li> <li>• Event code 22091 - Switch Discovered by the Controller</li> </ul>

## Terminology

The following table lists the terms used in this guide.

**TABLE 2** Terms used

Term	Description
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting

**TABLE 2** Terms used (continued)

Term	Description
AD	Active Directory
AMBR	Aggregate Maximum Bit Rate
AP	Access Point
APN	Access Point Name
ASP	Application Service Provider
ASPDN	ASP Down
ASPDN ACK	ASP Down Acknowledgment
ASR	Abort Session Request
AVP	RUCKUS Vendor specific attribute Pair
BMD	Billing Mediation Device is a network component in a telecommunications network that receives, processes, reformats and sends information to other formats between network elements.
BSSID	Basic Service Set Identifier
CCM	Common Configuration Module
CDF	Charging Data Function
CDR	Call Detail Record.  A formatted collection of information on chargeable events used for accounting and billing. For example, call set-up, call duration and amount of data transferred.
CEA	Capabilities Exchange Answer
CER	Capabilities Exchange Request
CGF	Charging Gateway Function
CHAP	Challenge Handshake Authentication Protocol
CIP	Channel Interface Processor
CLB	Client Load Balance
CNN	Configuration Change Notifier
CNR	Configuration Notification Receiver
CoA	Change of Authorization
Controller	Refers to either SZ300 or vSZ-H as the case may be.
CPE	Customer-Premises Equipment
CTF	Charging Trigger Function
DEA	Diameter-EAP-Answer
DER	Diameter-EAP-Request
DHCP	Dynamic Host Configuration Protocol
DM	Dynamic Multipoint
DNS	Domain Name System
DPR	Diameter Disconnect Peer Request
DRT	Data Record Transfer
EAP	Extensible Authentication Protocol
EBI	EPS Bearer ID
EMAP	Ethernet Mesh AP
EPC	Evolved Packet Core
EPS	Evolved Packet System
F-TEID	Fully Qualified Tunnel Endpoint Identifier

## About This Guide

### Terminology

**TABLE 2** Terms used (continued)

Term	Description
FTP	File Transfer Protocol
Ga	Reference point between a CDF and the CGF for CDR transfer
GGSN	Gateway GPRS Support Node
GPDU	GTP Packet Data Unit
GPB	Google Protocol Buffer
GPRS	General Packet Radio Service
GSN	GPRS Support Node
GSN APN	GPRS serving node, is an application module in the controller, which handles GTP messages.
GTP	GPRS Tunneling Protocol
GTP-C	GTP control plane
GTP-U	GTP user plane
GTP'	GPRS protocol, used for CDR transport. It is derived from GTP with enhancements to improve transport reliability necessary for CDRs
GTPP	GPRS Tunneling Protocol Prime
GTPv1-U	GTP version 1, user plane
GTPv2-C	GTP version 2, control plane
HIP	Host Identity Protocol
HLR	Home Location Register
ICMP	Internet Control Message Protocol
IE	Information Element
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IPSP	IP Signalling Protocol
LBS	Location Based Service
LCS	Location Services
LDAP	Lightweight Directory Access Protocol
LMA	Local Mobility Anchor
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MOR	Maximum Outstanding Requests
MS-ISDN	Mobile Subscriber Integrated Services Digital Network Number
MTU	Maximum Transmission Unit
MWSG	Metro Wireless Security Gateway
NAS	Network Access Server
NTP	Network Time Protocol)
OUI	Organization Unique ID
P-GW	Packet Data Network Gateway
PAA	PDN Address Allocation
PCN	Packet switched Core network Node (SGSN, GGSN, S-GW, P-GW)
PCO	Protocol Configuration Options

**TABLE 2** Terms used (continued)

Term	Description
PDN	Packet Data Network
PDP	Packet Data Protocol
PGW	PDN Gateway
produce.short.name	Refers to either SZ300 or vSZ-H
R-WSG/WSG	RUCKUS Security Gateway
RAC	Radio Access Controller
RAP	Root Access Point
RAR	Re-Auth Request
RSSI	Received Signal Strength Indicator
S-CDR	SGSN Call Detail Record
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
SG	Signalling Gateway
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SSID	Service Set Identifier (SSID)
STR	STR (Session Termination-Request)
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TEID	Tunnel End Point Identifier
UDP	User Datagram Protocol
UE	User Equipment
UI	Web User Interface
USB	Universal Serial Bus
WDS	Wireless Distribution System





# Alarm and Event Management

---

- [Overview](#)..... 33
- [Alarm and Event Management](#)..... 33

## Overview

This guide lists and describes the various types of alarm and event that the controller generates. For each alarm and event, this guide provides the code, type, attributes, and description.

### NOTE

Refer to [About This Guide](#) on page 27 for the conventions used in this guide.

## Alarm and Event Management

This subsystem contains set of functions that help users to detect, isolate, and eventually correct malfunctions in the managed network. This section covers:

- [Event Categories](#) on page 33
- [Event Attributes](#) on page 34
- [Generation of Alarm and Event](#) on page 34

## Event Categories

Events are used for many different purposes, mainly for notifying users of certain conditions in the system components as well as the managed network. They can be classified into the following categories:

- **Alarms:** These are unexpected events indicating a condition that typically requires management attention.
- **Configuration Change Events:** Configuration change events are events that inform of a configuration change effect on the device.
- **Threshold Crossing Alerts:** These are events that inform of a performance-related state variable that has exceeded a certain value. These events point to conditions that might require management attention to prevent network and service degradation.
- **Logging Events:** These are events that occur regularly and are expected to occur during the operation of a network, that indicate what is currently going on in the network. Some examples of these events include:
  - Activity on the network and service
  - Operator activity
  - System activity
  - Informational events – Any other kind of event.
  - Debug and Informational events - All the debug and informational events pertaining to TTG modules like RADIUS proxy, HIP, CIP and AUT are not displayed on the Web Interface. This is because it reduces the performance of the system since its large in numbers. Enabling display of these events on the Web Interface is possible through CLI but it is not recommended.

## Event Attributes

An event always includes the following attributes:

- Event Source: The identifier of the source component that generates the event
- Timestamp: The time when the event occurred
- Event Severity: Severity is classified as critical, major, minor, warning, informational or debug
- Event Type: The type of event that has occurred
- Event Information: Contains detail attribute fields in a key-value pair, where a list of field names is provided

## Generation of Alarm and Event

The following are the steps of how alarm and event are generated.

1. Alarm
  - a. An alarm is a persistent indication of a fault that clears only when the triggering condition had been resolved.
  - b. An alarm can be filtered in the controller web interface based on:
    - Alarm Category - Alarm classifications
    - Alarm Source: Source of the alarm
    - Alarm Status: Could either be outstanding or cleared
    - Acknowledge Time: The time when the alarm is acknowledged
    - Date and Time - Date and time when the alarm is acknowledged
    - Severity: Severity is classified as critical, major or minor
    - Status - Could either be cleared or outstanding
    - Type - Alarm type
  - c. To view the below alarm information in the controller web interface navigate to **Events & Alarms > Alarms**
    - Date and Time
    - Code
    - Alarm Type
    - Severity
    - Status
    - Acknowledged on
    - Cleared By
    - Cleared On
    - Comments
    - Activity
    - Actions
  - d. On an alarm generation, the controller web interface provides the following information as seen in the figure below.
    - Alarm console, which displays the cleared and outstanding alarms visible to the user who is currently logged on.
    - Alarm summary, which lists various information such as outstanding alarm counts, unacknowledged alarm counts, etc.
    - You may clear an alarm or a set of alarms to let other administrators know that you have already resolved the issue. When you select a group of alarms, the **Clear Alarm** button is activated. Click this button. A text box appears where you can enter comments or notes about the resolved issue. Click Apply when done. To view the cleared alarms, select the cleared option.

- You may acknowledge an alarm or a set of alarms to let other administrators know that you have acknowledged it. When you select an alarm or group of alarms, the **Acknowledge Alarm** button is activated. Click this button. A text box appears where you need to confirm the acknowledgment. Click **Yes** when done. The **Acknowledged on** column in the Alarms table gets updated.
- Filtering features based on the alarm attributes.  
The **Filter** button is deactivated by default. Click this button if you want to turn on the filter. Click the gear icon to set the filter. A text box appears where you can enter the severity, status and start and end date and time. Click **OK** when done.
- You may also export the data as a CSV file.

FIGURE 1 Alarms

Date and Time	Code	Alarm Type	Severity	Status	Activity	Acknowledged On	Cleared By	Cleared On
2017/01/24 16:...	302	AP rebooted by system	Major	Outstanding	AP [INDIA-AP-H510@1C:B9:C4:23:03...	N/A	N/A	N/A
2017/01/26 15:...	302	AP rebooted by system	Major	Outstanding	AP [R710-215@D4:68:4D:1A:6B:20] r...	N/A	N/A	N/A
2017/01/25 16:...	303	AP disconnected	Major	Outstanding	AP [INDIA-AP-H510@1C:B9:C4:23:03...	N/A	N/A	N/A
2017/01/25 16:...	303	AP disconnected	Major	Outstanding	AP [C110@F0:3E:90:3F:7F:40] disco...	N/A	N/A	N/A
2017/01/24 21:...	803	Node out of service	Critical	Outstanding	Node [set-2] in cluster [set-1] is out ...	N/A	N/A	N/A
2017/01/24 16:...	1261	Data plane fails to connects to the other ...	Warning	Outstanding	Data plane[N/A@74:FE:48:08:AF:BE...	N/A	N/A	N/A
2017/01/24 16:...	1261	Data plane fails to connects to the other ...	Warning	Outstanding	Data plane[N/A@74:FE:48:08:AF:BE...	N/A	N/A	N/A
2017/01/26 15:...	1601	Authentication server not reachable	Major	Outstanding	Authentication Server [172.19.13.10...	N/A	N/A	N/A
2017/01/25 13:...	1601	Authentication server not reachable	Major	Outstanding	Authentication Server [172.19.13.20...	N/A	N/A	N/A

9 total records - 1 -

2. Event - On an event generation the following:
  - a. The controller collects, receives, and maintains the raw events from the managed entities (control plane, data plane, access points, etc.). These raw events are kept in the database, and are automatically purged.
  - b. The controller allows users to enable/disable certain event types from the managed entities.

**Events** - The web interface provides event log window as seen in the figure below, for users to visualize and analyze the events. To view the event information in the controller web interface navigate to **Events & Alarms > Events**.

- Date and Time
- Code
- Type
- Severity
- Activity

**Event Management** lists the disabled events that are filtered at the source whenever possible to minimize resources for processing events. The SMTP server is disabled by default. You must enable and configure the SMTP server so notification emails can be delivered successfully.

**Threshold Events** are triggered at the source whenever possible.

Users are able to perform various operations on the events, such as filtration, aggregation and counting. The **Filter** button is deactivated by default. Click this button if you want to turn on the filter. Click on the gear icon to set the filter. A text box appears where you can enter the severity, status and start and end date and time. Click **OK** when done.

The controller gives you the option of exporting the data as a CSV file.

**FIGURE 2** Events

The screenshot shows a web interface for managing events. At the top, there are tabs for 'Events', 'Event Management', and 'Event Threshold'. Below the tabs, there are controls for filtering (a dropdown set to 'Filter Off'), a search box, and a 'Refresh' button. The main content is a table with the following columns: 'Date and Time', 'Code', 'Type', 'Severity', and 'Activity'. The table contains ten rows of event data.

Date and Time	Code	Type	Severity	Activity
2017/01/30 17:21:30	608	AP created a tunnel	Informational	AP [R710-215@D4:68:4D:1A:68:20] created a tunnel to data plane [[10.148.124.62]:23233].
2017/01/30 17:21:16	608	AP created a tunnel	Informational	AP [AP@D4:68:4D:02:39:A0] created a tunnel to data plane [[10.148.124.60]:23233].
2017/01/30 17:21:11	601	Data plane accepted a tunn...	Informational	Data plane [74:FE:48:08:AF:A1] accepted the tunnel request from AP [AP@D4:68:4D:02:39:A0].
2017/01/30 17:21:05	750	Syslog server reachable	Informational	Syslog server [172.19.13.102] is reachable on SmartZone.
2017/01/30 17:21:05	750	Syslog server reachable	Informational	Syslog server [172.19.13.101] is reachable on SmartZone.
2017/01/30 17:21:00	314	AP heartbeat lost	Informational	AP [T710@F0:3E:90:1B:A7:90] heartbeat lost.
2017/01/30 17:21:00	314	AP heartbeat lost	Informational	AP [T300@D4:68:4D:06:A8:00] heartbeat lost.
2017/01/30 17:21:00	314	AP heartbeat lost	Informational	AP [AP@D4:68:4D:02:39:A0] heartbeat lost.
2017/01/30 17:21:00	314	AP heartbeat lost	Informational	AP [R710-215@D4:68:4D:1A:68:20] heartbeat lost.
2017/01/30 17:20:30	314	AP heartbeat lost	Informational	AP [T710@F0:3E:90:1B:A7:90] heartbeat lost.

**NOTE**

Refer to [Alarm Types](#) on page 37 and [Events Types](#) on page 133 for the list of alarm and event that the controller generates.

**NOTE**

Refer to *SNMP MIB Reference Guide* for the list of SNMP alarm traps that the controller generates.

**NOTE**

Refer to Administrator Guide for viewing of Alarms and Events.

# Alarm Types

---

• Introduction.....	37
• Accounting Alarms.....	37
• AP Authentication Alarms.....	41
• AP Communication Alarms.....	44
• AP LBS Alarms.....	48
• AP State Change Alarms.....	50
• Authentication Alarms.....	54
• Control and Data Plane Interface Alarms.....	58
• Cloud Alarms.....	59
• Cluster Alarms.....	60
• Configuration Alarms.....	74
• Data Plane Alarms.....	76
• Data Streaming Alarms.....	82
• Gn/S2a Interface Alarms.....	82
• GR Interface Alarms.....	88
• IPMI Alarms.....	91
• Licensing Alarms.....	99
• PMIPv6 Alarms.....	102
• SCI Alarms.....	103
• Session Alarms.....	105
• System Alarms.....	105
• Switch.....	118
• Threshold Alarms.....	125
• Tunnel Alarms - Access Point.....	130

## Introduction

This chapter provides information on the various types of alarms that the controller generates. Alarms are a subset of the events defined. Categories are inherited from the event.

## Accounting Alarms

Following are the alarms related to accounting.

- [Accounting server not reachable](#) on page 38
- [Accounting fallback to primary](#) on page 38
- [Accounting fallback to primary](#) on page 38
- [AP accounting message mandatory parameter missing](#) on page 39
- [AP accounting message decode failed](#) on page 40
- [AP account message drop while no accounting start message](#) on page 40
- [Unauthorized CoA/DM message dropped](#) on page 41

## Accounting server not reachable

**TABLE 3** Accounting server not reachable alarm

Alarm	Accounting server not reachable
Alarm Type	accSrvrNotReachable
Alarm Code	1602
Severity	Major
Aggregation Policy	An alarm is raised for every event from the event code 1602. A single event triggers a single alarm.
Attribute	"mynoid"=12, "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd", "realm"="wlan.3gppnetwork.org", "radProxyIp"="7.7.7.7", "accSrvrIp"="30.30.30.30", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the accounting server cannot be reached.
Recommended Actions	Manual intervention is required. Check the web interface for the connection to the AAA interface. Also, check if the RADIUS server can reach the AAA server interface.

## Accounting failed over to secondary

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 4** Accounting failed over to secondary alarm

Alarm	Accounting failed over to secondary
Alarm Type	accFailedOverToSecondary
Alarm Code	1653
Severity	Major
Aggregation Policy	An alarm is raised for every event from the event code 1653. A single event triggers a single alarm.
Attribute	"mynoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [7.7.7.7] on SCG[2.2.2.2]
Description	This alarm is triggered when the secondary accounting RADIUS server is available after the primary server becomes zombie or dead.
Recommended Actions	No action is required.

## Accounting fallback to primary

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 5** Accounting fallback to primary alarm

Alarm	Accounting fallback to primary
Alarm Type	accFallbackToPrimary

**TABLE 5** Accounting fallback to primary alarm (continued)

Alarm	Accounting fallback to primary
Alarm Code	1654
Severity	Major
Aggregation Policy	An alarm is raised for every event from the event code 1654. A single event triggers a single alarm.
Attribute	"mvnold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the automatic fallback is enabled. The accounting failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.
Recommended Actions	No action is required.

## AP accounting message mandatory parameter missing

### NOTE

This alarm is not applicable for vSZ-H.

**TABLE 6** AP accounting message mandatory parameter missing alarm

Alarm	AP accounting message mandatory parameter missing
Alarm Type	apAcctMsgMandatoryPrmMissing
Alarm Code	1901
Severity	Critical
Aggregation Policy	From the event code 1901 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvnold"="12","wlanId"=1, "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut",  "realm"="wlan.3gppnetwork.org", "SCGMgmtIp"="2.2.2.2",  "ueMacAddr"="aa:bb:cc:gg:hh:ii","ueImsi"="12345",  "ueMsisdn"="98787"
Displayed on the web interface	[{srcProcess}] Mandatory attribute missing in Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}], with username [{ueImsi}@{realm}]
Description	This alarm is triggered when the controller fails to find the mandatory parameter in the RADIUS accounting message received from the AP. This mandatory parameter is required for generating the WAN-CDR.
Recommended Action	Download the RADIUS log file from the web interface to check the error cause.

## AP accounting message decode failed

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 7** AP accounting message decode failed alarm

Alarm	AP accounting message decode failed
Alarm Type	apAcctMsgDecodeFailed
Alarm Code	1904
Severity	Critical
Aggregation Policy	From the event code 1904 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvnold"="12","wlanId"=1,"zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="wlan.3gppnetwork.org", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	{{srcProcess}} Malformed Accounting Packet received from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}}, with username {{userName}}
Description	This alarm is triggered when an AP accounting message decode fails due to a malformed packet.
Recommended Action	Download the RADIUS log file from the web interface to check the error cause.

## AP account message drop while no accounting start message

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 8** AP account message drop while no accounting start message alarm

Alarm	AP account message drop while no accounting start message
Alarm Type	apAcctMsgDropNoAcctStartMsg
Alarm Code	1910
Severity	Critical
Aggregation Policy	From the event code 1910 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvnold"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="wlan.3gppnetwork.org",
Displayed on the web interface	{{srcProcess}} Dropped Accounting Packet received from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}}, with username {{userName}}. Accounting session timer expired, stop or interim message not received, as Account Start not received from NAS/AP
Description	This alarm is raised when accounting messages from the AP is dropped. The attributes <b>Acct Interim/Stop</b> message as account start is not received from the AP.
Recommended Action	Check the accounting retransmit timer and retransmit count in the Access Point (AP) configuration. Also check if the interface from the AP to the controller is congested.



## Unauthorized CoA/DM message dropped

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 9** Unauthorized CoA/DM message dropped alarm

Alarm	Unauthorized CoA/DM message dropped
Alarm Type	unauthorizedCoaDmMessageDropped
Alarm Code	1911
Severity	Critical
Aggregation Policy	From the event code 1911 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"="12" "wlanId"="1" "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "radSrvrIp"="7.7.7.7" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} Dropped CoA/DM Packet received from AAA {{radSrvrIp}} on {{produce.short.name}} {{SCGMgmtIp}}, Received message from unauthorized AAA
Description	This alarm is triggered when the controller receives a Change of Authorization (CoA) or Dynamic Multipoint (DM) message from an unauthorized AAA server.
Recommended Action	Check the RADIUS configuration server settings in the RADIUS service profile. Check if the AAA server is authorized to send the change of authorization (CoA) or dynamic multipoint (DM) messages. If it is authorized, include for RADIUS server to send CoA/DM message in RADIUS service.

## AP Authentication Alarms

Following are the alarms related to AP authentication.

- [RADIUS server unreachable](#) on page 41
- [LDAP server unreachable](#) on page 42
- [AD server unreachable](#) on page 42
- [WeChat ESP authentication server unreachable](#) on page 43
- [WeChat ESP authentication server unresolvable](#) on page 43
- [WeChat ESP DNAT server unreachable](#) on page 43
- [WeChat ESP DNAT server unresolvable](#) on page 44

## RADIUS server unreachable

**TABLE 10** RADIUS server unreachable alarm

Alarm	RADIUS server unreachable
Alarm Type	radiusServerUnreachable
Alarm Code	2102
Severity	Major
Aggregation Policy	From the event code 2102 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ip"="17.0.0.12", "fwVersion"="3.2.0.0.x", "model"="ZF798 2", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""

## Alarm Types

### AP Authentication Alarms

**TABLE 10** RADIUS server unreachable alarm (continued)

Alarm	RADIUS server unreachable
Auto Clearance	The alarm is auto cleared with the event code 2101.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach radius server [{ip}].
Description	This alarm is triggered when AP is unable to reach RADIUS server.
Recommended Actions	Check the network connectivity between AP and RADIUS server.

## LDAP server unreachable

**TABLE 11** LDAP server unreachable alarm

Alarm	LDAP server unreachable
Alarm Type	ldapServerUnreachable
Alarm Code	2122
Severity	Major
Aggregation Policy	From the event code 2122 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF798 2","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2121.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach LDAP server [{ip}].
Description	This alarm is triggered when AP is unable to reach LDAP server.
Recommended Actions	Check the network connectivity between AP and LDAP server.

## AD server unreachable

**TABLE 12** AD server unreachable alarm

Alarm	AD server unreachable
Alarm Type	adServerUnreachable
Alarm Code	2142
Severity	Major
Aggregation Policy	From the event code 2142 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF798 2","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2141.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].
Description	This alarm is triggered when AP is unable to reach AD server.
Recommended Actions	Check the network connectivity between AP and AD server.

## WeChat ESP authentication server unreachable

**TABLE 13** WeChat ESP authentication server unreachable alarm

Alarm	WeChat ESP authentication server unreachable
Alarm Type	espAuthServerUnreachable
Alarm Code	2152
Severity	Major
Aggregation Policy	From the event code 2152 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2151
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach WeChat ESP authentication server [{ip}]
Description	This alarm is triggered when AP is unable to reach WeChat ESP authentication server.
Recommended Actions	.Check the network connectivity between controller web interface and WeChat ESP authentication server.

## WeChat ESP authentication server unresolvable

**TABLE 14** WeChat ESP authentication server unresolvable alarm

Alarm	WeChat ESP authentication server unresolvable
Alarm Type	espAuthServerUnResolvable
Alarm Code	2154
Severity	Major
Aggregation Policy	From the event code 2154 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","dn"="www.test.com","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2153.
Displayed on the web interface	AP [{apName&&apMac}] is unable to resolve WeChat ESP authentication server domain name [{dn}] to IP
Description	This alarm is triggered when AP is unable to resolve WeChat ESP authentication server domain name.
Recommended Actions	Check the DNS server configuration settings in the controller web interface.

## WeChat ESP DNAT server unreachable

**TABLE 15** WeChat ESP DNAT server unreachable alarm

Alarm	WeChat ESP DNAT server unreachable
Alarm Type	espDNATServerUnreachable
Alarm Code	2162
Severity	Major

## Alarm Types

### AP Communication Alarms

**TABLE 15** WeChat ESP DNAT server unreachable alarm (continued)

Alarm	WeChat ESP DNAT server unreachable
Aggregation Policy	From the event code 2162 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2161.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach WeChat ESP DNAT server [{ip}].
Description	This alarm is triggered when the AP is unable to reach WeChat ESP DNAT server.
Recommended Actions	Check the network connectivity between controller web interface and WeChat ESP DNAT server.

## WeChat ESP DNAT server unresolvable

**TABLE 16** WeChat ESP DNAT server unresolvable alarm

Alarm	WeChat ESP DNAT server unresolvable
Alarm Type	espDNATServerUnresolvable
Alarm Code	2164
Severity	Major
Aggregation Policy	From the event code 2164 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","dn"="www.test.com","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2163.
Displayed on the web interface	AP [{apName&&apMac}] is unable to resolve WeChat ESP DNAT server domain name [{dn}] to IP
Description	This alarm is triggered when the AP is unable to resolve WeChat ESP DNAT server domain name.
Recommended Actions	Check the DNS server configuration settings in the controller web interface.

## AP Communication Alarms

Following are the alarms related to access point communications.

- [AP rejected](#) on page 45
- [AP configuration update failed](#) on page 45
- [AP swap model mismatched](#) on page 45
- [AP pre-provision model mismatched](#) on page 46
- [AP firmware update failed](#) on page 46
- [AP WLAN oversubscribed](#) on page 47
- [AP join zone failed](#) on page 47
- [AP image signing failed](#) on page 47

## AP rejected

**TABLE 17** AP rejected alarm

Alarm	AP rejected
Alarm Type	apStatusRejected
Alarm Code	101
Severity	Minor
Aggregation Policy	From the event code 105 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 103.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx", "reason"="xxx"
Displayed on the web interface	{produce.short.name} [{wsgIP}] rejected AP [{apName&&apMac}] because of [{reason}]
Description	This alarm is triggered when the AP is rejected.
Recommended Actions	Check if the number of licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses.

## AP configuration update failed

**TABLE 18** AP configuration update failed alarm

Alarm	AP configuration update failed
Alarm Type	apConfUpdateFailed
Alarm Code	102
Severity	Major
fAggregation Policy	From the event code 111 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 110.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "configID"="23456781234"
Displayed on the web interface	AP [{apName&&apMac}] failed to update to configuration [{configID}]
Description	This alarm is triggered when the controller is unable to update the AP configuration details.
Recommended Actions	Retrieve the AP support text. Reboot the AP and trigger another configuration change for upgrading the AP. If it fails revert to the previous zone firmware.

## AP swap model mismatched

**TABLE 19** AP swap model mismatched alarm

Alarm	AP swap model mismatched
Alarm Type	apModelDiffWithSwapOutAP
Alarm Code	104
Severity	Major
Aggregation Policy	From the event code 113 an alarm is raised for every event. A single event triggers a single alarm.

## Alarm Types

### AP Communication Alarms

**TABLE 19** AP swap model mismatched alarm (continued)

Alarm	AP swap model mismatched
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx " "configModel"="xxx.xxx.xxx.xxx", "model"="xxx.xxx.xxx.xxx
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from swap configuration model [{configModel}]
Description	This alarm is triggered when the AP model differs from the swapped configuration model.
Recommended Actions	If the model is incorrect delete and rejoin the AP.

## AP pre-provision model mismatched

**TABLE 20** AP pre-provision model mismatched alarm

Alarm	AP pre-provision model mismatched
Alarm Type	apModelDiffWithPreProvConfig
Alarm Code	105
Severity	Major
Aggregation Policy	From the event code 112 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx", "configModel"="xxx.xxx.xxx.xxx". "model"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from per-provision configuration model [{configModel}]
Description	This alarm is triggered when the AP model differs from the pre-provision configuration model.
Recommended Actions	If the model is incorrect delete the AP for the AP to rejoin to get the proper AP configuration.

## AP firmware update failed

**TABLE 21** AP firmware update failed alarm

Alarm	AP firmware update failed
Alarm Type	apFirmwareUpdateFailed
Alarm Code	107
Severity	Major
Aggregation Policy	From the event code 107 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 106.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}] [{reason}]
Description	This alarm is triggered when the AP fails to update the firmware details.
Recommended Actions	Retrieve the AP support text. Reboot the AP and trigger another configuration change for upgrading the AP. If it fails revert to the previous zone firmware.

## AP WLAN oversubscribed

**TABLE 22** AP WLAN oversubscribed alarm

Alarm	AP WLAN oversubscribed
Alarm Type	apWlanOversubscribed
Alarm Code	1081
Severity	Major
Aggregation Policy	From the event code 114 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] does not have enough capacity to deploy all wlangs. Only maximum wlan number of the AP can be deployed
Description	This alarm is triggered when the AP exceeds the maximum capacity for deploying all WLANs.
Recommended Actions	Any of the following are the recommended actions. <ul style="list-style-type: none"> <li>• Create a new WLAN group with WLANs. Ensure that it is not more than the AP's WLAN capacity. Apply the new WLAN group to either the AP or the AP's AP Group.</li> <li>• Find the WLAN group used by the AP and reduce the number of WLAN.</li> </ul>

## AP join zone failed

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 23** AP join zone failed alarm

Alarm	AP join zone failed
Alarm Type	apJoinZoneFailed
Alarm Code	115
Severity	Major
Aggregation Policy	From the event code 115 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "zoneUUID"="xx:xx:xx:xx:xx:xx", "targetZoneUUID"="xx:xx:xx:xx:xx:xx", "reason"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] failed to join to zone [{targetZoneName}]. Reason: [{reason}]
Description	This alarm is triggered when the AP fails to join the specified zone
Recommended Actions	Check if the number of RXGW (AP direct tunnel license) licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses.

## AP image signing failed

**NOTE**

APs earlier than release 3.4 cannot be aligned to join SmartZone release 3.6.x due to mismatch in image format. Alarm code 187 will be raised with AP MAC address.

**NOTE**

USI: Un Signed Image

ISI: Intermediate Signed Image

FSI: Fully Signed Image

**TABLE 24** AP image signing failed alarm

Alarm	AP Image signing failed
Alarm Type	apSigningInformation
Alarm Code	187
Severity	Informational
Aggregation Policy	From the event code 187 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP Image Signing: The AP[apMac] with firmware version [fwVersion] is USI. USI to FSI upgrade is not allowed due to difference in Image formats.
Description	This alarm is triggered when the upgrade fails due to AP image mismatch.
Recommended Actions	<p>This issue of not able to upgrade from releases prior to or from 3.2.x to R3.6+ occurs as per the following category.</p> <ul style="list-style-type: none"> <li>• <b>Category 1:</b> AP firmware images for releases prior to 3.4.x is in the format USI (Un Signed Image)</li> <li>• <b>Category 2:</b> AP firmware images for releases 3.4.x and 3.5.x is in the format ISI (Intermediate Signed Image)</li> <li>• <b>Category 3:</b> AP firmware images for releases 3.6 and above is in the format FSI (Fully Signed Image)</li> </ul> <p>When upgrading from releases prior to 3.4 to 3.6.x and above, the AP image in category1 (USI) should be first upgraded to category 2 (ISI) and only then upgraded to category 3 (FSA). For example, move the AP image first to 3.4 or 3.5 zone and then to 3.6.x zone. If you attempt to do a direct upgrade (from USI to FSI) alarm 187 is triggered.</p> <p>If you are unable to upgrade the AP image using the controller web user interface, you can alternatively upgrade through TFTP or FTP using CLI mode as per the below steps.</p> <ul style="list-style-type: none"> <li>• <b>Step 1:</b> Configure FTP or TFTP server in the network with any image (even FSI for 3.6.x is allowed)</li> <li>• <b>Step 2:</b> Login to AP CLI and configure TFTP or FTP server IP address and image file name by using the command <code>fw set</code> and its related sub options.</li> <li>• <b>Step 3:</b> Execute the command <code>fw update</code></li> <li>• <b>Step 4:</b> On completion of step 3 you can now upgrade the API image to <b>ISI &gt; FSI</b> using the controller web user interface.</li> </ul>

## AP LBS Alarms

Following are the alarms related to AP Location Based Service (LBS).

- [No LS responses](#) on page 49
- [LS authentication failure](#) on page 49
- [AP failed to connect to LS](#) on page 49



## No LS responses

**TABLE 25** No LS responses alarm

Alarm	No LS responses
Alarm Type	apLBSNoResponses
Alarm Code	701
Severity	Major
Aggregation Policy	From the event code 701 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""
Displayed on the SmartZone web interface	AP [{apName}&&apMac] no response from LS: url=[{url}], port=[{port}]
Description	This alarm is triggered when the AP does not get a response when trying to connect to the location based service.
Recommended Actions	This alarm is triggered when the location server fails to respond to the AP request due to an error or the server is in a maintenance mode. Report this to the location server owner.

## LS authentication failure

**TABLE 26** LS authentication failure alarm

Alarm	LS authentication failure
Alarm Type	apLBSAuthFailed
Alarm Code	702
Severity	Major
Aggregation Policy	From the event code 702 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""
Displayed on the SmartZone web interface	AP [{apName}&&apMac] LBS authentication failed: url=[{url}], port=[{port}]
Description	This alarm is triggered due to the authentication failure on connecting to the location based service.
Recommended Actions	The password needs to be corrected in the LBS service page.

## AP failed to connect to LS

**TABLE 27** AP failed to connect to LS alarm

Alarm	AP failed to connect to LS
Alarm Type	apLBSConnectFailed
Alarm Code	704
Severity	Major
Aggregation Policy	From the event code 704 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 703.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""

## Alarm Types

### AP State Change Alarms

**TABLE 27** AP failed to connect to LS alarm (continued)

Alarm	AP failed to connect to LS
Displayed on the SmartZone web interface	AP [{apName}&{apMac}] connection failed to LS: url={url}, port={port}
Description	This alarm is triggered when the AP fails to connect to the location based service.
Recommended Actions	This alarm is triggered either when the location server is unreachable or the network connection is unstable or the Domain Named System (DNS) configuration is incorrect. It is recommended to check all the three possible error codes - 701, 702 and 704.

## AP State Change Alarms

Following are the alarms related to access point state changes:

- [AP rebooted by system](#) on page 50
- [AP disconnected](#) on page 51
- [AP deleted](#) on page 51
- [AP cable modem interface down](#) on page 51
- [AP DHCP service failure](#) on page 52
- [AP NAT failure](#) on page 52
- [AP DHCP/NAT DWPD Ethernet port configuration override](#) on page 52
- [SZ DHCP/NAT DWPD Ethernet port configuration override](#) on page 53
- [SIM removal](#) on page 53
- [AP System Anomaly](#) on page 54

## AP rebooted by system

**TABLE 28** AP rebooted by system alarm

Alarm	AP rebooted by system
Alarm Type	apRebootBySystem
Alarm Code	302
Severity	Major
Aggregation Policy	From the event code 302 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxx"
Displayed on the web interface	AP [{apName}&{apMac}] rebooted by the system because of [{reason}]
Description	This alarm is triggered when system reboots the AP.
Recommended Actions	Check the reasons for the reboot. If the reason is unknown, retrieve the AP support text and send it to RUCKUS support.

## AP disconnected

**TABLE 29** AP disconnected alarm

Alarm	AP disconnected
Alarm Type	apConnectionLost
Alarm Code	303
Severity	Major
Aggregation Policy	From the event code 303 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 312
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] disconnected
Description	This alarm is triggered when the AP disconnects from the controller.
Recommended Actions	Check the network and the communicator process on the controller. Try rebooting the AP locally.

## AP deleted

**TABLE 30** AP deleted alarm

Alarm	AP deleted
Alarm Type	apDeleted
Alarm Code	306
Severity	Major
Aggregation Policy	From the event code 313 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] deleted
Description	This alarm is triggered when the AP is deleted.
Recommended Actions	This is a user action and to confirm check the user audit.

## AP cable modem interface down

**TABLE 31** AP cable modem interface down alarm

Alarm	AP cable modem interface down
Alarm Type	cableModemDown
Alarm Code	308
Severity	Major
Aggregation Policy	From the event code 316 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 325.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] cable modem interface is down

## Alarm Types

### AP State Change Alarms

**TABLE 31** AP cable modem interface down alarm (continued)

Alarm	AP cable modem interface down
Description	This alarm is triggered when the AP cable modem interface is down.
Recommended Actions	Check cable modem. Try rebooting the cable modem.

## AP DHCP service failure

**TABLE 32** AP DHCP service failure alarm

Alarm	Both primary and secondary DHCP server APs are down
Alarm Type	apDHCPServiceFailure
Alarm Code	341
Severity	Major
Aggregation Policy	From the event code 341 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"primaryServerMac"="xx:xx:xx:xx:xx:xx", "secondaryServerMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP DHCP service failure. Both primary DHCP AP [{primaryServerMac}] and secondary DHCP server AP [{secondaryServerMac}] are down.
Description	This alarm is triggered when the primary and secondary DHCP server APs fail.
Recommended Actions	Deploy DHCP service on another AP.

## AP NAT failure

**TABLE 33** AP NAT failure alarm

Alarm	AP cable modem interface down NAT failure detected by controller due to three (3) consecutive NAT gateway APs are down
Alarm Type	apNATFailureDetectedbySZ
Alarm Code	346
Severity	Major
Aggregation Policy	From the event code 346 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac1"="xx:xx:xx:xx:xx:xx", "apMac2"="xx:xx:xx:xx:xx:xx", "apMac3"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	NAT failure detected by SZ since three (3) consecutive NAT gateway IPs are down AP1=[{apMac1}] AP2=[{apMac2}] AP3=[{apMac3}] (All consecutive NAT APs are down in case of less than 3 NAT Gateway APs configured). The NAT traffic for some of the clients may get affected for the respective VLANs.
Description	This alarm is triggered when the controller detects three (3) consecutive failures of NAT server APs.

## AP DHCP/NAT DWPD Ethernet port configuration override

**TABLE 34** AP DHCP/NAT DWPD Ethernet port configuration override alarm

Alarm	AP DHCP/NAT DWPD Ethernet port configuration override
Alarm Type	clusterRedundancyApRehomeIncomplete

**TABLE 34** AP DHCP/NAT DWPDP Ethernet port configuration override alarm (continued)

Alarm	AP DHCP/NAT DWPDP Ethernet port configuration override
Alarm Code	1026
Severity	Major
Aggregation Policy	From the event code 1026 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac" = "xx:xx:xx:xx:xx:xx", "ethPort" = "xxx", "forwardingType" = "xxx"
Displayed on the web interface	AP[apMac] does not have any available ethernet port for LAN. Overriding [ethPort] configured as [forwardingType], to LAN/Local Subnet by DHCP/NAT DWPDP configuration.
Description	This alarm is triggered when the AP does not have an available Ethernet port for LAN.

## SZ DHCP/NAT DWPDP Ethernet port configuration override

**TABLE 35** SZ DHCP/NAT DWPDP Ethernet port configuration override alarm

Alarm	SZ DHCP/NAT DWPDP Ethernet port configuration override
Alarm Type	sZCfgDhcpNatManualEthPortConfigOverride
Alarm Code	1027
Severity	Major
Aggregation Policy	From the event code 10276 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac" = "xx:xx:xx:xx:xx:xx", "ethPort" = "xxx", "forwardingType" = "xxx"
Displayed on the web interface	[ethPort] already configured as [forwardingType] for AP[apMac]. Overriding to LAN/Local Subnet by DHCP/NAT configuration.
Description	This alarm is triggered when the Ethernet port is already configured for the AP.

## SIM removal

**TABLE 36** SIM removal alarm

Alarm	SIM removal
Alarm Type	simRemoval
Alarm Code	9109
Severity	Major
Aggregation Policy	From the event code 7002, an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 7002.
Attribute	apMac = "xx:xx:xx:xx:xx:xx", currSim = "SIM 0"
Displayed on the web interface	AP [apName&&apMac] [currSim] removed
Description	This alarm is triggered when the SIM is removed.
Recommended Actions	No action is required.

## AP System Anomaly

**TABLE 37** AP System Anomaly alarm

Alarm	AP System Anomaly
Alarm Type	apWritableRO
Alarm Code	285
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "apName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] /writable partition is mounted as Read-Only
Description	This alarm is triggered when AP /writable partition is mounted as Read-Only

## Authentication Alarms

The following are the alarms related to authentication.

- [Authentication server not reachable](#) on page 54
- [Authentication failed over to secondary](#) on page 55
- [Authentication fallback to primary](#) on page 55
- [AD/LDAP connectivity failure](#) on page 55
- [Bind fails with AD/LDAP](#) on page 56
- [Bind success with LDAP, but unable to find clear text password for the user](#) on page 56
- [RADIUS fails to connect to AD NPS server](#) on page 57
- [RADIUS fails to authenticate with AD NPS server](#) on page 57
- [Fails to establish TLS tunnel with AD/LDAP](#) on page 58

## Authentication server not reachable

**TABLE 38** Authentication server not reachable alarm

Alarm	Authentication server not reachable
Alarm Type	authSvrNotReachable
Alarm Code	1601
Severity	Major
Aggregation Policy	From the event code 1601 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvnold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "authSvrIp"="20.20.20.20" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}].
Description	This alarm is triggered when the authentication fails since the primary or secondary servers are not reachable.
Recommended Actions	Manual intervention is required. Check the web interface for the interface from the controller to AAA server. Also check if the AAA server can be reached from the RADIUS server. Ensure that the AAA server is UP.

## Authentication failed over to secondary

**TABLE 39** Authentication failed over to secondary alarm

Alarm	Authentication failed over to secondary
Alarm Type	authFailedOverToSecondary
Alarm Code	1651
Severity	Major
Aggregation Policy	From the event code 1651 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]a
Description	This alarm is triggered when the secondary RADIUS server is available after the primary server becomes zombie or dead.
Recommended Actions	No operator action is required.

## Authentication fallback to primary

**TABLE 40** Authentication fallback to primary alarm

Alarm	Authentication fallback to primary
Alarm Type	authFallbackToPrimary
Alarm Code	1652
Severity	Major
Aggregation Policy	From the event code 1652 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when automatic fallback is enable. Consequently, the authentication failover to the secondary server occurs and the revival timer for the primary server expires, and the requests falls back to the primary server.
Recommended Actions	No action is required.

## AD/LDAP connectivity failure

**TABLE 41** AD/LDAP connectivity failure alarm

Alarm	AD/LDAP connectivity failure
Alarm Type	racADLDAPFail
Alarm Code	1752
Severity	Major
Aggregation Policy	From the event code 1752 an alarm is raised for every event. A single event triggers a single alarm.

## Alarm Types

### Authentication Alarms

**TABLE 41** AD/LDAP connectivity failure alarm (continued)

Alarm	AD/LDAP connectivity failure
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "SCGMgmtIp"="2.2.2.2"  "desc"="Connection to AD/LDAP fails"
Displayed on the web interface	[[srcProcess]] Connect to AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]]
Description	This alarm is triggered when RADIUS server fails to connect with AD/LDAP server.
Recommended Actions	<ul style="list-style-type: none"><li>• Check whether AD/LDAP server instance is running on the target machine</li><li>• Check whether the AD/LDAP server can be reached from the controller</li><li>• Verify if AD/LDAP server instances are listening on ports 3268 and 389</li><li>• Verify if the requests are reaching AD/LDAP servers by any packet capture tool (tcpdump, wireshark)</li></ul>

## Bind fails with AD/LDAP

**TABLE 42** Bind fails with AD/LDAP alarm

Alarm	Bind fails with AD/LDAP
Alarm Type	racADLDAPBindFail
Alarm Code	1753
Severity	Major
Aggregation Policy	From the event code 1753 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"= "1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Bind to AD/LDAP fails"
Displayed on the web interface	[[srcProcess]] Bind to AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]] for User[[userName]]
Description	This alarm is triggered when RADIUS server binding fails to AD/LDAP server.
Recommended Actions	<ul style="list-style-type: none"><li>• Verify the base and administrator domain names as configured in the controller web interface</li><li>• Verify the administrator user name and password as configured in the controller web interface</li><li>• Verify whether the configured administrator user name and password is authenticated by the AD/LDAP servers</li></ul>

## Bind success with LDAP, but unable to find clear text password for the user

**TABLE 43** Bind success with LDAP, but unable to find clear text password for the user alarm

Alarm	Bind success with LDAP, but unable to find clear text password for the user
Alarm Type	racLDAPFailToFindPassword
Alarm Code	1754
Severity	Major
Aggregation Policy	From the event code 1754 an alarm is raised for every event. A single event triggers a single alarm.



**TABLE 43** Bind success with LDAP, but unable to find clear text password for the user alarm (continued)

Alarm	Bind success with LDAP, but unable to find clear text password for the user
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Fail to find password"
Displayed on the web interface	{{srcProcess}} failed to find password from LDAP{{authSrvrIp}} for SCG{{SCGMgmtIp}} for User{{userName}}
Description	This alarm is triggered when binding is successful with LDAP server using root credentials but it is unable to retrieve the clear text password for the user.
Recommended Actions	Verify whether the given username and clear text password are configured in the LDAP server.

## RADIUS fails to connect to AD NPS server

**TABLE 44** RADIUS fails to connect to AD NPS server alarm

Alarm	RADIUS fails to connect to AD NPS server
Alarm Type	racADNPSFail
Alarm Code	1755
Severity	Major
Aggregation Policy	From the event code 1755 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12  "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Fails to connect to AD NPS server"
Displayed on the web interface	{{srcProcess}} Fails to connect to AD NPS{{authSrvrIp}} from SCG{{SCGMgmtIp}}
Description	This alarm is triggered when the RADIUS server fails to connect to the AD NPS server.
Recommended Actions	<ul style="list-style-type: none"> <li>Verify if the configured NPS server instance is up and running (Network Policy Server)</li> <li>Verify if the NPS server instance is communicating on the standard RADIUS port 1812</li> <li>Ensure that Windows server where AD/NPS server is provisioned can be reached from the controller web interface</li> </ul>

## RADIUS fails to authenticate with AD NPS server

**TABLE 45** RADIUS fails to authenticate with AD NPS server alarm

Alarm	RADIUS fails to authenticate with AD NPS server
Alarm Type	racADNPSFailToAuthenticate
Alarm Code	1756
Severity	Major
Aggregation Policy	From the event code 1756 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Fails to authenticate with AD NPS"

## Alarm Types

### Control and Data Plane Interface Alarms

**TABLE 45** RADIUS fails to authenticate with AD NPS server alarm (continued)

Alarm	RADIUS fails to authenticate with AD NPS server
Displayed on the web interface	{{srcProcess}} Fails to authenticate AD NPS{{authSrvrIp}} on SCG{{SCGMgmtIp}} for User{{userName}}
Description	This alarm is triggered when the RADIUS server fails to authenticate with the AD NPS server.
Recommended Actions	<ul style="list-style-type: none"><li>• The shared secret for NPS server should be same as that of administrator password provisioned in the controller web interface for AD server</li><li>• NPS should be configured to accept request (CHAP and MSCHAPv2) from the controller</li><li>• For CHAP authentication to work the AD server should store the password in reversible encryption format</li><li>• Ensure that NPS is registered with AD server</li></ul>

#### NOTE

Refer to [Authentication Events](#) on page 192.

## Fails to establish TLS tunnel with AD/LDAP

**TABLE 46** Fails to establish TLS tunnel with AD/LDAP alarm

Alarm	Fails to establish TLS tunnel with AD/LDAP
Alarm Type	racADLDAPTLSFailed
Alarm Code	1762
Severity	Major
Aggregation Policy	From the event code 1762 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12 "srcProcess"="RAC", "authSrvrIp" = "1.1.1.1" "authSrvrPort"="636", "SCGMgmtIp"="2.2.2.2" "desc"=" Fail to establish TLS Tunnel with LDAP/AD"
Displayed on the web interface	{{srcProcess}} Fails to authenticate AD NPS{{authSrvrIp}} on SCG{{SCGMgmtIp}} for User{{userName}}
Description	This alarm is triggered when TLS connection between the controller and AD/LDAP fails.

## Control and Data Plane Interface Alarms

#### NOTE

This section is not applicable for vSZ-H.

Following alarm is related to control and data plane.

- [GtpManager \(DP\) disconnected](#) on page 59

## GtpManager (DP) disconnected

**TABLE 47** GtpManager (DP) disconnected alarm

Alarm	GtpManager (DP) disconnected
Alarm Type	lostCnxnToDblade
Alarm Code	1202
Severity	Major
Aggregation Policy	From the event code 1202 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1201.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="NA", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2
Displayed on the web interface	The connectivity between Control plane {{ctrlBladeIp}} and Data plane {{dataBladeIp}} is lost at {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered due to transmission control protocol (TCP) connection loss or when control plane is unable to complete the configuration procedure successfully.
Recommended Actions	A manual intervention is required. Refer to <a href="#">Control and Data Plane Interface</a> on page 203 event 1201.

## Cloud Alarms

### Cloud Analytics Service has been Enabled

**TABLE 48** Cloud Analytics Service has been Enabled Alarm

Alarm	Cloud Analytics Service has been Enabled
Alarm Type	cloudAnalyticsEnabled
Alarm Code	4503
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service has been enabled successfully.
Description	This alarm occurs when Smart Zone successfully enables cloud analytics service.

### Cloud Analytics Service has been Disabled

**TABLE 49** Cloud Analytics Service has been Disabled Alarm

Alarm	Cloud Analytics Service has been Disabled
Alarm Type	cloudAnalyticsDisabled
Alarm Code	4504
Severity	Major
Attribute	

**TABLE 49** Cloud Analytics Service has been Disabled Alarm (continued)

Alarm	Cloud Analytics Service has been Disabled
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This alarm occurs when Smart Zone successfully disables cloud analytics service.

## Cloud Analytics Disconnected

**TABLE 50** Cloud Analytics Disconnected Alarm

Alarm	Cloud Analytics Disconnected
Alarm Type	cloudAnalyticsDisconnected
Alarm Code	4505
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service has been disconnected.
Description	This alarm occurs when Smart Zone disconnects cloud analytics service.

## Cluster Alarms

Following are the alarms related to cluster:

- [New node failed to join](#) on page 61
- [Node removal failed](#) on page 61
- [Node out of service](#) on page 62
- [Cluster in maintenance state](#) on page 62
- [Cluster backup failed](#) on page 63
- [Cluster restore failed](#) on page 63
- [Cluster upgrade failed](#) on page 64
- [Cluster application stopped](#) on page 64
- [Node bond interface down](#) on page 65
- [Node physical interface down](#) on page 65
- [Cluster node rebooted](#) on page 66
- [Cluster node shut down](#) on page 66
- [Disk usage exceed threshold](#) on page 67
- [Cluster out of service](#) on page 67
- [Cluster upload AP firmware failed](#) on page 68
- [Cluster add AP firmware failed](#) on page 68
- [Unsync NTP time](#) on page 69
- [Cluster upload KSP file failed](#) on page 69
- [Configuration backup failed](#) on page 69
- [Configuration restore failed](#) on page 70

- [AP certificate updated](#) on page 70
- [Upgrade SS table failed](#) on page 70
- [Cluster redundancy sync configuration failed](#) on page 71
- [Cluster redundancy restoring configuration failed](#) on page 71
- [Not all APs rehome after timeout](#) on page 71
- [Over switch max capacity](#) on page 72
- [AP is connected to Standby Cluster Over The Expiration Date](#) on page 72
- [Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy](#) on page 72
- [External DP Connected to Standby Cluster after Rehome Timeout](#) on page 73

## New node failed to join

**TABLE 51** New node failed to join alarm

Alarm	New node failed to join
Alarm Type	newNodeJoinFailed
Alarm Code	801
Severity	Critical
Aggregation Policy	From the event code 803 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 802.
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	New node [{nodeMac}] ({nodeName}) failed to join cluster [{clusterName}]
Description	This alarm is triggered when a node fails to join a cluster session. The web interface displays the error message.
Recommended Actions	When the operation fails, the user can run the <b>join process</b> . If it continues to fail, please send the complete system log files (stored in the path - /opt/ ruckuswireless/controller/log/system for analysis to RUCKUS support. Possible causes are: <ul style="list-style-type: none"> <li>• The joining node is unable to complete the syncing of data in time. This could be due to the existing node performing compaction/repair etc.</li> <li>• The communication between the nodes may be broken. This could cause the operation to timeout such as IP address change or due to other events, which affects the network. Usually, it does not last for a long period of time.</li> </ul>

## Node removal failed

**TABLE 52** Node removal failed alarm

Alarm	Node removal failed
Alarm Type	removeNodeFailed
Alarm Code	802
Severity	Major

**TABLE 52** Node removal failed alarm (continued)

Alarm	Node removal failed
Aggregation Policy	From the event code 805 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 804.
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] failed to remove from cluster [{clusterName}].
Description	This alarm is triggered when it is unable to remove a node from the cluster.
Recommended Actions	In general, this alarm should rarely occur. If it occurs, restore to the previous backup file and please send the system log files (stored in the path - /opt/ ruckuswireless/controller/log/system for analysis to RUCKUS support.

## Node out of service

**TABLE 53** Node out of service alarm

Alarm	Node out of service
Alarm Type	nodeOutOfService
Alarm Code	803
Severity	Critical
Aggregation Policy	From the event code 806 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 835.
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service. Reason:[{reason}].
Description	This alarm is triggered when a node is out of service.
Recommended Actions	The operator/user needs to check the application/interface state.

## Cluster in maintenance state

**TABLE 54** Cluster in maintenance state alarm

Alarm	Cluster in maintenance state
Alarm Type	clusterInMaintenanceState
Alarm Code	804
Severity	Critical
Aggregation Policy	From the event code 807 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 808.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] is in maintenance state

**TABLE 54** Cluster in maintenance state alarm (continued)

Alarm	Cluster in maintenance state
Description	This alarm is triggered when a cluster is in a maintenance state.
Recommended Actions	<p>Possible causes:</p> <ul style="list-style-type: none"> <li>The entire system backup is in process.</li> <li>In a two-node cluster, the remove-node process is working.</li> </ul> <p>For any other cause, please send the complete system log files (stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.</p>

## Cluster backup failed

**TABLE 55** Cluster backup failed alarm

Alarm	Cluster backup failed
Alarm Type	backupClusterFailed
Alarm Code	805
Severity	Major
Aggregation Policy	From the event code 810 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 809.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason:[{reason}].
Description	This alarm is triggered when a cluster backup fails.
Recommended Actions	<p>Check the disk usage. Try restoring the communication between nodes for a few more times. If the backup continues to fail or if you encounter Python script errors, please collect the complete system log files (stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis. Possible causes:</p> <ul style="list-style-type: none"> <li>Insufficient disk space.</li> <li>Communication between nodes may be broken.</li> <li>Errors due to the underlying Python script.</li> </ul>

## Cluster restore failed

**TABLE 56** Cluster restore failed alarm

Alarm	Cluster restore failed
Alarm Type	restoreClusterFailed
Alarm Code	806
Severity	Major
Aggregation Policy	From the event code 812 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 811.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] restore failed. Reason:[{reason}].

**TABLE 56** Cluster restore failed alarm (continued)

Alarm	Cluster restore failed
Description	This alarm is triggered when a cluster restore fails.
Recommended Actions	<p>Try a few more times. If the backup restore continues failing, please send the log files (stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.</p> <p>The possible cause could be that the command for all nodes in the cluster failed. This could be due to a broken communication link between the nodes.</p>

## Cluster upgrade failed

**TABLE 57** Cluster upgrade failed alarm

Alarm	Cluster upgrade failed
Alarm Type	upgradeClusterFailed
Alarm Code	807
Severity	Major
Aggregation Policy	From the event code 815 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 814.
Attribute	<p>"clusterName"="xxx", "nodeName"="xxx",</p> <p>"nodeMac"=" xx:xx:xx:xx:xx:xx", "fromVersion"="x.x",</p> <p>"toVersion"="x.x"</p>
Displayed on the web interface	Cluster {{clusterName}} could not be upgraded from {{fromVersion}} to {{toVersion}}. Reason:{{reason}}.
Description	This alarm is triggered when a version upgrade of a cluster fails.
Recommended Actions	<p>Check the disk usage. Try restoring the communication between nodes for a few more times. If the backup continues to fail or if you encounter Python script errors, please collect and send the complete system log files (stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.</p> <p>Possible causes:</p> <ul style="list-style-type: none"> <li>• Insufficient disk space</li> <li>• Communication between nodes might be broken.</li> <li>• Errors due to the underlying Python script.</li> </ul>

## Cluster application stopped

**TABLE 58** Cluster application stopped alarm

Alarm	Cluster application stopped
Alarm Type	clusterAppStop
Alarm Code	808
Severity	Critical
Aggregation Policy	From the event code 816 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 817.
Attribute	<p>"appName"="xxxx", "nodeName"="xxx",</p> <p>"nodeMac"=" xx:xx:xx:xx:xx:xx"</p>



**TABLE 58** Cluster application stopped alarm (continued)

Alarm	Cluster application stopped
Displayed on the web interface	Application [{appName}] on node [{nodeName}] stopped
Description	This alarm is triggered when the application on a node stops.
Recommended Actions	This could happen to any application for various reasons. Please collect and send the system log files of the stopped application (stored in the path - /opt/ ruckuswireless/controller/log/system to the application owner for analysis.

## Node bond interface down

**TABLE 59** Node bond interface down alarm

Alarm	Node bond interface down
Alarm Type	nodeBondInterfaceDown
Alarm Code	809
Severity	Major
Aggregation Policy	From the event code 821 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 822.
Attribute	"nodeName"="xxx", "nodeMac"="xxx", "ifName"="xxxx"
Displayed on the web interface	Network interface [{networkInterface}   {ifName}] on node [{nodeName}] is down.
Description	This alarm is triggered when the network interface of a node is down.
Recommended Actions	Check if the network cables of both the physical interfaces are broken. Alternatively, check if the physical interfaces for this bond interface are broken. Please send the log files stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.

## Node physical interface down

**TABLE 60** Node physical interface down alarm

Alarm	Node physical interface down
Alarm Type	nodePhyInterfaceDown
Alarm Code	810
Severity	Critical
Aggregation Policy	From the event code 824 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 825.
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Physical network interface [{networkInterface}   {ifName}] on node [{nodeName}] is down.
Description	This alarm is triggered when the physical interface of a node is down.

**TABLE 60** Node physical interface down alarm (continued)

Alarm	Node physical interface down
Recommended Actions	Check if the network cables of both the physical interfaces are broken. Alternatively, check if the physical interfaces for this bond interface are broken. Please send the log files stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.

## Cluster node rebooted

**TABLE 61** Cluster node rebooted alarm

Alarm	Cluster node rebooted
Alarm Type	nodeRebooted
Alarm Code	811
Severity	Major
Aggregation Policy	From the event code 826 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xxx", "nodeMac"="xxx"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] rebooted
Description	This alarm is triggered when the node is rebooted.
Recommended Actions	Usually, this occurs due to user actions like manual reboot of a node, upgrade or restoration of a cluster. Please send the log files stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.

## Cluster node shut down

**TABLE 62** Cluster node shut down alarm

Alarm	Cluster node shut down
Alarm Type	nodeShutdown
Alarm Code	813
Severity	Major
Aggregation Policy	From the event code 828 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 826.
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx "
Displayed on the web interface	Node [{nodeName}] has been shut down
Description	This alarm is triggered when the node shutdowns.
Recommended Actions	This usually occurs due to a user action. Please send the log files stored in the path - /opt/ ruckuswireless/controller/log/system to RUCKUS support for analysis.

## Node IP Changed

**TABLE 63** Node IP Changed alarm

Alarm	Node IP Changed
Alarm Type	nodeIPChanged
Alarm Code	823
Severity	Major
Aggregation Policy	From the event code 823 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 823.
Attribute	"clusterName"="xxx",
Displayed on the web interface	Cluster restore completed
Description	This alarm is triggered when the node IP is changed.
Recommended Actions	No Action Required

## Disk usage exceed threshold

**TABLE 64** Disk usage exceed threshold alarm

Alarm	Disk usage exceed threshold
Alarm Type	diskUsageExceed
Alarm Code	834
Severity	Critical
Aggregation Policy	From the event code 838 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xx", "status"="xx"
Displayed on the web interface	The disk usage of node [{nodeName}] is over {status}%.
Description	This alarm is triggered when the disk usage has reached the threshold limit. The disk usage percentage can be configured from 60% to 90%.
Recommended Actions	It is recommended that the user moves the backup files to the FTP server and deletes the moved backup files.

## Cluster out of service

**TABLE 65** Cluster out of service alarm

Alarm	Cluster out of service
Alarm Type	clusterOutOfService
Alarm Code	843
Severity	Critical
Aggregation Policy	From the event code 843 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 808.
Attribute	"clusterName"="xx"

**TABLE 65** Cluster out of service alarm (continued)

Alarm	Cluster out of service
Displayed on the web interface	Cluster {{clusterName}} is out of service.
Description	This alarm is triggered when the cluster service fails.
Recommended Actions	It is recommended that the operator or user checks the out of service node to locate the reason.

## Cluster upload AP firmware failed

**TABLE 66** Cluster upload AP firmware failed alarm

Alarm	Cluster upload AP firmware failed
Alarm Type	clusterUploadAPFirmwareFailed
Alarm Code	850
Severity	Major
Aggregation Policy	From the event code 850 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 849
Attribute	"clusterName"="xx"
Displayed on the web interface	Cluster {{clusterName}} upload AP firmware failed.
Description	This alarm is triggered when the cluster upload to AP firmware fails.
Recommended Actions	It is recommended that the operator uploads the AP patch.

## Cluster add AP firmware failed

**TABLE 67** Cluster add AP firmware failed alarm

Alarm	Cluster add AP firmware failed
Alarm Type	clusterAddAPFirmwareFailed
Alarm Code	853
Severity	Major
Aggregation Policy	From the event code 853 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 852
Attribute	"clusterName"="xx"
Displayed on the web interface	Cluster {{clusterName}} add AP firmware failed.
Description	This alarm is triggered when the cluster upload to AP firmware fails.
Recommended Actions	It is recommended that the operator applies the AP patch.

## Unsync NTP time

**TABLE 68** Unsync NTP time alarm

Alarm	Unsync NTP time
Alarm Type	unsyncNTPTime
Alarm Code	855
Severity	Major
Aggregation Policy	From the event code 855 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xx", "reason"="xx", "status"="xx"
Displayed on the web interface	Node {{nodeName}} time is not synchronized because of {{reason}}. The time difference is {{status}} seconds.
Description	This alarm is triggered when the cluster time is not synchronized.

## Cluster upload KSP file failed

**TABLE 69** Cluster upload KSP file failed alarm

Alarm	Cluster upload KSP file failed
Alarm Type	clusterUploadKspFileFailed
Alarm Code	858
Severity	Major
Aggregation Policy	From the event code 858 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 857
Attribute	"clusterName"="xx"
Displayed on the web interface	Cluster {{clusterName}} upload KSP file failed.
Description	This alarm is triggered when the cluster time is not synchronized.

## Configuration backup failed

**TABLE 70** Configuration backup failed alarm

Alarm	Configuration backup failed
Alarm Type	clusterCfgBackupFailed
Alarm Code	862
Severity	Major
Aggregation Policy	From the event code 862 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 861.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration backup failed.
Description	This alarm is triggered when the configuration backup fails.
Recommended Actions	Download the web log file from the controller web interface to check for errors.

## Configuration restore failed

**TABLE 71** Configuration restore failed alarm

Alarm	Configuration restore failed
Alarm Type	clusterCfgRestoreFailed
Alarm Code	864
Severity	Major
Aggregation Policy	From the event code 864 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 863.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration restore failed.
Description	This alarm is triggered when the cluster restoration fails.
Recommended Actions	Download the web log file from the web interface to check for errors.

## AP certificate updated

**TABLE 72** AP certificate updated alarm

Alarm	AP certificate updated
Alarm Type	apCertificateExpire
Alarm Code	865
Severity	Major
Aggregation Policy	From the event code 865 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 866.
Attribute	"count"="XXX"
Displayed on the web interface	{{count}} APs need to update their certificates.
Description	This alarm is triggered when the AP certificate expires.
Recommended Actions	Certificates on some APs need to be refreshed. On the web interface navigate to <b>Administration &gt; AP Certificate</b> replacement page to verify and follow the certificate refresh process.

## Upgrade SS table failed

**TABLE 73** Upgrade SS table failed alarm

Alarm	Upgrade SS table failed
Alarm Type	upgradeSSTableFailed
Alarm Code	868
Severity	Major
Aggregation Policy	From the event code 866 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xxx"

**TABLE 73** Upgrade SS table failed alarm (continued)

Alarm	Upgrade SS table failed
Displayed on the web interface	Node [{nodeName}] upgrade SSTable failed.
Description	This alarm is triggered when the SS table upgrade fails.

## Cluster redundancy sync configuration failed

**TABLE 74** Cluster redundancy sync configuration failed alarm

Alarm	Cluster redundancy sync configuration failed
Alarm Type	clusterRedundancySyncCfgFailed
Alarm Code	874
Severity	Major
Aggregation Policy	From the event code 874 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] sync configuration failed.
Description	This alarm is triggered when the cluster redundancy synchronization fails.

## Cluster redundancy restoring configuration failed

**TABLE 75** Cluster redundancy restoring configuration failed alarm

Alarm	Cluster redundancy restoring configuration failed
Alarm Type	clusterRedundantRestoreCfgFailed
Alarm Code	877
Severity	Major
Aggregation Policy	From the event code 868 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xxx"
Displayed on the web interface	Standby cluster [{clusterName}] restore a configuration failed.
Description	This alarm is triggered when the standby cluster restoration fails.

## Not all APs rehome after timeout

**TABLE 76** Not all APs rehome after timeout alarm

Alarm	Not all APs rehome after timeout
Alarm Type	clusterRedundancyApRehomeIncomplete
Alarm Code	881
Severity	Major
Aggregation Policy	From the event code 881 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"count"="xxx"

**TABLE 76** Not all APs rehome after timeout alarm (continued)

Alarm	Not all APs rehome after timeout
Displayed on the web interface	Standby cluster still has {{count}} AP connected.
Description	This alarm is triggered when the AP is still connected to the standby cluster.

## Over switch max capacity

**TABLE 77** Over switch max capacity alarm

Alarm	Over switch max capacity
Alarm Type	OverSwitchMaxCapacity
Alarm Code	21001
Severity	Critical
Aggregation Policy	From the event code 21001, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	
Displayed on the web interface	The volume of switches is over system capacity.
Description	This alarm is triggered when the volume of switches is over system capacity.

## AP is connected to Standby Cluster Over The Expiration Date

**TABLE 78** AP is connected to standby cluster over the expiration date alarm

Alarm	AP Certificate Expired
Alarm Type	ApConnectedToStandbyClusterOverTheExpirationDate
Alarm Code	188
Severity	Critical
Attribute	apMac="xx:xx:xx:xx:xx:xx", days="xx"
Displayed on the web interface	The AP{{apMac}} is connected to standby cluster over {{days}} days, please move it to active cluster to avoid service interruption
Description	This alarm occurs when a AP is connected to standby cluster over the expiration date.

## Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy

**TABLE 79** Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy alarm

Alarm	Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Alarm Type	ActiveClusterUnabletoConnectOtherActiveClustersforClusterRedundancy
Alarm Code	882
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}} Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Description	This alarm occurs when active cluster unable to connect to other active clusters for cluster redundancy.



## External DP Connected to Standby Cluster after Rehome Timeout

**TABLE 80** External DP Connected to Standby Cluster after Rehome Timeout alarm

Alarm	External DP Connected to Standby Cluster after Rehome Timeout
AlarmType	ExternalDPConnectedtoStandbyCluster
Alarm Code	887
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}}This alarm occurs when there is still external DP connected to standby cluster after rehome timeout
Description	This alarm occurs when there is still external DP connected to standby cluster after rehome timeout.

## Certificate is about to Expire

**TABLE 81** Certificate is about to Expire alarm

Alarm	Certificate is about to Expire
Alarm Type	certificateAboutToExpire
Alarm Code	890
Severity	Major
Aggregation Policy	From the event code 890 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate {{certName}} is about to expire in {{days}} days ({{expireDateTime}})
Description	This alarm occurs when a certificate is about to expire.
Recommended Actions	Renew the certificate that is about to expire or import another valid certificate to replace the current one.

## Certificate is already Expired

**TABLE 82** Certificate is already Expired alarm

Alarm	Certificate is already Expired
Alarm Type	restoreClusterExpired
Alarm Code	891
Severity	Major
Aggregation Policy	From the event code 891 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate {{certName}} is already expired since {expireDateTime}
Description	This alarm occurs when certificate already expires.
Recommended Actions	Renew the certificate that already expires or import another valid certificate to replace the current one.

## Configuration Alarms

Following are the alarms related to configuration.

- [Zone configuration preparation failed](#) on page 74
- [AP configuration generation failed](#) on page 74
- [End-of-life AP model detected](#) on page 75
- [VLAN configuration mismatch on non DHCP/NAT WLAN](#) on page 75
- [VLAN configuration mismatch on DHCP/NAT WLAN](#) on page 75

### Zone configuration preparation failed

**TABLE 83** Zone configuration preparation failed alarm

Alarm	Zone configuration preparation failed
Alarm Type	zoneCfgPrepareFailed
Alarm Code	1021
Severity	Major
Aggregation Policy	From the event code 1021 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone"
Displayed on the web interface	Failed to prepare zone [{zoneName}] configuration required by ap configuration generation
Description	This alarm is triggered when the controller is unable to prepare a zone configuration required by the AP.
Recommended Actions	APs under these zone stay functional but are unable to receive new settings. Contact RUCKUS support to file an error bug along with the log file.

### AP configuration generation failed

**TABLE 84** AP configuration generation failed alarm

Alarm	AP configuration generation failed
Alarm Type	apCfgGenFailed
Alarm Code	1022
Severity	Major
Aggregation Policy	From the event code 1022 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "apCfgGenFailedCount"="25"
Displayed on the web interface	Failed to generate configuration for [{apCfgGenFailedCount}] AP(s) under zone[{zoneName}]
Description	This alarm is triggered when the controller fails to generate the AP configuration under a particular zone.
Recommended Actions	APs under these zone stay functional but are unable to receive the new settings. Contact RUCKUS support to file an error bug along with the log file.

## End-of-life AP model detected

**TABLE 85** End-of-life AP model detected alarm

Alarm	End-of-life AP model detected
Alarm Type	cfgGenSkippedDueToEolAp
Alarm Code	1023
Severity	Major
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "model"="R300,T300"
Displayed on the web interface	Detected usage of end-of-life ap model(s)[{model}] while generating configuration for AP(s) under zone[{zoneName}]
Description	This alarm is triggered when the controller detects the AP model's end-of-life under a certain zone.
Recommended Actions	<p>These obsoleted APs occupies licensed AP space. Disconnect these unsupported AP models from the given zone by:</p> <ul style="list-style-type: none"> <li>Reset the APs to a factory setting using the AP command line</li> <li>Delete these APs through the <b>controller Web Interface &gt; Configuration AP List</b></li> </ul>

**NOTE**

Refer to [Configuration Events](#) on page 251.

## VLAN configuration mismatch on non DHCP/NAT WLAN

**TABLE 86** VLAN configuration mismatch on non DHCP/NAT WLAN alarm

Alarm	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN
Alarm Type	apCfgNonDhcpNatWlanVlanConfigMismatch
Alarm Code	1024
Severity	Critical
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ssid"="xxxx", "wlanID"="xxxx", "configuredVlan"="5"
Displayed on the web interface	DHCP/NAT gateway AP [{apMac}] detected VLAN configuration mismatch on non-DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This alarm is triggered when the AP detects a non DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

## VLAN configuration mismatch on DHCP/NAT WLAN

**TABLE 87** VLAN configuration mismatch on DHCP/NAT WLAN alarm

Alarm	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on DHCP/NAT WLAN
Alarm Type	apCfgDhcpNatWlanVlanConfigMismatch
Alarm Code	1025

## Alarm Types

### Data Plane Alarms

**TABLE 87** VLAN configuration mismatch on DHCP/NAT WLAN alarm (continued)

Alarm	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on DHCP/NAT WLAN
Severity	Critical
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ssid"="xxxx", "wlanID"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [{apMac}] detected VLAN configuration mismatch on DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This alarm is triggered when the AP detects a DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

## Data Plane Alarms

### NOTE

Alarms 510, 516, 517 and 519 are not applicable for vSZ-H.

Following are the alarms related to data plane.

- [Data plane configuration update failed](#) on page 76
- [Data plane disconnected](#) on page 77
- [Data plane physical interface down](#) on page 77
- [Data plane rebooted](#) on page 78
- [Data plane packet pool is under low water mark](#) on page 78
- [Data plane packet pool is under critical low water mark](#) on page 78
- [Data plane core dead](#) on page 79
- [Data plane process restarted](#) on page 79
- [Data plane license is not enough](#) on page 79
- [Data plane upgrade failed](#) on page 80
- [Data plane of data center side fails to connect to the CALEA server](#) on page 81
- [Data plane fails to connects to the other data plane](#) on page 81
- [Data plane DHCP IP pool usage rate is 100 percent](#) on page 81

## Data plane configuration update failed

**TABLE 88** Data plane configuration update failed alarm

Alarm	Data plane configuration update failed
Alarm Type	dpConfUpdateFailed
Alarm Code	501
Severity	Major
Aggregation Policy	From the event code 505 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 504

**TABLE 88** Data plane configuration update failed alarm (continued)

Alarm	Data plane configuration update failed
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"=" 123456781234567"
Displayed on the web interface	Data plane [{dpName}   {dpKey}] failed to update to configuration [{configID}].
Description	This alarm is triggered when the data plane configuration update fails since it was unable to transfer the configuration update from the control plane to the data plane.
Recommended Actions	Check the data plane configuration and the CPU utilization of the control plane. The possible cause could be of the server being busy at that particular moment. Check to see if the event is persistent.

## Data plane disconnected

**TABLE 89** Data plane disconnected alarm

Alarm	Data plane disconnected
Alarm Type	dpDisconnected
Alarm Code	503
Severity	Critical
Aggregation Policy	From the event code 513 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 512.
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName}   {dpKey}] disconnected from {produce.short.name} [{cpName}   {wsgIP}]
Description	This alarm is triggered when the data plane gets disconnected from the controller since it fails to update its status to the control plane.
Recommended Actions	Check if the communicator is still alive and if the cluster interface is working.

## Data plane physical interface down

**TABLE 90** Data plane physical interface down alarm

Alarm	Data plane physical interface down
Alarm Type	dpPhyInterfaceDown
Alarm Code	504
Severity	Critical
Aggregation Policy	From the event code 514 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 515.
Attribute	"portID"="xx", "dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName}   {dpKey}] is down
Description	This alarm is triggered when the physical interface link of the data plane is down due to the fiber cable connection.
Recommended Actions	Check if the fiber cable between the data plane and the switch is firmly connected.

## Data plane rebooted

**TABLE 91** Data plane rebooted alarm

Alarm	Data plane rebooted
Alarm Type	dpReboot
Alarm Code	510
Severity	Minor
Aggregation Policy	From the event code 506 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx",
Displayed on the web interface	Data plane [{dpName   dpKey}] rebooted
Description	This alarm is triggered when the data plane is rebooted.
Recommended Actions	No action is required.

## Data plane packet pool is under low water mark

**TABLE 92** Data plane packet pool is under low water mark alarm

Alarm	Data plane packet pool is under low water mark
Alarm Type	dpPktPoolLow
Alarm Code	516
Severity	Major
Aggregation Policy	From the event code 516 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 518.
Attribute	"dpKey"="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName   dpKey}] is under low-water mark.
Description	This alarm is triggered when the data core packet pool is below the water mark level.
Recommended Actions	The operator needs to check for network looping.

## Data plane packet pool is under critical low water mark

**TABLE 93** Data plane's packet pool is under critical low water mark alarm

Alarm	Data plane packet pool is under critical low water mark
Alarm Type	dpPktPoolCriticalLow
Alarm Code	517
Severity	Critical
Aggregation Policy	From the event code 517 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpKey="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName   dpKey}] is under critical low-water mark.
Description	This alarm is triggered when the data core packet pool reaches the critical water mark level.

**TABLE 93** Data plane's packet pool is under critical low water mark alarm (continued)

Alarm	Data plane packet pool is under critical low water mark
Recommended Actions	The operator needs to check for network looping.

## Data plane core dead

**TABLE 94** Data plane core dead alarm

Alarm	Data plane core dead
Alarm Type	dpCoreDead
Alarm Code	519
Severity	Critical
Aggregation Policy	From the event code 519 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpKey="xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane {{dpName     dpKey}} has dead data core.
Description	This alarm is triggered when one or multiple data core packet pool is lost /dead.
Recommended Actions	No action required.

## Data plane process restarted

**TABLE 95** Data plane process restarted alarm

Alarm	Data plane process restarted
Alarm Type	dpProcessRestart
Alarm Code	520
Severity	Major
Aggregation Policy	From the event code 520 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpKey="xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	{{processName}} process got re-started on data plane {{dpName&&dpKey}}
Description	This alarm is triggered when any process on data plane crashes and restarts.
Recommended Actions	No action required.

## Data plane license is not enough

**NOTE**

Alarm 538 is applicable only for vSZ-H.

**TABLE 96** Data plane license is not enough alarm

Alarm	Data plane license is not enough
Alarm Type	dpLicenseInsufficient
Alarm Code	538
Severity	Major

## Alarm Types

### Data Plane Alarms

**TABLE 96** Data plane license is not enough alarm (continued)

Alarm	Data plane license is not enough
Aggregation Policy	From the event code 538 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"count"=<delete-vdp-count>
Displayed on the web interface	DP license is not enough, [{count}] instance of DP will be deleted.
Description	This alarm is triggered when the number of data plane licenses are insufficient.
Recommended Actions	Check if the number of data plane licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses and synchronize the licenses.

## Data plane upgrade failed

### NOTE

Alarm 553 is applicable only for vSZ-H

**TABLE 97** Data plane upgrade failed alarm

Alarm	Data plane upgrade failed
Alarm Type	dpLicenseInsufficient
Alarm Code	553
Severity	Major
Aggregation Policy	From the event code 553 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to upgrade.
Description	This alarm is triggered when the data plane upgrade fails.
Recommended Actions	<p>There are several possible reasons to trigger alarm 553. The operator has to ensure the accuracy of network connectivity and version availability. For advanced process, check the debug log for reason of upgrade failure. Debug file includes the upgrade log file. The operator can get the debug log from vSZ web interface or through vSZ-D CLI.</p> <p>The operator can use the following vSZ-D CLI commands to:</p> <ul style="list-style-type: none"><li>• View the previous upgrade status and reason in case of a failure - ruckus# show upgrade-state / ruckus# show upgrade-history</li><li>• Save the debug file for viewing - ruckus (debug) # save-log</li><li>• Check the connection status between vSZ and vSZ-D - ruckus# show status</li><li>• Check the current vSZ-D software version - ruckus # show version</li></ul> <p><b>NOTE</b> Refer to the vSZ-D CLI Reference Guide for details on the CLI commands mentioned above.</p>



## Data plane of data center side fails to connect to the CALEA server

**TABLE 98** Data plane of data center side fails to connect to the CALEA server alarm

Alarm	Data plane of data center side fails to connect to the CALEA server
Alarm Type	dpDcToCaleaConnectFail
Alarm Code	1258
Severity	Major
Aggregation Policy	From the event code 1258 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side[{dpName&&dpKey}] fails to connects to the CALEA server[{caleaServerIP}]
Description	This alarm is triggered when the data plane fails to connect to the CALEA server.
Recommended Actions	Check the connectivity between data plane and CALEA server.

## Data plane fails to connects to the other data plane

**TABLE 99** Data plane fails to connects to the other data plane alarm

Alarm	Data plane fails to connects to the other data plane
Alarm Type	dpP2PTunnelConnectFail
Alarm Code	1261
Severity	Major
Aggregation Policy	From the event code 1261 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] fails connects to the other Data Plane[{targetDpKey&&targetDpIP}]
Description	This alarm is triggered when the data plane fails to connect to another data plane.
Recommended Actions	Check the connectivity between data planes.

## Data plane DHCP IP pool usage rate is 100 percent

**TABLE 100** Data plane DHCP IP pool usage rate is 100 percent alarm

Alarm	Data plane DHCP IP pool usage rate is 100 percent
Alarm Type	dpDhcpIpPoolUsageRate100
Alarm Code	1265
Severity	Critical
Aggregation Policy	From the event code 1265 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] DHCP IP Pool usage rate is 100 percent
Description	This alarm is triggered when the data plane DHCP pool usage rate reaches 100%

## Alarm Types

### Data Streaming Alarms

**TABLE 100** Data plane DHCP IP pool usage rate is 100 percent alarm (continued)

Alarm	Data plane DHCP IP pool usage rate is 100 percent
Recommended Actions	Increase the size of the DHCP IP address pool, or reduce the number of stations requiring addresses.

## Data Streaming Alarms

[Connecting Failure to a Data Streaming Profile](#) on page 82

### Connecting Failure to a Data Streaming Profile

**TABLE 101** Connecting Failure to a Data Streaming Profile alarm

Alarm	Connecting Failure to a Data Streaming Profile
Alarm Type	connectingFailure
Alarm Code	4703
Severity	Critical
Displayed on the web interface	The system is failing to connect to a data streaming profile.
Description	This alarm is triggered when the system is failing to connect to a data streaming profile.

## Gn/S2a Interface Alarms

### NOTE

This section is not applicable for vSZ-H.

Following are the alarms related to Gn/S2a interface.

- [GGSN restarted](#) on page 83
- [GGSN not reachable](#) on page 83
- [GGSN not resolved](#) on page 83
- [PDNGW could not be resolved](#) on page 84
- [PDNGW version not supported](#) on page 84
- [Associated PDNGW down](#) on page 85
- [Create session response failed](#) on page 85
- [Decode failed](#) on page 86
- [Modify bearer response failed](#) on page 86
- [Delete session response failed](#) on page 86
- [Delete bearer request failed](#) on page 87
- [Update bearer request failed](#) on page 87
- [CGF server not configured](#) on page 88

## GGSN restarted

**TABLE 102** GGSN restarted alarms

Alarm	GGSN restarted
Alarm Type	ggsnRestarted
Alarm Code	1210
Severity	Major
Aggregation Policy	From the event code 1210 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm", "realm"="NA", "gtpclp"="5.5.5.5", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2",
Displayed on the web interface	GGSN [{{ggsnIp}}] connected to {produce.short.name} [{{SCGMgmtIp}}] (GTPC-IP [{{gtpclp}}]) is restarted.
Description	This alarm is triggered when the GTP control plane (GTP-C) receives a new recovery value.
Recommended Actions	Refer to the log file for Gateway GPRS Support Node (GGSN) restart.

## GGSN not reachable

**TABLE 103** GGSN not reachable alarms

Alarm	GGSN not reachable
Alarm Type	ggsnNotReachable
Alarm Code	1211
Severity	Major
Aggregation Policy	From the event code 1211 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm", "realm"="NA", "gtpclp"="5.5.5.5", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2",
Displayed on the web interface	GGSN [{{ggsnIp}}] connected to {produce.short.name} (GTPC-IP [{{gtpclp}}]) is not reachable
Description	This alarm is triggered when the echo request is timed out.
Recommended Actions	Refer to the log file.

## GGSN not resolved

**TABLE 104** GGSN not resolved alarm

Alarm	GGSN not resolved
Alarm Type	ggsnNotResolved
Alarm Code	1215
Severity	Major

## Alarm Types

### Gn/S2a Interface Alarms

**TABLE 104** GGSN not resolved alarm (continued)

Alarm	GGSN not resolved
Aggregation Policy	From the event code 1215 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="wlan.3gppnetwork.org", "gtcpIp"="5.5.5.5", "apn"="ruckuswireless.com", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787",
Displayed on the web interface	Failed to resolve GGSN from APN [{apn}] for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]
Description	This alarm is triggered when the access point name (APN) fails at GGSN.
Recommended Actions	Manual intervention is required. Correct the DNS configuration in the controller web interface.

## PDNGW could not be resolved

**TABLE 105** PDNGW could not be resolved alarm

Alarm	PDNGW could not be resolved
Alarm Type	pdnGwNotResolved
Alarm Code	1950
Severity	Critical
Aggregation Policy	From the event code 1950 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	mvsold"=12 "wlanId"=1 "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", srcProcess"="aut" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com"
Displayed on the web interface	[[srcProcess]] APN [{apn}] could not be resolved on {produce.short.name} [[SCGMgmtIp]], with username [{ueImsi}@{realm}]
Description	This alarm is triggered when the APN is unable to resolve to PDN Gateway (PDN GW).
Recommended Actions	Modify the DNS server configuration in the controller web interface.

## PDNGW version not supported

**TABLE 106** PDNGW version not supported alarm

Alarm	PDNGW version not supported
Alarm Type	pdnGwVersionNotSupportedMsgReceived
Alarm Code	1952
Severity	Major
Aggregation Policy	From the event code 1952 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_process" "realm"="NA" "gtcpIp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2"

**TABLE 106** PDNGW version not supported alarm (continued)

Alarm	PDNGW version not supported
Displayed on the web interface	{{srcProcess}} Version not supported message received from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}}.
Description	This alarm is triggered when the version is not supported for messages received from PDN GW.
Recommended Actions	Verify and correct the GPRS tunneling protocol (GTP) version supported in the PGW is GTPv1 and GTPv2.

## Associated PDNGW down

**TABLE 107** Associated PDNGW down alarm

Alarm	Associated PDNGW down
Alarm Type	pdnGwAssociationDown
Alarm Code	1953
Severity	Critical
Aggregation Policy	From the event code 1953 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_process" "realm"="NA" "gtPclp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} Association with PDN GW with IP {{pgwIp}} from {produce.short.name} {{SCGMgmtIp}} down
Description	This alarm is triggered when the association with PDN GW is down due to echo request time out or it fails to send messages to PDN GW.
Recommended Actions	Check the interface from the controller to PDN GW in the web interface to ensure it is reachable.

## Create session response failed

**TABLE 108** Create session response failed alarm

Alarm	Create session response failed
Alarm Type	createSessionResponseFailed
Alarm Code	1954
Severity	Major
Aggregation Policy	From the event code 1954 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mVnld"="12" "wlanId"="1" "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "gtPclp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "apn"="ruckus.com" "cause"="<reason for failure>"
Displayed on the web interface	{{srcProcess}} Create Session response from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	This alarm is triggered when create session response from PDN GW fails as per the specified cause.
Recommended Actions	Download the SM log to check the cause of the error.

## Decode failed

**TABLE 109** Decode failed alarm

Alarm	Decode failed
Alarm Type	decodeFailed
Alarm Code	1955
Severity	Major
Aggregation Policy	From the event code 1955 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="NA" "gtplcp"="5.5.5.5" "pgwlp"="1.1.1.1" "SCGMgmtlp"="2.2.2.2"
Displayed on the web interface	[[srcProcess]] Decode of message received from PDN GW with IP [[pgwlp]] on {produce.short.name} [[SCGMgmtlp]] failed.
Description	This alarm is triggered when decoding of messages received from PDN GW fails.
Recommended Actions	Download the SM log to check the cause of the error.

## Modify bearer response failed

**TABLE 110** Modify bearer response failed alarm

Alarm	Modify bearer response failed
Alarm Type	modifyBearerResponseFailed
Alarm Code	1956
Severity	Major
Aggregation Policy	From the event code 1956 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mncid"="12" "wlanId"="1" "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "gtplcp"="5.5.5.5" "pgwlp"="1.1.1.1" "SCGMgmtlp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "apn"="ruckus.com" "cause"="<reason for failure>"
Displayed on the web interface	[[srcProcess]] Modify Bearer Response from PDN GW with IP [[pgwlp]] on {produce.short.name} [[SCGMgmtlp]] failed, for UE with username [[ueImsi]]@{realm} because [[cause]]
Description	This alarm is reported when the modify bearer response from PDN GW fails as per the specified cause.
Recommended Actions	Download the SM log to check the cause of the error.

## Delete session response failed

**TABLE 111** Delete session response failed alarm

Alarm	Delete session response failed
Alarm Type	deleteSessionResponseFailed
Alarm Code	1957
Severity	Major
Aggregation Policy	From the event code 1957 an alarm is raised for every event. A single event triggers a single alarm.

**TABLE 111** Delete session response failed alarm (continued)

Alarm	Delete session response failed
Attribute	"mvnold"="12" "wlanId"="1" "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "gtcpIp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "apn"="ruckus.com" "cause"="<reason for failure>"
Displayed on the web interface	{{srcProcess}} Delete Session response from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	Delete session response from PDN GW fails due to the specified cause.
Recommended Actions	Download the SM log to check the cause of the error.

## Delete bearer request failed

**TABLE 112** Delete bearer request failed alarm

Alarm	Delete bearer request failed
Alarm Type	deleteBearerRequestFailed
Alarm Code	1958
Severity	Major
Aggregation Policy	From the event code 1958 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "gtcpIp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2" "cause"="<reason for failure>"
Displayed on the web interface	{{srcProcess}} Delete Bearer Request from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	This alarm is triggered when the delete bearer request from PDN GW fails.
Recommended Actions	Download the SM log to check the cause of the error.

## Update bearer request failed

**TABLE 113** Update bearer request failed alarm

Alarm	Update bearer request failed
Alarm Type	updateBearerRequestFailed
Alarm Code	1959
Severity	Major
Aggregation Policy	From the event code 1959 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "gtcpIp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2" "cause"="<reason for failure>"
Displayed on the web interface	{{srcProcess}} Update bearer request from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	Update bearer request failed, decode failed.
Recommended Actions	Download the SM log to check the cause of the error.

## CGF server not configured

**TABLE 114** CGF server not configured alarm

Alarm	CGF server not configured
Alarm Type	cgfServerNotConfigured
Alarm Code	1960
Severity	Major
Aggregation Policy	From the event code 1960 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"mvsold"="12" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="CIP" "realm"="NA" "ggsnIp"="10.10.10.10" "SCGMgmtIp"="2.2.2.2" "radSvrIp"="7.7.7.7" "cgfSvrIp"="1.1.1.1"
Displayed on the web interface	CGF server IP {{cgfSvrIp}} received from PDN GW/GGSN with IP {{ggsnIp}} on {produce.short.name} [{SCGMgmtIp}] is not configured
Description	This alarm is triggered when the IP address of the CGF server received from GGSN/PDNGW is not configured in the controller web interface and therefore is not considered.
Recommended Actions	Check the controller web interface to ensure that the IP address of the CGF server received from PDNGW/GGSN is configured. If it is not configure navigate to Configurations > Services and Profiles > CGF Services to create the configuration.

## GR Interface Alarms

### NOTE

This section is not applicable for vSZ-H.

Following are the alarms related to GR interface.

- [Destination not reachable](#) on page 88
- [App server down](#) on page 89
- [App server inactive](#) on page 89
- [Association establishment failed](#) on page 90
- [Association down](#) on page 90
- [Outbound routing failure](#) on page 91
- [Did allocation failure](#) on page 91

## Destination not reachable

**TABLE 115** Destination not reachable alarm

Alarm	Destination not reachable
Alarm Type	destNotReacheable
Alarm Code	1618
Severity	Critical
Aggregation Policy	From the event code 1618 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1620.



**TABLE 115** Destination not reachable alarm (continued)

Alarm	Destination not reachable
Attribute	"mvmold"="2", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip";"pointCode"="1.1.1"
Displayed on the web interface	Remote Point Code {{pointCode}} is unavailable
Description	This alarm is triggered when the point code is unreachable due to a pause indicator.
Recommended Actions	Manual intervention is required.

## App server down

**TABLE 116** App server down alarm

Alarm	App server down
Alarm Type	appServerDown
Alarm Code	1623
Severity	Critical
Aggregation Policy	From the event code 1623 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1625.
Attribute	"mvmold"="2", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip", "routingContext"="1", "pointCode"="1.1.1", "SSN"="7"
Displayed on the web interface	Application Server Down, Routing Context {{routingContext}}, local Point Code {{pointCode}}, local SSN {{SSN}}
Description	This alarm is triggered when the local application server is down due to the receipt of ASP down (ASPDN) or ASP down acknowledgment (ASPDN ACK) received from the remote IP security protocol (IPSP) or signalling gateway (SG).
Recommended Actions	Manual intervention is required.

## App server inactive

**TABLE 117** App server inactive alarm

Alarm	App server inactive
Alarm Type	appServerInactive
Alarm Code	1624
Severity	Critical
Aggregation Policy	From the event code 1624 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1625.
Attribute	"mvmold"="2", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip", "routingContext"="1", "pointCode"="1.1.1", "SSN"="7"
Displayed on the web interface	Application Server Inactive, Routing Context {{routingContext}}, lpcal Point Code {{pointCode}}, local SSN {{SSN}}

## Alarm Types

### GR Interface Alarms

**TABLE 117** App server inactive alarm (continued)

Alarm	App server inactive
Description	This alarm is triggered when the local application server is inactive due to application service provider inactive (ASP_INACTIVE) or application service provider inactive acknowledgment (ASP_INACTIVE_ACK) from remote IP security protocol (IPSP) or signalling gateway (SG).
Recommended Actions	Manual intervention is required.

## Association establishment failed

**TABLE 118** Association establishment failed alarm

Alarm	Association establishment failed
Alarm Type	assocEstbFailed
Alarm Code	1626
Severity	Critical
Aggregation Policy	From the event code 1626 an alarm is raised for every five events or events occurring within a span of 2 minutes.
Auto Clearance	The alarm code is auto cleared with the event code 1628.
Attribute	"mvsold"="3", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip", "srcIP"="10.1.4.10", "srcPort"="2960", "destIP"="10.1.4.20", "destPort"="2960"
Displayed on the web interface	Unable to establish SCTP association. srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This alarm is triggered when it is unable to establish an association to the IP security protocol (IPSP) or signalling gateway (SG).
Recommended Actions	Manual intervention is required.

## Association down

**TABLE 119** Association down alarm

Alarm	Association down
Alarm Type	assocDown
Alarm Code	1627
Severity	Critical
Aggregation Policy	From the event code 1627 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1628.
Attribute	"mvsold"="3", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip", "srcIP"="10.1.4.10", "srcPort"="2960", "destIP"="10.1.4.20", "destPort"="2960"
Displayed on the web interface	SCTP association DOWN. srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This alarm is triggered when the stream control transmission protocol (SCTP) association is down.
Recommended Actions	Manual intervention is required.

## Outbound routing failure

**TABLE 120** Outbound routing failure alarm

Alarm	Outbound routing failure
Alarm Type	outboundRoutingFailure
Alarm Code	1636
Severity	Critical
Aggregation Policy	From the event code 1636 an alarm is raised for every 10 events. Alarm is raised for 10 or more events or events occurring within a span of 60 seconds.
Attribute	"mvsold"="2", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip", "operation"="updateGprsLocationReq", "hlrInstance"=" Operator_HLR", "uelmsi"=" 04844624203918"
Displayed on the web interface	Unable to route [{operation}] for IMSI [{uelmsi}] to HLR [{hlrInstance}]
Description	This alarm is triggered when a transaction capabilities application part (TCAP) message is unable to route to its destination.
Recommended Actions	Manual intervention is required.

## Did allocation failure

**TABLE 121** Did allocation failure alarm

Alarm	Did allocation failure
Alarm Type	didAllocationFailure
Alarm Code	1637
Severity	Critical
Aggregation Policy	From the event code 1637 an alarm is raised for every 50 events. Alarm is raised for 50 or more events or events occurring within a span of 60 seconds.
Attribute	"mvsold"="2", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="hip"
Displayed on the web interface	HIP unable to allocate new dialogue
Description	This alarm is triggered when it is unable to allocate a dialogue identifier for a new transaction. This indicates an overload condition.
Recommended Actions	Manual intervention is required.

## IPMI Alarms

### NOTE

This section is not applicable for vSZ-H.

Following are the alarms related to IPMIs.

- [ipmiVoltage](#) on page 93
- [ipmiThempBB](#) on page 94
- [ipmiThempFP](#) on page 94
- [ipmiThempIOH](#) on page 95

## Alarm Types

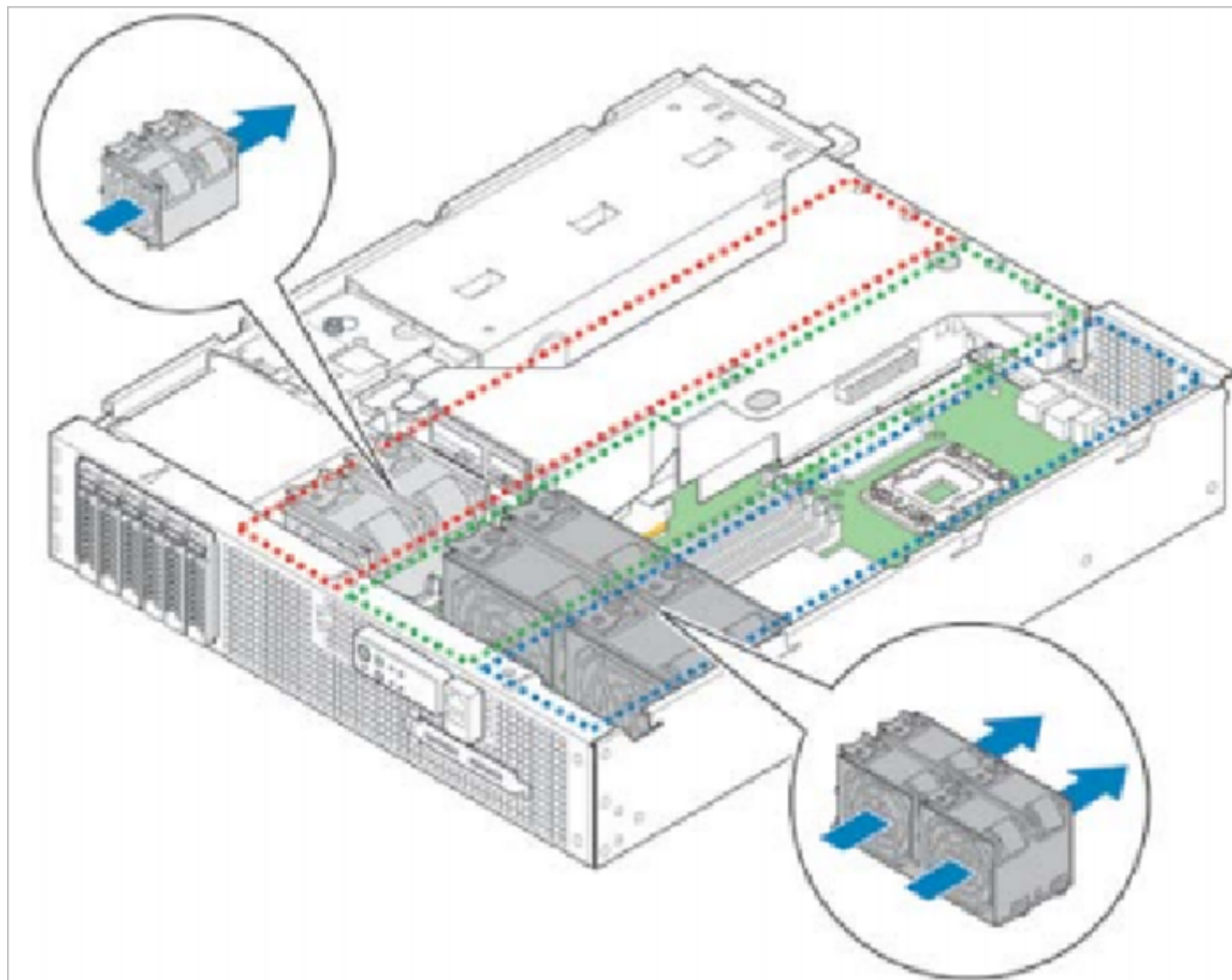
### IPMI Alarms

- [ipmiThempMemP](#) on page 95
- [ipmiThempPS](#) on page 96
- [ipmiThempP](#) on page 96
- [ipmiThempHSBP](#) on page 96
- [ipmiFan](#) on page 97
- [ipmiPower](#) on page 97
- [ipmiCurrent](#) on page 98
- [ipmiFanStatus](#) on page 98
- [ipmiPsStatus](#) on page 98
- [ipmiDrvStatus](#) on page 99

The controller has redundant six-fan cooling with four 80x38mm fans and two 60x38mm fans. There are four main cooling zones, as shown in [Figure 3](#):

- Zone 1 contains fans 0 and 1, which cool CPU1 and all the components in this zone.
- Zone 2 contains fans 2 and 3, which cool CPU2, low-profile PCI cards, and all the other components in this zone.
- Zone 3 contains fans 4 and 5, which cool full-height/length PCI cards and all the other components in this area.
- Zone 4 is cooled by the power supply fans. This zone contains the SAS RAID and SAS/SATA boards. Cooling redundancy in this zone is only achieved when there are two power supplies installed.

**FIGURE 3** Server Cooling Areas



## ipmiVoltage

**TABLE 122** ipmiVoltage alarm

Alarm	ipmiVoltage
Alarm Type	ipmiVoltage
Alarm Code	901
Severity	Major
Aggregation Policy	From the event code 901 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 926.
Attribute	"id"="x", "status"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"

**TABLE 122** ipmiVoltage alarm (continued)

Alarm	ipmiVoltage
Displayed on the web interface	Baseboard voltage [{status}] on control plane [{nodeMac}]
Description	<p>This alarm is triggered due to under/over voltage on the control plane. Baseboard threshold temperatures are:</p> <ul style="list-style-type: none"> <li>• Critical high - 66<sup>0</sup> C</li> <li>• Non critical high - 61<sup>0</sup> C</li> <li>• Non critical low - 10<sup>0</sup> C</li> <li>• Critical low - 5<sup>0</sup> C</li> </ul>
Recommended Actions	Replace the power supply cord. If it does not work, the motherboard needs replacement.

## ipmiThempBB

**TABLE 123** ipmiThempBB alarm

Alarm	ipmiThempBB
Alarm Type	ipmiThempBB
Alarm Code	902
Severity	Major
Aggregation Policy	From the event code 902 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 927.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered due to the increase/decrease of the baseboard temperature status of the control plane. Baseboard threshold temperatures are in the range of 10 <sup>0</sup> Celsius to 61 <sup>0</sup> Celsius. The default threshold is 61 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

## ipmiThempFP

**TABLE 124** ipmiThempFP alarm

Alarm	ipmiThempFP
Alarm Type	ipmiThempFP
Alarm Code	903
Severity	Major
Aggregation Policy	From the event code 903 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 928.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}]

**TABLE 124** ipmiThempFP alarm (continued)

Alarm	ipmiThempFP
Description	This alarm is triggered due to increase/decrease of the front panel temperature status of the control plane. Front panel threshold temperatures are in the range of 5 <sup>0</sup> Celsius to 44 <sup>0</sup> Celsius. The default threshold is 44 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

## ipmiThempIOH

**TABLE 125** ipmiThempIOH alarm

Alarm	ipmiThempIOH
Alarm Type	ipmiThempIOH
Alarm Code	904
Severity	Major
Aggregation Policy	From the event code 904 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 929.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Chipset temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the chip set temperature status on the control plane increases/decreases. IOH thermal margin threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

## ipmiThempMemP

**TABLE 126** ipmiThempMemP alarm

Alarm	ipmiThempMemP
Alarm Type	ipmiThempMemP
Alarm Code	905
Severity	Major
Aggregation Policy	From the event code 905 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 930.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] memory temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's processor memory shows the status as either an increase/decrease in temperature. Process 1 memory thermal margin threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

## ipmiThempPS

**TABLE 127** ipmiThempPS alarm

Alarm	ipmiThempPS
Alarm Type	ipmiThempPS
Alarm Code	906
Severity	Major
Aggregation Policy	From the event code 906 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 931.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's power supply shows the status as either an increase/decrease in temperature. Power supply 1 and power supply 2 threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Recommended Actions	Replace the power supply cord. If the problem persists, decrease the ambient temperature.

## ipmiThempP

**TABLE 128** ipmiThempP alarm

Alarm	ipmiThempP
Alarm Type	ipmiThempP
Alarm Code	907
Severity	Major
Aggregation Policy	From the event code 907 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 932.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the reading surpasses threshold value is <= 55 <sup>0</sup> Celsius. The default threshold is 55 <sup>0</sup> C.
Recommended Actions	Check and replace the CPU fan module if required. Decrease the ambient temperature if the fan module is working.

## ipmiThempHSBP

**TABLE 129** ipmiThempHSBP alarm

Alarm	ipmiThempHSBP
Alarm Type	ipmiThempHSBP
Alarm Code	908
Severity	Major



**TABLE 129** ipmiThempHSBP alarm (continued)

Alarm	ipmiThempHSBP
Aggregation Policy	From the event code 908 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 933.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Hot swap backplane temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's hot swap backplane shows the status as either an increase/decrease in temperature in the range of 9 <sup>0</sup> Celsius to 55 <sup>0</sup> Celsius. The default threshold is 55 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

## ipmiFan

**TABLE 130** ipmiFan alarm

Alarm	ipmiFan
Alarm Type	ipmiFan
Alarm Code	909
Severity	Major
Aggregation Policy	From the event code 909 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 934.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's fan module status is shown.
Recommended Actions	Replace the fan module.

## ipmiPower

**TABLE 131** ipmiPower alarm

Alarm	ipmiPower
Alarm Type	ipmiPower
Alarm Code	910
Severity	Major
Aggregation Policy	From the event code 910 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 935.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's power supply status is shown as a low/high input.
Recommended Actions	Replace the power supply cord.

## ipmiCurrent

**TABLE 132** ipmiCurrent alarm

Alarm	ipmiCurrent
Alarm Type	ipmiCurrent
Alarm Code	911
Severity	Major
Aggregation Policy	From the event code 911 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 936.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] +12V% of maximum current output [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's power supply shows the status as maximum voltage.
Recommended Actions	Replace the power supply cord. If the problem persists, replace the mother board.

## ipmiFanStatus

**TABLE 133** ipmiFanStatus alarm

Alarm	ipmiFanStatus
Alarm Type	ipmiFanStatus
Alarm Code	912
Severity	Major
Aggregation Policy	From the event code 912 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 937.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's fan module shows the status as not working.
Recommended Actions	Replace the fan module.

## ipmiPsStatus

**TABLE 134** ipmiPsStatus alarm

Alarm	ipmiPsStatus
Alarm Type	ipmiPsStatus
Alarm Code	913
Severity	Major
Aggregation Policy	From the event code 913 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 938.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"

**TABLE 134** ipmiPsStatus alarm (continued)

Alarm	ipmiPsStatus
Displayed on the web interface	Power supply [{id}] [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's power supply status is shown as a low/high input.
Recommended Actions	Check the power supply cord. If the problem persists, replace the power supply cord.

## ipmiDrvStatus

**TABLE 135** ipmiDrvStatus alarm

Alarm	ipmiDrvStatus
Alarm Type	ipmiDrvStatus
Alarm Code	914
Severity	Major
Aggregation Policy	From the event code 914 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 939.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Disk drive [{id}] [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's disk drive status is shown as either not working or corrupted.
Recommended Actions	The operator / user needs to replace the hard disk drive.

## Licensing Alarms

### NOTE

Alarms 1242 and 1243 are not applicable for vSZ-H.

Following are the alarms related to licensing:

- [TTG session critical threshold](#) on page 100
- [TTG session license exhausted](#) on page 100
- [License going to expire](#) on page 100
- [Insufficient license capacity](#) on page 101
- [Data plane DHCP IP license insufficient](#) on page 101
- [Data plane NAT session license insufficient](#) on page 101
- [Insufficient license capacity](#) on page 102

## TTG session critical threshold

**TABLE 136** TTG session critical threshold alarm

Alarm	TTG session critical threshold
Alarm Type	ttgSessionCriticalThreshold
Alarm Code	1242
Severity	Critical
Aggregation Policy	From the event code 1242 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached critical level.
Description	This alarm is triggered when the number of user equipment attached to the system has reached the critical threshold limit.
Recommended Actions	Download the SM log file from the controller web interface to check the error cause.

## TTG session license exhausted

**TABLE 137** TTG session license exhausted alarm

Alarm	TTG session license exhausted
Alarm Type	ttgSessionLicenseExhausted
Alarm Code	1243
Severity	Critical
Aggregation Policy	From the event code 1243 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed of {produce.short.name} [{SCGMgmtIp}] have been exhausted for all sessions.
Description	This alarm is triggered when the number of user equipment attached to the system has exceeded the license limit.
Recommended Actions	Download the SM log file from the controller web interface to check the error cause.

## License going to expire

**TABLE 138** License going to expire alarm

Alarm	License going to expire
Alarm Type	licenseGoingToExpire
Alarm Code	1255
Severity	Major
Aggregation Policy	From the event code 1255 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xxx", "licenseType"=" xxx"
Displayed on the web interface	The [{licenseType}] on node [{nodeName}] will expire on [{associationTime}].
Description	This alarm is triggered when the validity of the license is going to expire.

**TABLE 138** License going to expire alarm (continued)

Alarm	License going to expire
Recommended Actions	Check the validity of licenses. You would need to purchase additional licenses if validity expires.

## Insufficient license capacity

**TABLE 139** Insufficient license capacity alarm

Alarm	Insufficient license capacity
Alarm Type	apConnectionTerminatedDueToInsufficientLicense
Alarm Code	1256
Severity	Major
Aggregation Policy	From the event code 1256 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{{licenseType}}] license is detected and it will cause existing AP connections to terminate.
Description	This alarm is triggered when connected APs are rejected due to insufficient licenses.
Recommended Actions	Check the number of licenses. You would need to purchase additional licenses due to insufficient number of licenses.

## Data plane DHCP IP license insufficient

**TABLE 140** Data plane DHCP IP license insufficient alarm

Alarm	Data plane DHCP IP license insufficient
Alarm Type	dpDhcpIpLicenseNotEnough
Alarm Code	1277
Severity	Major
Aggregation Policy	From the event code 1277 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This alarm occurs when Data Plane DHCP IP license insufficient. ( total [{{totalLicenseCnt}}, consumed [{{consumedLicenseCnt}}, available [{{availableLicenseCnt}}] )
Description	This alarm is triggered when the data plane DHCP IP license is insufficient.

## Data plane NAT session license insufficient

**TABLE 141** Data plane NAT session license insufficient alarm

Alarm	Data plane NAT session license insufficient
Alarm Type	dpNatSessionLicenseNotEnough
Alarm Code	1278

## Alarm Types

### PMIPv6 Alarms

**TABLE 141** Data plane NAT session license insufficient alarm (continued)

Alarm	Data plane NAT session license insufficient
Severity	Major
Aggregation Policy	From the event code 1277 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This alarm occurs when Data Plane NAT session license insufficient. ( total {{totalLicenseCnt}}, consumed {{consumedLicenseCnt}}, available {{availableLicenseCnt}} )
Description	This alarm is triggered when the data plane NAT server license is insufficient.

## Insufficient license capacity

**TABLE 142** Insufficient license capacity alarm

Alarm	Insufficient license capacity
Alarm Type	switchConnectionTerminatedDueToInsufficientLicense
Alarm Code	1289
Severity	Major
Aggregation Policy	From the event code 1289 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient {{licenseType}} license is detected and it will cause existing switch connections to terminate.
Description	This alarm is triggered when some connected switches are rejected due to insufficient license capacity.

## PMIPv6 Alarms

### NOTE

This section is not applicable for vSZ-H.

Following are the alarms related to PMIPv6.

- [Config update failed](#) on page 102
- [DHCP connection lost](#) on page 103

## Config update failed

**TABLE 143** Config update failed alarm

Alarm	Config update failed
Alarm Type	updateCfgFailed
Alarm Code	5004
Severity	Major

**TABLE 143** Config update failed alarm (continued)

Alarm	Config update failed
Aggregation Policy	From the event code 5004 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2", "cause"="reason",
Displayed on the web interface	Failed to apply configuration [{cause}] in PMIPv6 process at {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the PMIPv6 gets an error or a negative acknowledgment or improper/incomplete information from the D-bus client.
Recommended Actions	Check to ensure that the IP address of the CGF server received from PDNGW/GGSN is configured in the controller web interface > Configurations > Services and Profiles > CGF. Configure the IP address if it is missing.

## DHCP connection lost

### NOTE

This alarm is not applicable for vSZ-H.

**TABLE 144** DHCP connection lost alarm

Alarm	DHCP connection lost
Alarm Type	lostCnxnToDHCP
Alarm Code	5102
Severity	Major
Aggregation Policy	From the event code 5102 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 5101.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2",
Displayed on the web interface	PMIPv6 process cannot connect to DHCP server on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the transmission control protocol (TCP) connection is lost or when the control plane fails to complete the configuration procedure.
Recommended Actions	Download the PMIPv6d and dynamic host configuration protocol (DHCP) server logs from the controller to check the error cause.

## SCI Alarms

Following are the alarms related to SCI (Small Cell Insight).

- [Connect to SCI failure](#) on page 104
- [SCI has been disabled](#) on page 104
- [SCI and FTP have been disabled](#) on page 104

## Connect to SCI failure

**TABLE 145** Connect to SCI failure alarm

Alarm	Connect to SCI failure
Alarm Type	connectToSciFailure
Alarm Code	4003
Severity	Major
Aggregation Policy	From the event code 4003 an alarm is raised for every event. A single event triggers a single alarm.
Displayed on the web interface	Try to connect to SCI with all SCI profiles but failure.
Description	This alarm occurs when the controller tries connecting to SCI with its profiles but fails.

## SCI has been disabled

**TABLE 146** SCI has been disabled alarm

Alarm	SCI has been disabled
Alarm Type	disabledSciDueToUpgrade
Alarm Code	4004
Severity	Warning
Aggregation Policy	From the event code 4004 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 4003.
Displayed on the web interface	SCI has been disabled due to SZ upgrade, please reconfigure SCI if needed.
Description	This alarm occurs when SCI is disabled due to the controller upgrade. This could require reconfiguration of SCI.
Recommended Actions	The controller does not support SCI prior to version 2.3. You would need to upgrade SCI to 2.3 or above and reconfigure the required information of SCI on the controller dashboard.

## SCI and FTP have been disabled

**TABLE 147** SCI and FTP have been disabled alarm

Alarm	SCI and FTP have been disabled
Alarm Type	disabledSciAndFtpDueToMutuallyExclusive
Alarm Code	4005
Severity	Warning
Aggregation Policy	From the event code 4005 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 4004.
Displayed on the web interface	SCI and FTP have been disabled. It is recommended to enable SCI instead of FTP
Description	This event occurs when the SCI and FTP are disabled.



## Session Alarms

### NOTE

This section is not applicable for vSZ-H.

Following is the alarm related to session.

- [Binding failed](#) on page 105

## Binding failed

**TABLE 148** Binding failed alarm

Alarm	Binding failed
Alarm Type	bindingFailure
Alarm Code	5010
Severity	Major
Aggregation Policy	From the event code 5010 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 5009.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2", "lmaIp"="1.1.1.1", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "dataBladeIp"="3.3.3.3", "uelpAddr"="5.5.5.5"
Displayed on the web interface	Binding for [{ueMacAddr}] UE binding update failure on {produce.short.name}-D [{dataBladeIp}]. Failure Cause [{cause}].
Description	This alarm is triggered when the mobile node binding fails.
Recommended Actions	No action is required.

## System Alarms

Following are the alarms with the system log severity:

### NOTE

{produce.short.name} refers to the controller.

- [No LS responses](#) on page 106
- [LS authentication failure](#) on page 106
- [{produce.short.name} failed to connect to LS](#) on page 107
- [Syslog server unreachable](#) on page 107
- [CSV export FTP maximum retry](#) on page 108
- [CSV export disk threshold exceeded](#) on page 108
- [CSV export disk max capacity reached](#) on page 108
- [Process restart](#) on page 109
- [Service unavailable](#) on page 109
- [Keepalive failure](#) on page 109

- [Resource unavailable](#) on page 110
- [HIP failed over](#) on page 110
- [Unconfirmed program detection](#) on page 111
- [Diameter initialization error](#) on page 111
- [Diameter peer transport failure](#) on page 112
- [Diameter CER error](#) on page 112
- [Diameter peer add error](#) on page 113
- [Diameter peer remove successful](#) on page 113
- [Diameter realm entry error](#) on page 114
- [Diameter failover to alternate peer](#) on page 114
- [Diameter fail back to peer](#) on page 115
- [Diameter CEA unknown peer](#) on page 115
- [Diameter no common application](#) on page 116
- [Process initiated](#) on page 116
- [PMIPv6 unavailable](#) on page 117
- [Memory allocation failed](#) on page 117
- [The last one data plane is disconnected zone affinity profile alarm](#) on page 117

## No LS responses

**TABLE 149** No LS responses alarm

Alarm	No LS responses
Alarm Type	scgLBSNoResponse
Alarm Code	721
Severity	Major
Aggregation Policy	From the event code 721 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the SmartZone web interface	{produce.short.name} [{SCGMgmtIp}] no response from LS: url={url}, port={port}
Description	This alarm is triggered when the controller does not get a response while connecting to the location based service.
Recommended Actions	Check if location server is working properly.

## LS authentication failure

**TABLE 150** LS authentication failure alarm

Alarm	LS authentication failure
Alarm Type	scgLBSAuthFailed
Alarm Code	722
Severity	Major

**TABLE 150** LS authentication failure alarm (continued)

Alarm	LS authentication failure
Aggregation Policy	From the event code 722 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the SmartZone web interface	{produce.short.name} [{SCGMgmtIp}] authentication failed: url={url}, port={port}
Description	This alarm is triggered due to the authentication failure on connecting to the location based service.
Recommended Actions	Check the location server password.

## {produce.short.name} failed to connect to LS

**TABLE 151** {produce.short.name} failed to connect to LS alarm

Alarm	{produce.short.name} failed to connect to LS
Alarm Type	scgLBSConnectFailed
Alarm Code	724
Severity	Major
Aggregation Policy	From the event code 724 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 723.
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the SmartZone web interface	{produce.short.name} [{SCGMgmtIp}] connection failed to LS: url={url}, port={port}
Description	This alarm is triggered when the controller fails to connect to the location based service.
Recommended Actions	Check the location service configuration. Also check the network connectivity between the controller and location server.

## Syslog server unreachable

**TABLE 152** Syslog server unreachable alarm

Alarm	Syslog server unreachable
Alarm Type	syslogServerUnreachable
Alarm Code	751
Severity	Major
Aggregation Policy	From the event code 751 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 750.
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the SmartZone web interface	Syslog server [{syslogServerAddress}] is unreachable on {produce.short.name}.
Description	This alarm is triggered when the syslog server is unreachable.
Recommended Actions	Check the network between the controller and the syslog server.

## CSV export FTP maximum retry

**TABLE 153** CSV export FTP maximum retry alarm

Alarm	CSV export FTP maximum retry
Alarm Type	csvFtpTransferMaxRetryReached
Alarm Code	974
Severity	Major
Aggregation Policy	From the event code 974 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 750.
Attribute	"nodeName"="xx:xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx:xx", "portID"="xx:xx:xx:xx:xx:xx", "filename"="xxx.xxx.xxx.xxx"
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV file fails to transfer after a maximum of five (5) retries.

## CSV export disk threshold exceeded

**TABLE 154** CSV export disk threshold exceeded alarm

Alarm	CSV export disk threshold exceeded
Alarm Type	csvDiskThresholdExceeded
Alarm Code	975
Severity	Warning
Aggregation Policy	From the event code 975 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xx:xx:xx:xx:xx:xx", "threshold"="xx:xx:xx:xx:xx:xx", "availableDiskSize"="xx:xx:xx:xx:xx:xx"
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV report size exceeds 80% of its capacity.
Recommended Actions	

## CSV export disk max capacity reached

**TABLE 155** CSV export disk max capacity reached alarm

Alarm	CSV export disk max capacity reached
Alarm Type	csvDiskMaxCapacityReached
Alarm Code	976
Severity	Critical
Aggregation Policy	From the event code 976 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xx:xx:xx:xx:xx:xx", "allocatedDiskSize"="xx:xx:xx:xx:xx:xx"
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV report size reaches its maximum capacity.

**TABLE 155** CSV export disk max capacity reached alarm (continued)

Alarm	CSV export disk max capacity reached
Recommended Actions	

## Process restart

**TABLE 156** Process restart alarm

Alarm	Process restart
Alarm Type	processRestart
Alarm Code	1001
Severity	Major
Aggregation Policy	From the event code 1001 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA", "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{processName}} process got re-started on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when any process crashes and restarts.
Recommended Actions	Download the process log file from the controller web interface to understand the cause of the error.

## Service unavailable

**TABLE 157** Service unavailable alarm

Alarm	Service unavailable
Alarm Type	serviceUnavailable
Alarm Code	1002
Severity	Critical
Aggregation Policy	From the event code 1002 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA", "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{processName}} process is not stable on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the process repeatedly restarts and is unstable.
Recommended Actions	A manual intervention is required. Download the process log file from the controller web interface to find the cause of the error.

## Keepalive failure

**TABLE 158** Keepalive failure alarm

Alarm	Keepalive failure
Alarm Type	keepAliveFailure
Alarm Code	1003

**TABLE 158** Keepalive failure alarm (continued)

Alarm	Keepalive failure
Severity	Major
Aggregation Policy	From the event code 1003 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA", "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} on {produce.short.name} {{SCGMgmtIp}} restarted {{processName}} process
Description	This alarm is triggered when the <b>mon/nc</b> restarts the process due to a keep alive failure.
Recommended Actions	Download the process log file from the controller web interface to locate the cause of the error.

## Resource unavailable

**TABLE 159** Resource unavailable alarm

Alarm	Resource unavailable
Alarm Type	resourceUnavailable
Alarm Code	1006
Severity	Critical
Aggregation Policy	From the event code 1006 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd", "realm"="NA", "SCGMgmtIp"="3.3.3.3", "cause"="xx"
Displayed on the web interface	System resource {{cause}} not available in {{srcProcess}} process at {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is generated due to unavailability of any other system resource, such as memcached.
Recommended Actions	A manual intervention is required. Check the memcached process. Also check if the <b>br1</b> interface is running.

## HIP failed over

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 160** HIP failed over alarm

Alarm	HIP failed over
Alarm Type	hipFailover
Alarm Code	1016
Severity	Major
Aggregation Policy	Alarm is raised for every event from event code 1016. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"

**TABLE 160** HIP failed over alarm (continued)

Alarm	HIP failed over
Displayed on the web interface	{{srcProcess}} Node transitioned to Active on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the standby host identity protocol (HIP) transits to an active node and is included in control plane identifier of the newly active HIP.
Recommended Actions	A manual intervention is required.

## Unconfirmed program detection

**TABLE 161** Unconfirmed program detection alarm

Alarm	Unconfirmed program detection
Alarm Type	Unconfirmed Program Detection
Alarm Code	1019
Severity	Warning
Aggregation Policy	Alarm is raised for every event from event code 1019. A single event triggers a single alarm.
Attribute	"nodeName"="xxx", "status"="xxxxx"
Displayed on the web interface	Detect unconfirmed program on control plane [{nodeName}]. [{status}]
Description	This alarm is triggered when the controller detects an unconfirmed program on the control plane.

## Diameter initialization error

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 162** Diameter initialization error alarm

Alarm	Diameter initialization error
Alarm Type	dialnitalizeErr
Alarm Code	1401
Severity	Critical
Aggregation Policy	An alarm is raised for every 2events within a duration of 30 minutes.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "desc" = "Diameter Stack Initialization Failure on {produce.short.name}"
Displayed on the web interface	{{srcProcess}} Diameter Stack Initialization Failure on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered due to stack initialization failure.
Recommended Actions	Check the network interface settings and port settings. The port could be in use by another application.

## Diameter peer transport failure

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 163** Diameter peer transport failure alarm

Alarm	Diameter peer transport failure
Alarm Type	diaPeerTransportFailure
Alarm Code	1403
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerIp" = "3.3.3.3" "peerName" = "OCS1" "peerRealmName" = "organization.com" "desc" = "Failed to read from peer socket"
Displayed on the web interface	{{srcProcess}} Failed to read from peer {{peerName}} Transport Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the diameter stack fails to read from the peer socket and the peer transport is down.
Recommended Actions	Check if the transport is up for the peer. Peer application may not be running.

## Diameter CER error

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 164** Diameter CER error alarm

Alarm	Diameter CER error
Alarm Type	diaCERError
Alarm Code	1404
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerIp" = "3.3.3.3" "peerName" = "OCS1" "peerRealmName" = "organization.com" "desc" = "Failed to read from peer socket"
Displayed on the web interface	{{srcProcess}} Failed to decode CER from Peer {{peerName}} Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the diameter stack fails to decode the capabilities exchange request (CER) received from peer.
Recommended Actions	Check if the transport is up for the peer. Peer application may not be running.



## Diameter peer add error

### NOTE

This alarm is not applicable for vSZ-H.

**TABLE 165** Diameter peer add error alarm

Alarm	Diameter peer add error
Alarm Type	diaPeerAddError
Alarm Code	1407
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerIp" = "3.3.3.3" "peerName" = "OCS1" "peerRealmName" = "organization.com" "desc" = "Failed to add Peer" "cause"="Cause Value"
Displayed on the web interface	{{srcProcess}} Failed to add Peer {{peerName}}, Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the diameter stack fails to add a peer to the peer table.
Recommended Actions	Check if the peer IP address is reachable and if the peer responds to the configured port.

## Diameter peer remove successful

### NOTE

This alarm is not applicable for vSZ-H.

**TABLE 166** Diameter peer remove successful alarm

Alarm	Diameter peer remove successful
Alarm Type	diaPeerRemoveSuccess
Alarm Code	1409
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerIp" = "3.3.3.3" "peerName" = "OCS1" "peerRealmName" = "organization.com" "desc" = "Peer removal success"
Displayed on the web interface	{{srcProcess}} Peer {{peerName}} Realm {{peerRealmName}} removal is successful on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the peer is removed successfully from the table. The remote peer sends a diameter disconnect peer request (DPR) with the cause of not wanting to talk.
Recommended Actions	Ensure that the peer removal is intentional. It is also removed when the peer sends a cause message.

## Diameter realm entry error

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 167** Diameter realm entry error alarm

Alarm	Diameter realm entry error
Alarm Type	diaRealmEntryErr
Alarm Code	1410
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerRealmName" = "organization.com" "peerName" = "OCS1" "desc" = "Failed to add route for Realm"
Displayed on the web interface	{{srcProcess}} Failed to add route for Realm {{peerRealmName}} on {{produce.short.name}} {{SCGMgmtIp}}
Description	This alarm is triggered due to realm route entry add error. This may arise when the realm entry exists and another realm entry is added. Creating two diameter services with same realm name causes this problem.
Recommended Actions	Ensure that peer supports the application for the given realm and is up and running.

## Diameter failover to alternate peer

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 168** Diameter failover to alternate peer alarm

Alarm	Diameter failover to alternate peer
Alarm Type	diaFailOverToAltPeer
Alarm Code	1411
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"="OCS1" "peerRealmName" = "organization.com" "altPeerName" = "OCS2" "altPeerRealmName" = "india.internal.net" "desc" = "Fwd to alt peer"
Displayed on the web interface	{{srcProcess}} Fwd from Peer {{peerName}} to AltPeer {{altPeerName}} Realm {{peerRealmName}} on {{produce.short.name}} {{SCGMgmtIp}}
Description	This alarm is triggered due to retransmission to an alternate peer.
Recommended Actions	Verify that the failover has occurred to the alternate peer and the request is processed by the same peer. Also verify if the primary peer is having a problem or is not reachable.

## Diameter fail back to peer

### NOTE

This alarm is not applicable for vSZ-H.

**TABLE 169** Diameter fail back to peer alarm

Alarm	Diameter fail back to peer
Alarm Type	diaFailbackToPeer
Alarm Code	1412
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"="ÖCS1 "peerRealmName" = "organization.com" "altPeerName" = "OCS2" "altPeerRealmName" = "india.internal.net" "desc" = "Failback to main peer"
Displayed on the web interface	{{srcProcess}} Failback to Main Peer {{peerName}} Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered due to retransmission to the main peer in case of a failover.
Recommended Actions	Verify that the primary peer is restored and the request is processed by the primary peer.

## Diameter CEA unknown peer

### NOTE

This alarm is not applicable for vSZ-H.

**TABLE 170** Diameter CEA unknown peer alarm

Alarm	Diameter CEA unknown peer
Alarm Type	diaCEAUnknownPeer
Alarm Code	1414
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="SessMgr" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"="ÖCS8 "peerRealmName" = "organization.com" "desc" = "CEA received from Unknown peer"
Displayed on the web interface	{{srcProcess}} CEA received from Unknown Peer {{peerName}} Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the capabilities exchange answer (CEA) is received from an unknown peer.
Recommended Actions	Verify that the origin host received from capabilities exchange answer (CEA) is not in the remote service configuration.

## Diameter no common application

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 171** Diameter no common application alarm

Alarm	Diameter no common application
Alarm Type	diaNoCommonApp
Alarm Code	1415
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"=ÖCS1 "peerRealmName" = "organization.com""desc" = "No common App with peer"
Displayed on the web interface	{{srcProcess}} No common App with Peer {{peerName}} Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the common application is not with the peer.
Recommended Actions	Verify that the peer is in the remote service configuration and is sending the capability negotiation message that the authentication application identifier is not compliant to the remote service.

## Process initiated

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 172** Process initiated alarm

Alarm	Process initiated
Alarm Type	processInit
Alarm Code	5001
Severity	Major
Aggregation Policy	From the event code 5001 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process got re-started on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when PMIPv6 process restarts.
Recommended Actions	A manual intervention is required. Download the PMIPv6d log file from the controller to check the cause of error.

## PMIPv6 unavailable

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 173** PMIPv6 unavailable alarm

Alarm	PMIPv6 unavailable
Alarm Type	pmipUnavailable
Alarm Code	5002
Severity	Critical
Aggregation Policy	From the event code 5002 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process is not stable on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the PMIPv6 process repeatedly restarts and is not stable.
Recommended Actions	Check the PMIPv6d application log and status from the controller web interface.

## Memory allocation failed

**NOTE**

This alarm is not applicable for vSZ-H.

**TABLE 174** Memory allocation failed alarm

Alarm	Memory allocation failed
Alarm Type	unallocatedMemory
Alarm Code	5003
Severity	Critical
Aggregation Policy	From the event code 5003 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Insufficient Heap Memory in PMIPv6 process at {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the memory allocation fails in the PMIPv6 process.
Recommended Actions	Check the PMIPv6d application log and status from the controller web interface.

## The last one data plane is disconnected zone affinity profile alarm

**TABLE 175** The last one data plane is disconnected zone affinity profile alarm

Alarm	The last one data plane is disconnected zone affinity profile
Alarm Type	zoneAffinityLastDpDisconnected
Alarm Code	1267
Severity	Informational
Aggregation Policy	From the event code 1267 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpName="xxxxxxx", "dpKey"="xx:xx:xx:xx:xx:xx", "zoneAffinityProfileId"="xxxxxxx"

## Alarm Types

Switch

**TABLE 175** The last one data plane is disconnected zone affinity profile alarm (continued)

Alarm	The last one data plane is disconnected zone affinity profile
Displayed on the web interface	The Last one Data Plane{{dpName&&dpKey}} is disconnected Zone Affinity profile{{zoneAffinityProfileId}}.
Description	This alarm is triggered when the last data plane disconnects from the zone affinity.

## Switch

Following are the alarms related to switch severity:

- [Power supply failure](#) on page 118
- [Fan failure](#) on page 119
- [Module insertion](#) on page 119
- [Module removal](#) on page 119
- [Temperature above threshold warning](#) on page 120
- [Stack member unit failure](#) on page 120
- [PoE power allocation failure](#) on page 121
- [DHCP\\_Snooping: DHCP offer dropped message](#) on page 121
- [Port put into error disable state](#) on page 121
- [Switch offline](#) on page 122
- [Switch duplicated](#) on page 122
- [Reject certificate signing request](#) on page 122
- [Pending certificate signing request](#) on page 123
- [Switch CPU major threshold exceed](#) on page 123
- [Switch CPU critical threshold exceed](#) on page 123
- [Switch memory major threshold exceed](#) on page 124
- [Switch memory critical threshold exceed](#) on page 124
- [Switch custom major threshold exceed](#) on page 124
- [Switch custom critical threshold exceed](#) on page 125
- [Switch Firmware Upgrade Failed](#) on page 125
- [Switch Configuration Update Failed](#) on page 125

## Power supply failure

**TABLE 176** Power supply failure alarm

Alarm	Power supply failure
Alarm Type	PowerSupplyfailure
Alarm Code	20000
Severity	Critical
Aggregation Policy	From the event code 20000, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"

**TABLE 176** Power supply failure alarm (continued)

Alarm	Power supply failure
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: System: Stack unit 3 Power supply 2 is not present
Description	This alarm is triggered when there is power supply failure.
Recommended Actions	Check the status of Switch power supply.

## Fan failure

**TABLE 177** Fan failure alarm

Alarm	Fan failure
Alarm Type	FanFailure
Alarm Code	20001
Severity	Critical
Aggregation Policy	From the event code 20001, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: System: Stack unit unit# Fan fan# ( description ), failed
Description	This alarm is triggered when there is fan failure.
Recommended Actions	Check the status of Switch fan.

## Module insertion

**TABLE 178** Module insertion alarm

Alarm	Module insertion
Alarm Type	ModuleInsertion
Alarm Code	20002
Severity	Critical
Aggregation Policy	From the event code 20002, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: System: Module inserted to slot %d in unit %d
Description	This alarm is triggered when the module is inserted into the slot.
Recommended Actions	Check slot module.

## Module removal

**TABLE 179** Module removal alarm

Alarm	Module removal
Alarm Type	ModuleRemoval
Alarm Code	20003
Severity	Critical

## Alarm Types

### Switch

**TABLE 179** Module removal alarm (continued)

Alarm	Module removal
Aggregation Policy	From the event code 20003, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: System: Module removed from slot %d in unit %d
Description	This alarm is triggered when the module is removed from the slot.
Recommended Actions	Check slot module.

## Temperature above threshold warning

**TABLE 180** Temperature above threshold warning alarm

Alarm	Temperature above threshold warning
Alarm Type	TemperatureAboveThresholdWarning
Alarm Code	20004
Severity	Critical
Aggregation Policy	From the event code 20004, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: Temperature is over warning level.
Description	This alarm is triggered when the temperature is above the warning level.
Recommended Actions	Check the status of Switch unit.

## Stack member unit failure

**TABLE 181** Stack member unit failure alarm

Alarm	Stack member unit failure
Alarm Type	StackMemberUnitFailure
Alarm Code	20005
Severity	Critical
Aggregation Policy	From the event code 20005, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: Stack: Stack unit # has been deleted from the stack system
Description	This alarm is triggered when the stack unit is deleted from the stack system.
Recommended Actions	Check Stack status.



## PoE power allocation failure

**TABLE 182** PoE power allocation failure alarm

Alarm	PoE power allocation failure
Alarm Type	PoePowerAllocationFailure
Alarm Code	20006
Severity	Critical
Aggregation Policy	From the event code 20006, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: PoE: Failed power allocation of %d mwatts on port %p. Will retry when more power budget
Description	This alarm is triggered when there is POE power allocation failure.
Recommended Actions	Check PoE power status.

## DHCP\_Snooping: DHCP offer dropped message

**TABLE 183** DHCP\_Snooping: DHCP offer dropped message alarm

Alarm	DHCP_Snooping: DHCP offer dropped message
Alarm Type	DhcpOfferDroppedMessage
Alarm Code	20007
Severity	Critical
Aggregation Policy	From the event code 20007, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: DHCP_Snooping: DHCP offer dropped message
Description	This alarm is triggered when there is DHCP Snooping.
Recommended Actions	Check network environment and DHCP status.

## Port put into error disable state

**TABLE 184** Port put into error disable state alarm

Alarm	Port put into error disable state
Alarm Type	PortPutIntoErrorDisableState
Alarm Code	20008
Severity	Critical
Aggregation Policy	From the event code 20008, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} {switchMsg} EX: ERR_DISABLE: Link flaps on port %s %p exceeded threshold; port in err-disable state
Description	This alarm is triggered when the port is in error-disable state.
Recommended Actions	Check port status.

## Alarm Types

Switch

### Switch offline

**TABLE 185** Switch offline alarm

Alarm	Switch offline
Alarm Type	SwitchOffline
Alarm Code	21000
Severity	Warning
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} offline for more than 15 minutes
Description	This alarm is triggered when the switch is offline.
Recommended Actions	Check Switch unit status.

### Switch duplicated

**TABLE 186** Switch duplicated alarm

Alarm	Switch duplicated
Alarm Type	SwitchDuplicated
Alarm Code	21002
Severity	Warning
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMac"="aa:bb:cc:dd:ee:ff", "duplicatedSwitchSerialNumber"="x", "duplicatedSwitchName"="x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} A duplicated switch mac address from {{duplicatedSwitchSerialNumber}/{{duplicatedSwitchName}} is coming while existing one {{switchMac}} is online.
Description	This alarm is triggered when the switch is duplicated.
Recommended Actions	Check the duplicated switches.

### Reject certificate signing request

**TABLE 187** Reject certificate signing request alarm

Alarm	Reject certificate signing request
Alarm Type	rejectCertificateSigningRequest
Alarm Code	22003
Severity	Major
Aggregation Policy	From the event code 22003, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Reject Certificate Signing Request.
Description	This alarm is triggered when there is a SCEP Reject certificate signing request.
Recommended Actions	Check if the switches are under the trust list.

## Pending certificate signing request

**TABLE 188** Pending certificate signing request alarm

Alarm	Pending certificate signing request
Alarm Type	pendingCertificateSigningRequest
Alarm Code	22004
Severity	Major
Aggregation Policy	From the event code 22004, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x"
Displayed on the web interface	[SCEP – {switchSerialNumber}] Pending Certificate Signing Request.
Description	This alarm is triggered when there is a SCEP Pending certificate signing request.

## Switch CPU major threshold exceed

**TABLE 189** Switch CPU major threshold exceed alarm

Alarm	Switch CPU major threshold exceed
Alarm Type	majorCpuThresholdExceed
Alarm Code	22011
Severity	Major
Aggregation Policy	From the event code 22011 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU major threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This alarm is triggered when the CPU usage exceeds the major threshold limit, which is based on the utilization rate.

## Switch CPU critical threshold exceed

**TABLE 190** Switch CPU critical threshold exceed alarm

Alarm	Switch CPU critical threshold exceed
Alarm Type	criticalCpuThresholdExceed
Alarm Code	22012
Severity	Critical
Aggregation Policy	From the event code 22012 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Major Threshold - 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU critical threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This alarm is triggered when the CPU usage exceeds the critical threshold limit, which is based on the utilization rate.

## Switch memory major threshold exceed

**TABLE 191** Switch memory major threshold exceed alarm

Alarm	Switch memory major threshold exceed
Alarm Type	majorMemoryThresholdExceed
Alarm Code	22021
Severity	Major
Aggregation Policy	From the event code 22021 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This alarm is triggered when the memory capacity exceeds the major threshold limit, which is based on the utilization rate.

## Switch memory critical threshold exceed

**TABLE 192** Switch memory critical threshold exceed alarm

Alarm	Switch memory critical threshold exceed
Alarm Type	criticalMemoryThresholdExceed
Alarm Code	22022
Severity	Critical
Aggregation Policy	From the event code 22021 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Major Threshold - 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory critical threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This alarm is triggered when the memory usage exceeds the critical threshold limit, which is based on the utilization rate.

## Switch custom major threshold exceed

**TABLE 193** Switch custom major threshold exceed alarm

Alarm	Switch custom major threshold exceed
Alarm Type	hitMajorSwitchCombinedEvent
Alarm Code	22031
Severity	Major
Aggregation Policy	From the event code 22031 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Major Event] {userDefinedDescription}
Description	This alarm is triggered when the switch custom crosses the threshold limit.

## Switch custom critical threshold exceed

**TABLE 194** Switch custom critical threshold exceed alarm

Alarm	Switch custom critical threshold exceed
Alarm Type	hitCriticalSwitchCombinedEvent
Alarm Code	22032
Severity	Critical
Aggregation Policy	From the event code 22032 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Critical Event] {userDefinedDescription}
Description	This alarm is triggered when the switch custom crosses the critical threshold limit.

## Switch Firmware Upgrade Failed

**TABLE 195** Switch Firmware Upgrade Failed alarm

Alarm	Switch Firmware Upgrade Failed
Alarm Type	SwitchFirmwareUpgradeFailed
Alarm Code	22042
Severity	Critical
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} switch firmware upgrade failed
Description	This Alarm occurs when the switch firmware upgrade is failed.

## Switch Configuration Update Failed

**TABLE 196** Switch Configuration Update Failed alarm

Alarm	Switch Configuration Update Failed
Alarm Type	SwitchConfigurationUpdateFailed
Alarm Code	22052
Severity	Critical
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} switch configuration update failed
Description	This alarm occurs when the switch configuration update is failed.

## Threshold Alarms

Following are the alarms related to threshold system set:

- [CPU threshold exceeded](#) on page 126
- [Memory threshold exceeded](#) on page 126

## Alarm Types

### Threshold Alarms

- [Disk usage threshold exceeded](#) on page 127
- [The drop of client count threshold exceeded](#) on page 127
- [License threshold exceeded](#) on page 128
- [Rate limit for TOR surpassed](#) on page 128
- [The number of users exceeded its limit](#) on page 129
- [The number of devices exceeded its limit](#) on page 129
- [Over AP maximum capacity](#) on page 130
- [Over Device maximum capacity](#) on page 130

## CPU threshold exceeded

**TABLE 197** CPU threshold exceeded alarm

Alarm	CPU threshold exceeded
Alarm Type	cpuThresholdExceeded
Alarm Code	950
Severity	Critical
Aggregation Policy	From the event code 950 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 953.
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	CPU threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the CPU usage exceeds the threshold limit. The CPU threshold value is 80%.
Recommended Actions	<p>Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to RUCKUS support.</p> <p>Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.</p>

## Memory threshold exceeded

**TABLE 198** Memory threshold exceeded alarm

Alarm	Memory threshold exceeded
Alarm Type	memoryThresholdExceeded
Alarm Code	951
Severity	Critical
Aggregation Policy	From the event code 951 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 954.
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].

**TABLE 198** Memory threshold exceeded alarm (continued)

Alarm	Memory threshold exceeded
Description	This alarm is triggered when the memory usage exceeds the threshold limit. The memory threshold value is 85% for SCG and 90% for vSZ-H.
Recommended Actions	<p>Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to RUCKUS support.</p> <p>Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.</p>

## Disk usage threshold exceeded

**TABLE 199** Disk usage threshold exceeded alarm

Alarm	Disk usage threshold exceeded
Alarm Type	diskUsageThresholdExceeded
Alarm Code	952
Severity	Critical
Aggregation Policy	From the event code 952 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 955.
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk usage threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the disk usage exceeds the threshold limit. The disk threshold value is 80%.
Recommended Actions	Check the backup files for disk usage. Each backup file may occupy a large disk space based on the database size. If there are multiple backup files/versions in the controller, it is recommended to delete the older backup files to free disk usage. If the problem persists, please take a screen shot and send it to RUCKUS support.

## The drop of client count threshold exceeded

**TABLE 200** The drop of client count threshold exceeded alarm

Alarm	The drop of client count threshold exceeded
Alarm Type	clientCountDropThresholdExceeded
Alarm Code	956
Severity	Major
Aggregation Policy	From the event code 956 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"perc"="XX"
Displayed on the web interface	The drop of client count exceeded threshold [{perc}%] in cluster.
Description	This alarm is triggered when client count drop exceeds the threshold limit.

## License threshold exceeded

**TABLE 201** License threshold exceeded alarm

Alarm	License threshold exceeded
Alarm Type	licenseThresholdExceeded
Alarm Code	960
Severity	Critical 90% Major 80%
Aggregation Policy	From the event code 960 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"perc"="xxx", "nodeMac"="xx:xx:xx:xx:xx", "nodeName"="box1", "licenseType"="SG00"
Displayed on the web interface	{{licenseType}} limit reached at {{perc}}%.
Description	This alarm is triggered when maximum number of licenses is utilized.
Recommended Actions	Check the license purchase and usage numbers. Alternatively, you would need to buy new licenses.

## HDD Health Degradation

**NOTE**

This alarm is supported on the SmartZone 100 controllers only. This alarm is not applicable for vSZ-E.

**TABLE 202** HDD Health Degradation Alarm

Alarm	HDD health degradation
Alarm Type	HDDHealthDegradation
Alarm Code	961
Severity	Critical
Aggregation Policy	From the event code 961 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="XXX", "status"="xxxxx"
Displayed on the web interface	Hard drive detects health degradation {{status}} on control plane {{nodeName}}, please backup the system to prevent losing the data on disk
Description	This alarm is triggered when the hard drive detects a health degradation on the control plane.

## Rate limit for TOR surpassed

**TABLE 203** Rate limit for TOR surpassed alarm

Alarm	Rate limit for TOR surpassed
Alarm Type	rateLimitTORSurpassed
Alarm Code	1302
Severity	Critical
Aggregation Policy	From the event code 1302 an alarm is raised for every event. A single event triggers a single alarm.



**TABLE 203** Rate limit for TOR surpassed alarm (continued)

Alarm	Rate limit for TOR surpassed
Auto Clearance	The alarm code is auto cleared with the event code 1301.
Attributef	"mvnold"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radius",  "UserName"="abc@xyz.com, "realm"="wlan.3gppnetwor"  "SCGMgmtIp"="2.2.2.2", "aaaSvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct", "ueMacAddr"="aa:bb:cc:gg:hh:ii"  "MOR"=1000, "THRESHOLD"="500", "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This alarm is triggered when maximum outstanding requests (MOR) is surpassed.
Recommended Actions	Download the SM log file from the controller web interface to check the error cause.

## The number of users exceeded its limit

**TABLE 204** The number of users exceeded its limit

Alarm	The number of users exceeded its limit
Alarm Type	tooManyUsers
Alarm Code	7003
Severity	Major
Aggregation Policy	From the event code 7001 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	No attributes for this alarm.
Displayed on the web interface	The number of users exceed the specified limit.
Description	This alarm is triggered when the number of users exceeds the specified limit.
Recommended Actions	No action is required.

## The number of devices exceeded its limit

**TABLE 205** The number of devices exceeded its limit alarm

Alarm	The number of devices exceeded its limit
Alarm Type	tooManyDevices
Alarm Code	7004
Severity	Major
Aggregation Policy	From the event code 7002 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	No attributes for this alarm.
Displayed on the web interface	The number of devices exceeded the limit.
Description	This alarm is triggered the number of devices exceeds the specified limit.
Recommended Actions	No action is required.

## Alarm Types

### Tunnel Alarms - Access Point

## Over AP maximum capacity

**TABLE 206** Over AP maximum capacity alarm

Alarm	Over AP maximum capacity
Alarm Type	apCapacityReached
Alarm Code	962
Severity	Warning
Aggregation Policy	From the event code 962, an alarm is raised for every event. A single event triggers a single alarm.
Displayed on the web interface	The volume of AP is over system capacity.
Description	This alarm is triggered when the volume of AP is over system capacity.

## Over Device maximum capacity

**TABLE 207** Over Device maximum capacity alarm

Alarm	Over Device maximum capacity
Alarm Type	connectedDeviceMaxCapacityReached
Alarm Code	963
Severity	Warning
Aggregation Policy	Alarm is raised for every event from event code 960. Alarm:Event => 1:1
Displayed on the web interface	The volume of {{deviceType}} is over maximum device capacity.
Description	This alarm is triggered when the volume is over maximum device capacity.

## Tunnel Alarms - Access Point

Following are the alarms related to tunnel.

- [AP softGRE gateway not reachable](#) on page 130
- [AP is disconnected from secure gateway](#) on page 131
- [AP secure gateway association failure](#) on page 131

## AP softGRE gateway not reachable

**TABLE 208** AP softGRE gateway not reachable alarm

Alarm	AP softGRE gateway not reachable
Alarm Type	apSoftGREGatewayNotReachable
Alarm Code	614
Severity	Critical
Aggregation Policy	From the event code 614 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 613.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softGREGatewayList"="xxx.xxx.xxx.xxx"

**TABLE 208** AP softGRE gateway not reachable alarm (continued)

Alarm	AP softGRE gateway not reachable
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}]
Description	This alarm is triggered when the AP fails to connect to the Soft-GRE gateway.
Recommended Actions	Check the primary and secondary soft-GRE gateway.

## AP is disconnected from secure gateway

**TABLE 209** AP is disconnected from secure gateway alarm

Alarm	AP is disconnected from secure gateway
Alarm Type	ipsecTunnelDisassociated
Alarm Code	661
Severity	Major
Aggregation Policy	From the event code 661 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	apMac="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is disconnected from secure gateway [{ipsecGWAddress}].
Description	This alarm is triggered when the AP is disconnected from secure gateway.
Recommended Actions	No action required.

## AP secure gateway association failure

**TABLE 210** AP secure gateway association failure alarm

Alarm	AP secure gateway association failure
Alarm Type	ipsecTunnelAssociateFailed
Alarm Code	662
Severity	Major
Aggregation Policy	From the event code 662 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 660
Attribute	apMac="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is unable to establish secure gateway with [{ipsecGWAddress}]
Description	This alarm is triggered when the AP is unable to connect to the secure gateway.
Recommended Actions	No action required.



# Events Types

---

• 3rd Party Access Point Events.....	133
• Accounting Events.....	134
• AP Authentication Events.....	139
• AP Communication Events.....	146
• AP LBS Events.....	160
• AP Mesh Events.....	163
• AP State Change Events.....	170
• AP USB Events.....	191
• Authentication Events.....	192
• Authorization Events.....	200
• Control and Data Plane Interface.....	203
• Client Events.....	206
• Cloud Events.....	223
• Cluster Events.....	226
• Configuration Events.....	251
• Datablade Events.....	256
• Data Plane Events.....	263
• Data Streaming Event.....	281
• DHCP Events.....	282
• GA Interface Events.....	283
• Gn/S2a Interface Events.....	285
• Gr Interface Event.....	296
• IPMI Events.....	303
• Licensing Interface Events.....	312
• Location Delivery Events.....	318
• PMIPv6 Events.....	319
• Session Events.....	321
• STA Interface Events.....	324
• System Events.....	326
• Switch Events.....	351
• Threshold Events.....	360
• Tunnel Events - Access Point (AP).....	366
• Tunnel Events - Data Plane.....	370
• AP Ethernet Phy Error Count.....	375
• AP Ethernet PHY Down Shift.....	375

## 3rd Party Access Point Events

### NOTE

This event is not applicable for vSZ-H.

Following event is related to 3rd party access points.

- [3rd party AP connected](#) on page 134

## 3rd party AP connected

**TABLE 211** 3rdparty AP connected event

Event	3rd party AP connected
Event Type	3rdPartyAPConnected
Event Code	1801
Severity	Debug
Attribute	"mvnold"=12,"zoneId"=10 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"=2.2.2.2 "apMac"="aa:bb:cc:dd:ee:aa" "apIpAddress"=10.1.4.11 " "srcProcess"=radius
Displayed on the web interface	3rd Party AP with Ip {{apIpAddress}} and MAC {{apMac}} is connected to Control plane {{ctrlBladeMac}} in zone {{zoneName}}
Description	This event occurs when a non-Ruckus AP connects to the controller.

## Accounting Events

**NOTE**

This event is not applicable for vSZ-H.

Following events are related to accounting.

- [Accounting session disabled](#) on page 134
- [Accounting server not reachable](#) on page 135
- [Accounting failed over to secondary](#) on page 135
- [Accounting fallback to primary](#) on page 136
- [AP accounting message mandatory parameter missing](#) on page 136
- [Unknown realm](#) on page 136
- [AP accounting message decode failed](#) on page 137
- [AP accounting retransmission message dropped](#) on page 137
- [AP accounting response while invalid config](#) on page 138
- [AP account message drop while no accounting start message](#) on page 138
- [Unauthorized COA/DM message dropped](#) on page 138

## Accounting session disabled

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 212** Accounting session disabled event

Event	Accounting session disabled
Event Type	accSessDisabled
Event Code	1234
Severity	Debug

**TABLE 212** Accounting session disabled event (continued)

Event	Accounting session disabled
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	Accounting session disabled for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the accounting is disabled for the session.

## Accounting server not reachable

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 213** Accounting server not reachable event

Event	Accounting server not reachable
Event Type	accSrvrNotReachable
Event Code	1602
Severity	Major
Attribute	"mvnoid"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd", "realm"="wlan.3gppnetwork.org", "radProxyIp"="7.7.7.7", "accSrvrIp"="30.30.30.30", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the controller is unable to connect to either the primary or secondary accounting server.

## Accounting failed over to secondary

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 214** Accounting failed over to secondary event

Event	Accounting failed over to secondary
Event Type	accFailedOverToSecondary
Event Code	1653
Severity	Major
Attribute	"mvnoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the secondary accounting RADIUS server is available after the primary server becomes zombie or dead.

## Accounting fallback to primary

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 215** Accounting fallback to primary event

Event	Accounting fallback to primary
Event Type	accFallbackToPrimary
Event Code	1654
Severity	Major
Attribute	"mvnold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the automatic fallback is enabled. The accounting failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.

## AP accounting message mandatory parameter missing

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 216** AP accounting message mandatory parameter missing event

Event	AP accounting message mandatory parameter missing
Event Type	apAcctMsgMandatoryPrmMissing
Event Code	1901
Severity	Critical
Attribute	"mvnold"="12","wlanId"="1","zoneId"="10","ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut","userName" = "hello@world.com" ,"SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueMsisdn"="98787","apIpAddress"="10.1.4.11"
Displayed on the web interface	[[srcProcess]] Mandatory attribute missing in Accounting Packet received from AP [[apIpAddress]] on {produce.short.name} [{SCGMgmtIp}], with username [[userName]]
Description	This event occurs when the controller fails to find the mandatory parameter in the RADIUS accounting message received from the AP. This is a mandatory parameter for generating the W-AN-CDR.

## Unknown realm

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 217** Unknown realm event

Event	Unknown realm
Event Type	unknownRealmAccounting



**TABLE 217** Unknown realm event (continued)

Event	Unknown realm
Event Code	1902
Severity	Debug
Attribute	"mvnold"="12","wlanId"="1","zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "userName"="acb@xyz.com", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii","ueMsisdn"="98787", "apIpAddress"="10.1.4.11"
Displayed on the web interface	{{srcProcess}} Failed to find realm for Accounting Packet received from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}}, with username {{userName}}
Description	This event occurs when the controller fails to find realm configuration for the accounting messages received from the AP.

## AP accounting message decode failed

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 218** AP accounting message decode failed event

Event	AP accounting message decode failed
Event Type	apAcctMsgDecodeFailed
Event Code	1904
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "SCGMgmtIp"="2.2.2.2", "apIpAddress"="10.1.4.11"
Displayed on the web interface	{{srcProcess}} Malformed Accounting Packet received from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}}, with username {{userName}}
Description	This event occurs when the AP accounting message decode fails due to receipt of a malformed packet.

## AP accounting retransmission message dropped

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 219** AP accounting retransmission message dropped event

Event	AP accounting retransmission message dropped
Event Type	apAcctRetransmittedMsgDropped
Event Code	1908
Severity	Debug
Attribute	mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii", "uelmsi"="12345", "ueMsisdn"="98787" "apIpAddress"="10.1.4.11"
Displayed on the web interface	{{srcProcess}} Accounting message from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}} dropped, {produce.short.name} did not receive Accounting start message.

## Events Types

### Accounting Events

**TABLE 219** AP accounting retransmission message dropped event (continued)

Event	AP accounting retransmission message dropped
Description	This event occurs when the retransmitted accounting message is dropped while the call detail record is generated and the transfer to charging gateway function server is in progress.

## AP accounting response while invalid config

**TABLE 220** AP accounting response while invalid config event

Event	AP accounting response while invalid config
Event Type	apAcctRespWhileInvalidConfig
Event Code	1909
Severity	Debug
Attribute	mvnold="12 "wlanId"=1, "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut" "realm"="wlan.3gppnetwork.org", "userName"="abc@xyz.com", "SCGMgmtIp"="2.2.2.2", "apIpAddress"="10.1.4.11"
Displayed on the web interface	{{srcProcess}} sending dummy response for Accounting Packet received from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}}, with username {{userName}}. Configuration is incorrect in {produce.short.name} to forward received message nor to generate CDR
Description	This event occurs when the controller sends a dummy response to the AP accounting message since the configuration in the controller is incorrect. The event could either occur when forwarding received messages or when generating call detail records.

## AP account message drop while no accounting start message

**TABLE 221** AP account message drop while no accounting start message event

Event	AP account message drop while no accounting start message
Event Type	apAcctMsgDropNoAcctStartMsg
Event Code	1910
Severity	Critical
Attribute	mvnold="12 "wlanId"=1, "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org", "userName"="abc@xyz.com", "SCGMgmtIp"="2.2.2.2", "apIpAddress"="10.1.4.11"
Displayed on the web interface	{{srcProcess}} Dropped Accounting Packet received from AP {{apIpAddress}} on {produce.short.name} {{SCGMgmtIp}}, with username {{userName}}. Accounting session timer expired, stop or interim message not received, as Account Start not received from NAS/AP
Description	This event occurs when the accounting session timer expires. Stop or interim messages are not received since the account start is not received from the network access server (NAS) or access point (AP).

## Unauthorized COA/DM message dropped

**TABLE 222** Unauthorized COA/DM message dropped event

Event	Unauthorized COA/DM message dropped
Event Type	unauthorizedCoaDmMessageDropped

**TABLE 222** Unauthorized COA/DM message dropped event (continued)

Event	Unauthorized COA/DM message dropped
Event Code	1911
Severity	Critical
Attribute	mvnoid="12 "wlanId"=1, "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "userName"="abc@xyz.com", "radSrvrIp"="7.7.7.7","SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} Dropped CoA/DM Packet received from AAA {{radSrvrIp}} on {{produce.short.name}} {{SCGMgmtIp}}, with username {{userName}}. Received message from unauthorized AAA
Description	This event occurs when the controller receives a change of authorization (CoA) or dynamic multipoint (DM) messages from an unauthorized AAA server.

## AP Authentication Events

Following are the events related to authentication.

- [Radius server reachable](#) on page 140
- [Radius server unreachable](#) on page 140
- [LDAP server reachable](#) on page 140
- [LDAP server unreachable](#) on page 141
- [AD server reachable](#) on page 141
- [AD server unreachable](#) on page 141
- [Wechat ESP authentication server reachable](#) on page 142
- [WeChat ESP authentication server unreachable](#) on page 142
- [WeChat ESP authentication server resolvable](#) on page 142
- [WeChat ESP authentication server unresolvable](#) on page 143
- [WeChat ESP DNAT server reachable](#) on page 143
- [WeChat ESP DNAT server unreachable](#) on page 143
- [WeChat ESP DNAT server resolvable](#) on page 144
- [WeChat ESP DNAT server unresolvable](#) on page 144
- [Authentication Attempts](#) on page 144
- [Authentication Unsuccessful](#) on page 145
- [Authentication Re-attempt](#) on page 145
- [Authentication 8021](#) on page 145
- [AP Local Session Timeout](#) on page 145
- [AP Remote Session Timeout](#) on page 146
- [AP Interactive Session Termination](#) on page 146

## Events Types

### AP Authentication Events

## Radius server reachable

**TABLE 223** Radius server reachable event

Event	Radius server reachable
Event Type	radiusServerReachable
Event Code	2101
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac]} is able to reach radius server [{ip}] successfully.
Description	This event occurs when the AP is able to reach the radius server successfully.

## Radius server unreachable

**TABLE 224** Radius server unreachable event

Event	Radius server unreachable
Event Type	radiusServerUnreachable
Event Code	2102
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac]} is unable to reach radius server [{ip]}.
Description	This event occurs when the AP is unable to reach the radius server.
Auto Clearance	This event triggers the alarm 2102, which is auto cleared by the event code 2101

## LDAP server reachable

**TABLE 225** LDAP server reachable event

Event	LDAP server reachable
Event Type	ldapServerReachable
Event Code	2121
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac]} is able to reach LDAP server [{ip}] successfully.
Description	This event occurs when AP is able to reach the lightweight directory access protocol (LDAP) server successfully.

## LDAP server unreachable

**TABLE 226** LDAP server unreachable event

Event	LDAP server unreachable
Event Type	ldapServerUnreachable
Event Code	2122
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach LDAP server [{ip}].
Description	This event occurs when AP is unable to reach the LDAP server.
Auto Clearance	This event triggers the alarm 2122, which is auto cleared by the event code 2121.

## AD server reachable

**TABLE 227** AD server reachable event

Event	AD server reachable
Event Type	adServerReachable
Event Code	2141
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is able to reach AD server [{ip}].
Description	This event occurs when AP is able to reach the active directory successfully.

## AD server unreachable

**TABLE 228** AD server unreachable event

Event	AD server unreachable
Event Type	adServerUnreachable
Event Code	2142
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].
Description	This event occurs when AP is unable able to reach the active directory.
Auto Clearance	This event triggers the alarm 2142, which is auto cleared by the event code 2141.

## Wechat ESP authentication server reachable

**TABLE 229** Wechat ESP authentication server reachable event

Event	Wechat ESP authentication server reachable
Event Type	espAuthServerReachable
Event Code	2151
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac] is able to reach WeChat ESP authentication server [{ip}] successfully.
Description	This event occurs when AP successfully reaches WeChat ESP authentication server.

## WeChat ESP authentication server unreachable

**TABLE 230** WeChat ESP authentication server unreachable event

Event	WeChat ESP authentication server unreachable
Event Type	espAuthServerUnreachable
Event Code	2152
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac] is unable to reach WeChat ESP authentication server [{ip}]
Description	This event occurs when AP fails to reach WeChat ESP authentication server.
Auto Clearance	This event triggers the alarm 2152, which is auto cleared by the event code 2151

## WeChat ESP authentication server resolvable

**TABLE 231** WeChat ESP authentication server resolvable event

Event	WeChat ESP authentication server resolvable
Event Type	espAuthServerResolvable
Event Code	2153
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","dn"="www.test.com","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac] is able to resolve WeChat ESP authentication server domain name [{dn}] to [{ip}] successfully.
Description	This event occurs when AP successfully resolves WeChat ESP authentication server domain name.

## WeChat ESP authentication server unresolvable

**TABLE 232** WeChat ESP authentication server unresolvable event

Event	WeChat ESP authentication server unresolvable
Event Type	espAuthServerUnResolvable
Event Code	2154
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dn"="www.test.com", "profileId"="1", "fwVersion"="3.2.0.0.x", "model"="ZF7982", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to resolve WeChat ESP authentication server domain name [{dn}] to IP.
Description	This event occurs when AP fails to resolves WeChat ESP authentication server domain name.
Auto Clearance	This event triggers the alarm 2154, which is auto cleared by the event code 2153.

## WeChat ESP DNAT server reachable

**TABLE 233** WeChat ESP DNAT server reachable event

Event	WeChat ESP DNAT server reachable
Event Type	espDNATServerReachable
Event Code	2161
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ip"="17.0.0.12", "profileId"="1", "fwVersion"="3.2.0.0.x", "model"="ZF7982", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is able to reach WeChat ESP DNAT server [{ip}] successfully.
Description	This event occurs when AP successfully able to reach WeChat ESP DNAT server.

## WeChat ESP DNAT server unreachable

**TABLE 234** WeChat ESP DNAT server unreachable event

Event	WeChat ESP DNAT server unreachable
Event Type	espDNATServerUnreachable
Event Code	2162
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ip"="17.0.0.12", "profileId"="1", "fwVersion"="3.2.0.0.x", "model"="ZF7982", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach WeChat ESP DNAT server [{ip}].
Description	This event occurs when AP fails to reach WeChat ESP DNAT server.
Auto Clearance	This event triggers the alarm 2162, which is auto cleared by the event code 2161

## Events Types

### AP Authentication Events

## WeChat ESP DNAT server resolvable

**TABLE 235** WeChat ESP DNAT server resolvable event

Event	WeChat ESP DNAT server resolvable
Event Type	espDNATServerResolvable
Event Code	2163
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dn"="www.test.com", "ip"="17.0.0.12", "profileId"="1", "fwVersion"="3.2.0.0.x", "model"="ZF7982", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac]} is able to resolve WeChat ESP DNAT server domain name [{dn}] to [{ip}] successfully.
Description	This event occurs when AP successfully resolve WeChat ESP DNAT server domain name.

## WeChat ESP DNAT server unresolvable

**TABLE 236** WeChat ESP DNAT server unresolvable event

Event	WeChat ESP DNAT server unresolvable
Event Type	espDNATServerUnresolvable
Event Code	2164
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dn"="www.test.com", "profileId"="1", "fwVersion"="3.2.0.0.x", "model"="ZF7982", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Displayed on the web interface	AP [{apName}&&apMac]} is unable to resolve WeChat ESP DNAT server domain name [{dn}] to IP.
Description	This event occurs when AP fails to resolve WeChat ESP DNAT server domain name.
Auto Clearance	This event triggers the alarm 2164, which is auto cleared by the event code 2163

## Authentication Attempts

**TABLE 237** Authentication attempt event

Event	Authentication Attempts
Event Type	Auth Attempts
Event Code	99005
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Number of failed attempts to switch to trusted channel, AP: [{apMac]}.
Description	Number of failed attempts to switch to trusted channel



## Authentication Unsuccessful

**TABLE 238** Authentication unsuccessful event

Event	Authentication Unsuccessful
Event Type	authUnsucces
Event Code	99006
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	User had tried maximum number of unsuccessful login attempts, AP: [{apMac}].
Description	The event shows when User had tried maximum number of unsuccessful login attempts.

## Authentication Re-attempt

**TABLE 239** Authentication re-attempt event

Event	Authentication Re-attempt
Event Type	authReauth
Event Code	99007
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apMac}] is blocked and waited for specified amount of time before getting login prompt.
Description	The event occurs once the use is blocked and waited for specified amount of time before getting login prompt.

## Authentication 8021

**TABLE 240** Authentication 8021 client event

Event	Authentication Unsuccessful
Event Type	auth8021xClient
Event Code	99008
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Receiving data frame before client is authorized, AP: [{apMac}].
Description	The event show when receiving Data frame before client is authorized.

## AP Local Session Timeout

**TABLE 241** AP local session timeout event

Event	AP Local Session Timeout
Event Type	apLocalSessionTimeout
Event Code	99015

## Events Types

### AP Communication Events

**TABLE 241** AP local session timeout event (continued)

Event	AP Local Session Timeout
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Local AP [{apMac}] session terminates due to session timeout.
Description	This event occurs when local AP session terminates due to session timeout.

## AP Remote Session Timeout

**TABLE 242** AP Remote session timeout event

Event	AP Remote session timeout
Event Type	apRemoteSessionTimeout
Event Code	99016
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Remote AP [{apMac}] session terminates due to session timeout.
Description	This event occurs when Remote AP session terminates due to session timeout.

## AP Interactive Session Termination

**TABLE 243** AP Interactive Session Termination event

Event	AP Interactive Session Termination
Event Type	apInteractiveSessionTerm
Event Code	99017
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	User-initiated termination of an interactive AP [{apMac}] session.
Description	This event occurs on user-initiated termination of an interactive AP session.

## AP Communication Events

All events from AP are appended with firmware, model name, zone ID (if there is no zone ID, the key will not be present) at the end. Following are the events related to AP communications:

- [AP discovery succeeded](#) on page 147
- [AP managed](#) on page 148
- [AP rejected](#) on page 148
- [AP firmware updated](#) on page 148
- [AP firmware update failed](#) on page 149
- [Updating AP firmware](#) on page 149

- [Updating AP configuration](#) on page 149
- [AP configuration updated](#) on page 150
- [AP configuration update failed](#) on page 150
- [AP pre-provision model mismatched](#) on page 150
- [AP swap model mismatched](#) on page 151
- [AP WLAN oversubscribed](#) on page 151
- [AP join zone failed](#) on page 151
- [AP illegal to change country code](#) on page 152
- [AP configuration get failed](#) on page 152
- [Rogue AP](#) on page 152
- [Rogue AP disappeared](#) on page 152
- [Classified Rogue AP](#) on page 153
- [AP image signing failed](#) on page 153
- [Jamming attack](#) on page 153
- [AP Communication Events](#)
- [Key gen fail](#) on page 154
- [Key dis fail](#) on page 154
- [Key dis fail GTK](#) on page 155
- [wpaendec fail](#) on page 155
- [IPsecsec fail](#) on page 155
- [Fw manual initiation](#) on page 156
- [AP Management TSF data](#) on page 156
- [AP TSF failure](#) on page 156
- [AP Self tests](#) on page 157
- [Firmware initiation update](#) on page 157
- [SSH initiation](#) on page 157
- [SSH termination](#) on page 158
- [SSH failure](#) on page 158
- [TLS initiation](#) on page 158
- [TLS termination](#) on page 158
- [TLS failure](#) on page 159
- [IP sec initiation](#) on page 159
- [IP sec termination](#) on page 159
- [IP sec failure](#) on page 160

## AP discovery succeeded

**TABLE 244** AP discovery succeeded event

Event	AP discovery succeeded
Event Type	apDiscoverySuccess

## Events Types

### AP Communication Events

**TABLE 244** AP discovery succeeded event (continued)

Event	AP discovery succeeded
Event Code	101
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] sent a discovery request to {produce.short.name} [{wsgIP}]
Description	This event occurs when AP sends a discovery request to the {produce.short.name} successfully.

## AP managed

**TABLE 245** AP managed event

Event	AP managed
Event Type	apStatusManaged
Event Code	103
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] approved by {produce.short.name} [{wsgIP}].
Description	This event occurs when the AP is approved by the controller.

## AP rejected

**TABLE 246** AP rejected event

Event	AP rejected
Event Type	apStatusRejected
Event Code	105
Severity	Minor
Attribute	"apMac"="xxx.xxx.xxx.xxx", "wsgIP"="xxx.xxx.xxx.xxx", "reason"="xxxxxx"
Displayed on the web interface	{produce.short.name} [{wsgIP}] rejected AP [{apName&&apMac}] because of [{reason}].
Description	This event occurs when the AP is rejected by the controller.
Auto Clearance	This event triggers the alarm 101, which is auto cleared by the event code 103.

## AP firmware updated

**TABLE 247** AP firmware updated event

Event	AP firmware updated
Event Type	apFirmwareUpdated
Event Code	106
Severity	Informational

**TABLE 247** AP firmware updated event (continued)

Event	AP firmware updated
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234", "toVersion"="x.x.x", "fromVersion"="x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] updated its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP successfully updates the firmware details to the controller.

## AP firmware update failed

**TABLE 248** AP firmware update failed event

Event	AP firmware update failed
Event Type	apFirmwareUpdateFailed
Event Code	107
Severity	Major
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234", "toVersion"="x.x.x", "fromVersion"="x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP fails to update the firmware details to the controller.
Auto Clearance	This event triggers the alarm 107, which is auto cleared by the event code 106.

## Updating AP firmware

**TABLE 249** Updating AP firmware event

Event	Updating AP firmware
Event Type	apFirmwareApplying
Event Code	108
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234", "toVersion"="x.x.x", "fromVersion"="x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] firmware is being updated from [{fromVersion}] to [{toVersion}].
Description	This event occurs when AP updates its firmware.

## Updating AP configuration

**TABLE 250** Updating AP configuration event

Event	Updating AP configuration
Event Type	apConfApplying
Event Code	109
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234"

## Events Types

### AP Communication Events

**TABLE 250** Updating AP configuration event (continued)

Event	Updating AP configuration
Displayed on the web interface	AP [{apName&&apMac}] is being updated to new configuration ID [{configID}]
Description	This event occurs when AP updates its configuration.

## AP configuration updated

**TABLE 251** AP configuration updated event

Event	AP configuration updated
Event Type	apConfUpdated
Event Code	110
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "configID"="23456781234"
Displayed on the web interface	AP [{apName&&apMac}] updated to configuration [{configID}]
Description	This event occurs when the AP successfully updates the existing configuration details to the controller.

## AP configuration update failed

**TABLE 252** AP configuration update failed event

Event	AP configuration update failed
Event Type	apConfUpdateFailed
Event Code	111
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "configID"="23456781234"
Displayed on the web interface	AP [{apName&&apMac}] failed to update to configuration [{configID}].
Description	This event occurs when the AP fails to update the configuration details to the controller.
Auto Clearance	This event triggers the alarm 102, which is auto cleared by the event code 110.

## AP pre-provision model mismatched

**TABLE 253** AP pre-provision model mismatched event

Event	AP pre-provision model mismatched
Event Type	apModelDiffWithPreProvConfig
Event Code	112
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx", "configModel"="ZF7962" "model"="R700"
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from per-provision configuration model [configModel]

**TABLE 253** AP pre-provision model mismatched event (continued)

Event	AP pre-provision model mismatched
Description	This event occurs when the AP model differs from the configuration model.

## AP swap model mismatched

**TABLE 254** AP swap model mismatched event

Event	AP swap model mismatched
Event Type	apModelDiffWithSwapOutAP
Event Code	113
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx", "configModel"="xxx.xxx.xxx.xxx" "model"="R700"
Displayed on the web interface	AP [{apName}&&apMac] model [{model}] is different from swap configuration model [{configModel}].
Description	This event occurs when the AP model differs from the swap configuration model.

## AP WLAN oversubscribed

**TABLE 255** AP WLAN oversubscribed event

Event	AP WLAN oversubscribed
Event Type	apWlanOversubscribed
Event Code	114
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName}&&apMac] does not have enough capacity to deploy all wlan. Only maximum wlan number of the AP can be deployed
Description	This event occurs when the AP exceeds the maximum capacity for deploying all WLANs.

## AP join zone failed

**TABLE 256** AP join zone failed event

Event	AP join zone failed
Event Type	apJoinZoneFailed
Event Code	115
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "zoneUUID"="xx:xx:xx:xx:xx:xx", "targetZoneUUID"="xx:xx:xx:xx:xx:xx", "reason"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName}&&apMac] failed to join to zone [{targetZoneName}]. Reason: [{reason}]
Description	This event occurs when the AP fails to join the specified zone.

## Events Types

### AP Communication Events

## AP illegal to change country code

**TABLE 257** AP illegal to change country code event

Event	AP illegal to change country code
Event Type	apIllegalToChangeCountryCode
Event Code	116
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234"
Displayed on the web interface	AP [{apName}&&apMac] does not support country code change.
Description	This event occurs when attempting to change the country code for an AP. Changing of country code is not allowed.

## AP configuration get failed

**TABLE 258** AP configuration get failed event

Event	AP configuration get failed
Event Type	apGetConfigFailed
Event Code	117
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234"
Displayed on the web interface	AP [{apName}&&apMac] failed to get the configuration [{configID}].
Description	This event occurs when the AP fails to get the configuration.

## Rogue AP

**TABLE 259** Rogue AP event

Event	Rogue AP
Event Type	genericRogueAPDetected
Event Code	180
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxx", "channel"="xx"
Displayed on the web interface	Rogue AP[{rogueMac}] with SSID[{ssid}] is detected by [{apName}&&apMac] on channel[{channel}].
Description	This event occurs when the AP detects a rogue AP.

## Rogue AP disappeared

**TABLE 260** Rogue AP disappeared event

Event	Rogue AP disappeared
Event Type	maliciousRogueAPTimeout
Event Code	185



**TABLE 260** Rogue AP disappeared event (continued)

Event	Rogue AP disappeared
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Malicious rogue [{rogueMac}] detected by [{apName&&apMac}] goes away.
Description	This event occurs when the rogue AP disappears.

## Classified Rogue AP

**TABLE 261** Classified Rogue AP event

Event	Classified Rogue AP
Event Type	generalRogueAPDetected
Event Code	186
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxxxx", "channel"="xx", "rogueType"="xxxxx", "roguePolicyName"="xxxxx", "rogueRuleName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] has detected a rogue AP rogue AP[{rogueMac}] with SSID[{ssid}] on channel[{channel}] classified as [{rogueType}] because of rogue classification policy (policy[{roguePolicyName}], rule[{rogueRuleName}]).
Description	This event occurs when the AP detects a rogue AP(malicious/known) that is classified by configurable rogue policy and its rules.

## AP image signing failed

**TABLE 262** AP image signing failed event

Event	AP image signing failed
Event Type	apSigningInformation
Event Code	187
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The AP[{apMac}] image signing failed with firmware version [{fwVersion}].
Description	This event occurs when an AP image signing fails.

## Jamming attack

**TABLE 263** Jamming attack event

Event	Jamming attack
Event Type	jammingDetected
Event Code	189
Severity	Warning

## Events Types

### AP Communication Events

**TABLE 263** Jamming attack event (continued)

Event	Jamming attack
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="" "xxx.xxx.xxx.xxx", "ssid"="xxxxxxxx", "channel"="xx" "rogueType"="xxxx" "roguePolicyName"="xxxx" "rogueRuleName"="xxxx"
Displayed on the web interface	A jamming rogue AP[{rogueMac}] with SSID[ssid] is detected by [{apName&&apMac}] on channel[{channel]}.
Description	This event occurs when an AP detects a radio jamming attack.

## Rogue client

**TABLE 264** Rogue client

Event	Rogue client
Event Type	Malicious rogue client
Event Code	194
Severity	Warning
Attribute	Rogue Client MAC; Rogue-Type; Monitoring AP-IP @Monitoring AP-MAC
Displayed on the web interface	Malicious rogue client [ Rogue Client MAC] detected by [Rogue Type] by [Monitoring AP-IP @Monitoring AP-MAC]
Description	This event occurs when an AP detects a malicious rogue client.

### ATTENTION

By default all the notifications are disabled. The Administrator has to enable **DB Persistence** notification for this event.

## Key gen fail

**TABLE 265** Key gen fail event

Event	Key gen fail
Event Type	KeyGenFail
Event Code	99000
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	PMK is not available to derive PTK, AP: [{apMac}].
Description	This event occurs when PMK is not available to derive PTK.

## Key dis fail

**TABLE 266** Key dis fail event

Event	Key gen fail
Event Type	KeyDisFail
Event Code	99001
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",

**TABLE 266** Key dis fail event (continued)

Event	Key gen fail
Displayed on the web interface	4-way handshake is failure, AP [{apMac}].
Description	This event occurs when 4-way handshake is failure.

## Key dis fail GTK

**TABLE 267** Key dis fail GTK event

Event	Key dis fail
Event Type	KeyDisFailGTK
Event Code	99002
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	4-way handshake is failure, AP [{apMac}].
Description	This event occurs when 4-way handshake is failure

## wpaendec fail

**TABLE 268** WpaEnDec fail event

Event	WpaEnDec fail
Event Type	wpaEnDecFail
Event Code	99003
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Failure of WPA encryption and decryption, AP: [{apMac}].
Description	This event occurs when there is a failure of WPA encryption and decryption.

## IPsecses fail

**TABLE 269** IPsecSes fail event

Event	IPsecSes Fail
Event Type	IpsecSesFail
Event Code	99004
Severity	Critical
Attribute	"apIP"="e.f.g.h", "dpIP"="a.b.c.d" "tunnelType"= RGRE/SGRE
Displayed on the web interface	IPsec session establishment and termination due to SA failure, AP: [{apIP}], vDP IP: [{dpIP}], Tunnel type: [{tunnelType}].
Description	This event occurs whenever there is IPsec session establishment and termination due to SA failure.

## Fw manual initiation

**TABLE 270** Fw manual initiation event

Event	Fw manual initiation
Event Type	FwManuallInitiation
Event Code	99009
Severity	Informational
Attribute	"apIP"="e.f.g.h", "dIP"="a.b.c.d" "tunnelType"= RGRE/SGRE "apMac"="xx:xx:xx:xx:xx:xx", " Manual FW update initiated" "apMac"="xx:xx:xx:xx:xx:xx", " Manual FW:'fwname' update, not needed. it is same!" "apMac"="xx:xx:xx:xx:xx:xx", " Manual FW:'fwname' update, not needed." "apMac"="xx:xx:xx:xx:xx:xx", "Manual FW:%s update successful" "apMac"="xx:xx:xx:xx:xx:xx", " Manual FW update failed with failcode:3"
Displayed on the web interface	AP [{apMac}] attempt to initiate a manual update, reason: [{reason}]
Description	This event occurs whenever there is manual firmware update.

## AP Management TSF data

**TABLE 271** AP Management TSF data event

Event	AP Management TSF data
Event Type	APMGMNTTSFdata
Event Code	99010
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	All management activities of TSF data initiated/started/executed, AP: [{apMac}].
Description	This event occurs whenever there is All management activities of TSF data initiated/started/executed.

## AP TSF failure

**TABLE 272** AP TSF failure event

Event	AP TSF failure
Event Type	APTSFFailure
Event Code	99011
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Failure of all or any management TSF, AP: [{apMac}].
Description	This event occurs whenever there is Failure of all or any management TSF

## AP Self tests

**TABLE 273** AP Self tests event

Event	AP Self tests
Event Type	apSelfTests
Event Code	99012
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "Power-up, dropbear, openssl, FIPS_WifiST, Integrity Tests and Kernel self test are passed"
Displayed on the web interface	AP [{apMac}] has execution of this set of TSF self-tests and detected integrity violations, reason: [{reason}]
Description	This event occurs whenever all self tests are passed for fips_sku builds

## Firmware initiation update

**TABLE 274** Firmware initiation update event

Event	Firmware initiation update
Event Type	FwInitiationUpdate
Event Code	99013
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx", " rsm_fw_update(FW_TYPE_TDTS_RULE) ret=1 no update" "apMac"="xx:xx:xx:xx:xx:xx", " rsm_fw_update(FW_TYPE_TDTS_RULE) ret=%d Successful update" "apMac"="xx:xx:xx:xx:xx:xx", " rsm_fwd_update(FW_TYPE_TDTS_RULE) ret=1 fail"
Displayed on the web interface	AP [{apMac}] has is firmware update, reason: [{reason}]
Description	This event occurs whenever there is firmware update.

## SSH initiation

**TABLE 275** SSH initiation event

Event	SSH initiation
Event Type	sshInitiation
Event Code	99018
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "Login with username admin successful"
Displayed on the web interface	SSH session started with successful authentication, AP: [{apMac}]
Description	This event occurs whenever there SSH session started with successful authentication.

## Events Types

### AP Communication Events

## SSH termination

**TABLE 276** SSH termination event

Event	SSH termination
Event Type	sshTermination
Event Code	99019
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "SSH session exited"
Displayed on the web interface	There is exit from established SSH session, AP: [{apMac}].
Description	This event occurs whenever there is exit from established SSH session

## SSH failure

**TABLE 277** SSH failure event

Event	SSH failure
Event Type	sshFailure
Event Code	99020
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "Login with username admin failed"
Displayed on the web interface	There SSH session initiation with failed authentication, AP: [{apMac}].
Description	This event occurs whenever there SSH session initiation with failed authentication.

## TLS initiation

**TABLE 278** TLS initiation event

Event	TLS initiation
Event Type	tlsInitiation
Event Code	99021
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "HTTPS Login with username admin successful"
Displayed on the web interface	There is login through AP [{apMac}] web-GUI is successful.
Description	This event occurs whenever there is login through AP web-GUI is successful or AP establishes a trusted TLS connection.

## TLS termination

**TABLE 279** TLS termination event

Event	TLS termination
Event Type	tlsTermination
Event Code	99022
Severity	Major

**TABLE 279** TLS termination event (continued)

Event	TLS termination
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "HTTPS Logout successful"
Displayed on the web interface	There is logout from AP [{apMac}] web-GUI session.
Description	This event occurs whenever there is logout from AP web-GUI session or AP gracefully terminates a trusted TLS connection.

## TLS failure

**TABLE 280** TLS failure event

Event	TLS failure
Event Type	tlsFailure
Event Code	99023
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "HTTPS Login with username admin failed"
Displayed on the web interface	There is login through AP [{apMac}] web-GUI is failed.
Description	This event occurs whenever there is login through AP web-GUI is failed or AP fails to establish a trusted TLS connection.

## IP sec initiation

**TABLE 281** IP sec initiation event

Event	IP sec initiation
Event Type	IPsecInitiation
Event Code	99024
Severity	Informational
Attribute	"apIP"="e.f.g.h", "dpIP"="a.b.c.d" "tunnelType"= RGRE/SGRE
Displayed on the web interface	There is ipsec session initiation, AP: [{apIP}], vDP IP: [{dpIP}], Tunnel type: [{tunnelType}].
Description	This event occurs whenever there is ipsec session initiation.

## IP sec termination

**TABLE 282** IP sec termination event

Event	IP sec termination
Event Type	IPsecTermination
Event Code	99025
Severity	Major
Attribute	"apIP"="e.f.g.h", "dpIP"="a.b.c.d" "tunnelType"= RGRE/SGRE
Displayed on the web interface	There is ipsec session terminated or exited, AP: [{apIP}], vDP IP: [{dpIP}], Tunnel type: [{tunnelType}].
Description	This event occurs whenever there is ipsec session terminated or exited.

## IP sec failure

**TABLE 283** IP sec failure event

Event	IP sec failure
Event Type	IPsecFailure
Event Code	99026
Severity	Critical
Attribute	"apIP"="e.f.g.h", "dpIP"="a.b.c.d" "tunnelType"= RGRE/SGRE
Displayed on the web interface	There is ipsec session attempt failure, AP: [{apIP}], vDP IP: [{dpIP}], Tunnel type: [{tunnelType}].
Description	This event occurs whenever there is ipsec session attempt failure.

## AP LBS Events

The following are the events related to AP Location Based Service (LBS).

- [No LS responses](#) on page 160
- [LS authentication failure](#) on page 161
- [AP connected to LS](#) on page 161
- [AP failed to connect to LS](#) on page 161
- [AP started location service](#) on page 161
- [AP stopped location service](#) on page 162
- [AP received passive calibration request](#) on page 162
- [AP received passive footfall request](#) on page 162
- [AP received unrecognized request](#) on page 163

## No LS responses

**TABLE 284** No LS responses event

Event	No LS responses
Event Type	apLBSNoResponses
Event Code	701
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""
Displayed on the web interface	AP [{apName}&&apMac}] no response from LS: url=[{url}], port=[{port}]
Description	This event occurs when the AP does not get a response when trying to connect to the location based service.



## LS authentication failure

**TABLE 285** LS authentication failure event

Event	LS authentication failure
Event Type	apLBSAuthFailed
Event Code	702
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""
Displayed on the web interface	AP [{apName}&&apMac]} LBS authentication failed: url= [{url}], port= [{port}]
Description	This event occurs due to the authentication failure on connecting to the location based service.

## AP connected to LS

**TABLE 286** AP connected to LS event

Event	AP connected to LS
Event Type	apLBSConnectSuccess
Event Code	703
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""
Displayed on the web interface	AP [{apName}&&apMac]} connected to LS: url= [{url}], port= [{port}]
Description	This event occurs when the AP successfully connects to the location based service.

## AP failed to connect to LS

**TABLE 287** AP failed to connect to LS event

Event	AP failed to connect to LS
Event Type	apLBSConnectFailed
Event Code	704
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"=""
Displayed on the web interface	AP [{apName}&&apMac]} connection failed to LS: url= [{url}], port= [{port}]
Description	This event occurs when the AP fails to connect to the location based service.
Auto Clearance	This event triggers the alarm 704, which is auto cleared by the event code 703.

## AP started location service

**TABLE 288** AP started location service event

Event	AP started location service
Event Type	apLBSStartLocationService
Event Code	705

**TABLE 288** AP started location service event (continued)

Event	AP started location service
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "venue"=""
Displayed on the web interface	AP [{apName}&&apMac] Start Ruckus Location Service: venue= [{venue}], band= [{band}]
Description	This event occurs when the AP starts to get the location data.

## AP stopped location service

**TABLE 289** AP stopped location service event

Event	AP stopped location service
Event Type	apLBSStopLocationService
Event Code	706
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "venue"=""
Displayed on the web interface	AP [{apName}&&apMac] Stop Ruckus Location Service: venue= [{venue}], band= [{band}]
Description	This event occurs when the AP stops getting the location data.

## AP received passive calibration request

**TABLE 290** AP received passive calibration request event

Event	AP received passive calibration request
Event Type	apLBSRcvdPassiveCalReq
Event Code	707
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"="", "count"=""
Displayed on the web interface	AP [{apName}&&apMac] received Passive Calibration Request: interval=[{interval}s], duration=[{duration}m], band=[{band}]
Description	This event occurs when the AP receives the passive calibration request.

## AP received passive footfall request

**TABLE 291** AP received passive footfall request event

Event	AP received passive footfall request
Event Type	apLBSRcvdPassiveFFReq
Event Code	708
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"=""
Displayed on the web interface	AP [{apName}&&apMac] received Passive Footfall Request: interval=[{interval}s], duration=[{duration}m], band=[{band}]
Description	This event occurs when the AP receives the passive footfall request.

## AP received unrecognized request

**TABLE 292** AP received unrecognized request event

Event	AP received unrecognized request
Event Type	apLBSRcvdUnrecognizedRequest
Event Code	709
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "type"="", "length"="", "SCGMgmtIp"=""
Displayed on the web interface	AP [{apName&&apMac}] received Unrecognized Request: type = [{type}], length = [{length}]
Description	This event occurs when the AP receives an unrecognized request.

## AP Mesh Events

Following are the events related to access point (AP) mesh.

- [EMAP downlink connected to MAP](#) on page 163
- [EMAP downlink disconnected from MAP](#) on page 164
- [EMAP uplink connected to MAP](#) on page 164
- [EMAP uplink disconnected from MAP](#) on page 164
- [MAP disconnected](#) on page 165
- [MAP downlink connected](#) on page 165
- [MAP downlink connected to EMAP](#) on page 165
- [MAP downlink disconnected from EMAP](#) on page 166
- [RAP downlink connected to MAP](#) on page 166
- [MAP uplink connected to EMAP](#) on page 166
- [MAP uplink disconnected from EMAP](#) on page 166
- [MAP uplink connected to RAP](#) on page 167
- [MAP uplink connected to MAP](#) on page 167
- [Mesh state updated to MAP](#) on page 167
- [Mesh state updated to MAP no channel](#) on page 168
- [Mesh state updated to RAP](#) on page 168
- [Mesh state update to RAP no channel](#) on page 168
- [MAP downlink connected to MAP](#) on page 169
- [MAP downlink disconnected from MAP](#) on page 169
- [RAP downlink disconnected from MAP](#) on page 169

## EMAP downlink connected to MAP

**TABLE 293** EMAP downlink connected to MAP event

Event	EMAP downlink connected to MAP
Event Type	emapDlinkConnectWithMap

**TABLE 293** EMAP downlink connected to MAP event (continued)

Event	EMAP downlink connected to MAP
Event Code	405
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	eMAP [{apName&&apMac}] accepted connection from MAP [{mapName&&mapMac}].
Description	This event occurs when mobile application part (MAP) to Ethernet Mesh AP (EMAP) connection is successful.

## EMAP downlink disconnected from MAP

**TABLE 294** EMAP downlink disconnected from MAP event

Event	EMAP downlink disconnected from MAP
Event Type	emapDlinkDisconnectWithMap
Event Code	406
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{mapName&&mapMac}] disconnects from eMAP [{apName&&apMac}].
Description	This event occurs when MAP disconnects from Ethernet Mesh AP

## EMAP uplink connected to MAP

**TABLE 295** EMAP uplink connected to MAP event

Event	EMAP uplink connected to MAP
Event Type	emapUlinkConnectWithMap
Event Code	407
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	eMAP [{apName&&apMac}] uplink connected to MAP [{mapName&&mapMac}]
Description	This event occurs when Ethernet Mesh AP uplink connection to MAP is successful.

## EMAP uplink disconnected from MAP

**TABLE 296** EMAP uplink disconnected from MAP event

Event	EMAP uplink disconnected from MAP
Event Type	emapUlinkDisconnectWithMap
Event Code	408
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	eMAP [{apName&&apMac}] uplink disconnected from MAP [{mapName&&mapMac}]

**TABLE 296** EMAP uplink disconnected from MAP event (continued)

Event	EMAP uplink disconnected from MAP
Description	This event occurs when Ethernet Mesh AP uplink disconnects from MAP.

## MAP disconnected

**TABLE 297** MAP disconnected event

Event	MAP disconnected
Event Type	mapDisconnected
Event Code	411
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{xapName&&xapMac}] disconnected from AP [{apName&&apMac}]
Description	This event occurs when MAP disconnects from AP.

## MAP downlink connected

**TABLE 298** MAP downlink connected event

Event	MAP downlink connected
Event Type	mapDlinkConnected
Event Code	412
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{apName&&apMac}] downlink connected
Description	This event occurs when MAP downlink connects to the AP.

## MAP downlink connected to EMAP

**TABLE 299** MAP downlink connected to EMAP event

Event	MAP downlink connected to EMAP
Event Type	mapDlinkConnectWitheMap
Event Code	413
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "emapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{apName&&apMac}] accepted connection from eMAP [{emapName&&emapMac}]
Description	This event occurs when MAP accepts the connection from Ethernet Mesh AP.

## MAP downlink disconnected from EMAP

**TABLE 300** MAP downlink disconnected from EMAP event

Event	MAP downlink disconnected from EMAP
Event Type	mapDlinkDisconnectWithMap
Event Code	414
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "emapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	eMAP [{emapName&&emapMac}] disconnected from MAP [{apName&&apMac}]
Description	This event occurs when Ethernet Mesh AP disconnects from MAP.

## RAP downlink connected to MAP

**TABLE 301** RAP downlink connected to MAP event

Event	RAP downlink connected to MAP
Event Type	rapDlinkConnectWithMap
Event Code	416
Severity	Informational
Attribute	"rapMac"="xx:xx:xx:xx:xx:xx", "mapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	RAP [{apName&&apMac}] accepted connection from MAP [{mapName&&mapMac}]
Description	This event occurs when the root access point (RAP) accepts MAP connection.

## MAP uplink connected to EMAP

**TABLE 302** MAP uplink connected to EMAP event

Event	MAP uplink connected to EMAP
Event Type	mapUlinkConnectToMap
Event Code	417
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "emapMac"="xx:xx:xx:xx:xx:xx", "rssi"="xx", "meshDepth"="x"
Displayed on the web interface	MAP [{apName&&apMac}] connected to eMAP [{emapName&&emapMac}] with RSSI [{rssi}] across [{meshDepth}] links
Description	This event occurs when MAP successfully connects to Ethernet Mesh AP with received signal strength indicator (RSSI) (across links).

## MAP uplink disconnected from EMAP

**TABLE 303** MAP uplink disconnected from EMAP event

Event	MAP uplink disconnected from EMAP
Event Type	mapUlinkDisconnectToMap
Event Code	418

**TABLE 303** MAP uplink disconnected from EMAP event (continued)

Event	MAP uplink disconnected from EMAP
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "emapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{apName&&apMac}] disconnected from eMAP [{emapName&&emapMac}]
Description	This event occurs when MAP disconnects from Ethernet Mesh AP.

## MAP uplink connected to RAP

**TABLE 304** MAP uplink connected to RAP event

Event	MAP uplink connected to RAP
Event Type	mapUlinkConnectToRap
Event Code	419
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "rootMac"="xx:xx:xx:xx:xx:xx", "rssi"="xx", "meshDepth"="x"
Displayed on the web interface	MAP [{apName&&apMac}] connected to RAP [{rootName&&rootMac}] with RSSI [{rssi}] across [{meshDepth}] links
Description	This event occurs when MAP connects to RAP with RSSI (across links).

## MAP uplink connected to MAP

**TABLE 305** MAP uplink connected to MAP event

Event	MAP uplink connected to MAP
Event Type	mapUlinkConnectToMap
Event Code	420
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "secondMapMac"="xx:xx:xx:xx:xx:xx", "rssi"="xx", "meshDepth"="x"
Displayed on the web interface	MAP [{apName&&apMac}] connected to MAP [{secondMapName&&secondMapMac}] with RSSI [{rssi}] across [{meshDepth}] links
Description	This event occurs when the MAP connects to a second MAP with RSSI (across links).

## Mesh state updated to MAP

**TABLE 306** Mesh state updated to MAP event

Event	Mesh state updated to MAP
Event Type	meshStateUpdateToMap
Event Code	421
Severity	Informational

**TABLE 306** Mesh state updated to MAP event (continued)

Event	Mesh state updated to MAP
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "mapMac"="xx:xx:xx:xx:xx:xx", "numHop"="x", "channel"="xx", "downlinkState"="xx", "radio"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] uplinks to [{mapName&&mapMac}] across [{numHop}] hops on channel [{channel}] at [{radio}] with downlink [{downlinkState}]
Description	This event occurs when the AP is set to MAP uplinks across hops on channel radio (with downlink).

## Mesh state updated to MAP no channel

**TABLE 307** Mesh state updated to MAP no channel event

Event	Mesh state updated to MAP no channel
Event Type	meshStateUpdateToMapNoChannel
Event Code	422
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "mapMac"="xx:xx:xx:xx:xx:xx", "numHop"="x", "downlinkState"="xx"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] uplinks to [{mapName&&mapMac}] across [{numHop}] hops with downlink [{downlinkState}]
Description	This event occurs when the AP is set to MAP links across hops (with downlink).

## Mesh state updated to RAP

**TABLE 308** Mesh state updated to RAP event

Event	Mesh state updated to RAP
Event Type	meshStateUpdateToRap
Event Code	423
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "channel"="xx", "downlinkState"="xx", "radio"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] on channel [{channel}] at [{radio}] with downlink [{downlinkState}]
Description	This event occurs when the AP is set to channel radio (with downlink).

## Mesh state update to RAP no channel

**TABLE 309** Mesh state update to RAP no channel event

Event	Mesh state update to RAP no channel
Event Type	meshStateUpdateToRapNoChannel
Event Code	424
Severity	Informational



**TABLE 309** Mesh state update to RAP no channel event (continued)

Event	Mesh state update to RAP no channel
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "downlinkState"="xx"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] with downlink [{downlinkState}]
Description	This event occurs when the AP is set to downlink.

## MAP downlink connected to MAP

**TABLE 310** MAP downlink connected to MAP event

Event	MAP downlink connected to MAP
Event Type	mapDlinkConnectWithMap
Event Code	425
Severity	Informational
Attribute	"mapMac"=" xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{apName&&apMac}] accepted connection from MAP [{mapName&&mapMac}]
Description	This event occurs when the MAP accepts a connection from another MAP.

## MAP downlink disconnected from MAP

**TABLE 311** MAP downlink disconnected from MAP event

Event	MAP downlink disconnected from MAP
Event Type	mapDlinkDisconnectWithMap
Event Code	426
Severity	Informational
Attribute	"secondMapMac"=" xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{secondMapName&&secondMapMac}] disconnected from MAP [{apName&&apMac}]
Description	This event occurs when the MAP disconnects from a second MAP.

## RAP downlink disconnected from MAP

**TABLE 312** RAP downlink disconnected from MAP event

Event	RAP downlink disconnected from MAP
Event Type	rapDlinkDisconnectWithMap
Event Code	427
Severity	Informational
Attribute	"secondMapMac"=" xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{secondMapName&&secondMapMac}] disconnected from RAP [{apName&&apMac}]
Description	This event occurs when the MAP disconnects from RAP.

# AP State Change Events

Following are the events related to access point state changes:

Event	Event	Event
<a href="#">AP rebooted by user</a> on page 170	<a href="#">AP rebooted by system</a> on page 171	<a href="#">AP disconnected</a> on page 171
<a href="#">AP IP address updated</a> on page 171	<a href="#">AP reset to factory default</a> on page 172	<a href="#">AP channel updated</a> on page 172
<a href="#">AP country code updated</a> on page 172	<a href="#">AP channel updated because dynamic frequency selection (DFS) detected a radar</a> on page 172	<a href="#">AP change control plane</a> on page 173
<a href="#">AP connected</a> on page 173	<a href="#">AP deleted</a> on page 173	<a href="#">AP heartbeat lost</a> on page 174
<a href="#">AP tagged as critical</a> on page 174	<a href="#">AP cable modem interface down</a> on page 174	<a href="#">AP brownout</a> on page 175
<a href="#">AP cable modem power-cycled by user</a> on page 175	<a href="#">AP smart monitor turn off WLAN</a> on page 175	<a href="#">AP client load balancing limit reached</a> on page 175
<a href="#">AP client load balancing limit recovered</a> on page 176	<a href="#">AP WLAN state changed</a> on page 176	<a href="#">AP capacity reached</a> on page 176
<a href="#">AP capacity recovered</a> on page 177	<a href="#">AP cable modem interface up</a> on page 177	<a href="#">AP cable modem soft-rebooted by user</a> on page 177
<a href="#">AP cable modem set to factory default by user</a> on page 178	<a href="#">AP health high latency flag</a> on page 178	<a href="#">AP health low capacity flag</a> on page 178
<a href="#">AP health high connection failure flag</a> on page 179	<a href="#">AP health high client count flag</a> on page 179	<a href="#">AP health high latency clear</a> on page 179
<a href="#">AP health low capacity clear</a> on page 180	<a href="#">AP health high connection failure clear</a> on page 180	<a href="#">AP health high client count clear</a> on page 180
<a href="#">Primary DHCP AP is down</a> on page 181	<a href="#">Primary DHCP AP is up</a> on page 181	<a href="#">Secondary DHCP AP is down</a> on page 181
<a href="#">Secondary DHCP AP is up</a> on page 182	<a href="#">Primary or secondary DHCP AP detects 90% of the configured total IPs</a> on page 182	<a href="#">Both primary and secondary DHCP server APs are down</a> on page 182
<a href="#">AP NAT gateway IP failover detected for particular VLAN pool</a> on page 182	<a href="#">AP NAT gateway IP fall back detected for particular VLAN pool</a> on page 183	<a href="#">NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool</a> on page 183
<a href="#">NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up</a> on page 184	<a href="#">AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down</a> on page 184	<a href="#">AP health high airtime utilization flag</a> on page 184
<a href="#">AP health high airtime utilization clear</a> on page 185	<a href="#">AP cluster failover</a> on page 185	<a href="#">AP cluster rehome</a> on page 185
<a href="#">AP switchover cluster failed</a> on page 186	<a href="#">AP MAC OUI violation</a> on page 186	<a href="#">Backhaul switched to primary</a> on page 186
<a href="#">Backhaul switched to secondary</a> on page 187	<a href="#">LTE network connectivity lost</a> on page 187	<a href="#">Ethernet network connectivity lost</a> on page 187
<a href="#">LTE DHCP timeout</a> on page 187	<a href="#">Ethernet link down</a> on page 188	<a href="#">Ethernet link up</a> on page 188
<a href="#">SIM switch</a> on page 188	<a href="#">Remote host blacklisted</a> on page 189	<a href="#">SIM removal</a> on page 189
<a href="#">LTE network registration status</a> on page 189	<a href="#">LTE connection status</a> on page 189	<a href="#">LTE good rssi status</a> on page 190
<a href="#">LTE weak rssi status</a> on page 190	<a href="#">AP client load balancing limit reached</a> on page 190	<a href="#">AP client load balancing limit recovered</a> on page 191
<a href="#">AP System Anomaly</a> on page 54		

## AP rebooted by user

**TABLE 313** AP rebooted by user event

Event	AP rebooted by user
Event Type	apRebootByUser
Event Code	301
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxx"

**TABLE 313** AP rebooted by user event (continued)

Event	AP rebooted by user
Displayed on the web interface	AP [{apName&&apMac}] rebooted because of [{reason}]
Description	This event occurs when an AP has to reboot.

## AP rebooted by system

**TABLE 314** AP rebooted by system event

Event	AP rebooted by system
Event Type	apRebootBySystem
Event Code	302
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] rebooted by the system because of [{reason}]
Description	This event occurs when the system reboots the AP.

## AP disconnected

**TABLE 315** AP disconnected event

Event	AP disconnected
Event Type	apConnectionLost (detected on the server)
Event Code	303
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] disconnected
Description	This event occurs when the AP disconnects from the controller.
Auto Clearance	This event triggers the alarm 303, which is auto cleared by the event code 312.

## AP IP address updated

**TABLE 316** AP IP address updated event

Event	AP IP address updated
Event Type	apIPChanged
Event Code	304
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] reset because of an IP address change
Description	This event occurs when the AP is reset due to a change in the IP address.

## Events Types

### AP State Change Events

## AP reset to factory default

**TABLE 317** AP reset to factory default event

Event	AP reset to factory default
Event Type	apFactoryReset
Event Code	305
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] reset to factory default settings
Description	This event occurs when the AP is reset to factory default settings.

## AP channel updated

**TABLE 318** AP channel updated event

Event	AP channel updated
Event Type	apChannelChanged
Event Code	306
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "radio"="xxx", "fromChannel"="xx", "toChannel"="xx"
Displayed on the web interface	AP [{apName&&apMac}] detected interference on radio [{radio}] and has switched from channel [{fromChannel}] to channel [{toChannel}]
Description	This event occurs when the AP detects the radio interference and switches to another channel.

## AP country code updated

**TABLE 319** AP country code updated event

Event	AP country code updated
Event Type	apCountryCodeChanged
Event Code	307
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] reset because of a country code change
Description	This event occurs when a change in country code causes the AP to reset.

## AP channel updated because dynamic frequency selection (DFS) detected a radar

**TABLE 320** AP channel updated because dynamic frequency selection (DFS) detected a radar event

Event	AP channel updated because dynamic frequency selection (DFS) detected a radar
Event Type	apDfsRadarEvent
Event Code	308
Severity	Informational

**TABLE 320** AP channel updated because dynamic frequency selection (DFS) detected a radar event (continued)

Event	AP channel updated because dynamic frequency selection (DFS) detected a radar
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "radio"="xxx", "channel"="xx"
Displayed on the web interface	AP [{apName}&&apMac] detected radar burst on radio [{radio}] and channel [{channel}] went into non-occupancy period
Description	This event occurs when the AP detects a radar burst on the radio and the channel moves to a non-occupancy mode.

## AP change control plane

**TABLE 321** AP change control plane event

Event	AP change control plane
Event Type	apChangeControlBlade
Event Code	311
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "oldwsgIP"="xxx.xxx.xxx.xxx", "newwsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName}&&apMac] switched from {produce.short.name} [{oldCpName   oldWsgIP}] to {produce.short.name} [{cpName   newWsgIP}].
Description	This event occurs when the AP switches from an existing controller connection to a new connection.

## AP connected

**TABLE 322** AP connected event

Event	AP connected
Event Type	apConnected
Event Code	312
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName}&&apMac] connected because of [{reason}].
Description	This event occurs when the AP is connected.

## AP deleted

**TABLE 323** AP deleted event

Event	AP deleted
Event Type	apDeleted (detected on the server)
Event Code	313
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"

## Events Types

### AP State Change Events

**TABLE 323** AP deleted event (continued)

Event	AP deleted
Displayed on the web interface	AP [{apName&&apMac}] deleted
Description	This event occurs when the AP is deleted on the server side.

## AP heartbeat lost

**TABLE 324** AP heartbeat lost event

Event	AP heartbeat lost
Event Type	apHeartbeatLost
Event Code	314
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] heartbeat lost.
Description	This event occurs when the AP is deleted due to a lost heartbeat.

## AP tagged as critical

**TABLE 325** AP tagged as critical event

Event	AP tagged as critical
Event Type	apTaggedAsCritical
Event Code	315
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] tagged as critical
Description	This event occurs when the AP is tagged critical.

## AP cable modem interface down

**TABLE 326** AP cable modem interface down event

Event	AP cable modem interface down
Event Type	cableModemDown
Event Code	316
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] cable modem interface is down
Description	This event occurs when the AP cable modem interface is down.
Auto Clearance	This event triggers the alarm 308, which is auto cleared by the event code 325.

## AP brownout

**TABLE 327** AP brownout event

Event	AP brownout
Event Type	apBrownout
Event Code	317
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apMac}] voltage deviation on [{cause}] port
Description	This event occurs due to a voltage deviation on the AP port.

## AP cable modem power-cycled by user

**TABLE 328** AP cable modem power-cycled by user event

Event	AP cable modem power-cycled by user
Event Type	cmRebootByUser
Event Code	318
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] cable modem power-cycled because of [{reason}].]
Description	This event occurs when AP cable modem is power-cycled because the user executes the power-cycle CLI command.

## AP smart monitor turn off WLAN

**TABLE 329** AP smart monitor turn off WLAN event

Event	AP smart monitor turn off WLAN
Event Type	smartMonitorTurnOffWLAN
Event Code	319
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "turnOffTime"="", "turnOnTime"=""
Displayed on the web interface	AP [{apName&&apMac}] turned off WLANs by Smart Monitor on [{time(turnOffTime)}] and turn on WLANs on [{time(turnOnTime)}]
Description	This event occurs when the smart monitor of the AP turns off the WLAN.

## AP client load balancing limit reached

**TABLE 330** AP client load balancing limit reached event

Event	AP client load balancing limit reached
Event Type	apCLBlimitReached
Event Code	320
Severity	Warning

## Events Types

### AP State Change Events

**TABLE 330** AP client load balancing limit reached event (continued)

Event	AP client load balancing limit reached
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "bssid"="xx:xx:xx:xx:xx:xx", "clb-load-limit"="", "cur-load"="", "min-clbpartner-bssid"="", "min-clbpartner-load"="", "num-clbpartners"="", "low-clbpartners"=""
Displayed on the web interface	AP [{apname@apMac}] reached client load limit, [{cur-load}] / [{clb-load-limit}], on WLAN [{ssid}]
Description	This event occurs when the AP reaches the client loading balance (CLB) limit. The adjacent threshold limit value is 50 for 2.4GHz radio and 43 for 5GHz radio.

## AP client load balancing limit recovered

**TABLE 331** AP client load balancing limit recovered event

Event	AP client load balancing limit recovered
Event Type	apCLBLimitRecovered
Event Code	321
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "bssid"="xx:xx:xx:xx:xx:xx", "clb-load-limit"="", "cur-load"="",
Displayed on the web interface	AP [{apname@apMac}] recovered from client load limit, [{cur-load}] / [{clb-load-limit}], on WLAN [{ssid}]
Description	This event occurs when the AP is recovered from client load balance (CLB) limit. The adjacent threshold limit value is 50 for 2.4GHz radio and 43 for 5GHz radio.

## AP WLAN state changed

**TABLE 332** AP WLAN state changed event

Event	AP WLAN state changed
Event Type	apWLANStateChanged
Event Code	322
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx" "state"="enable   disable" "ssid"="xxxxx" "apTime"="Tue Apr 22 12:15:00 2014" "reason"="State changed according to service schedule   State changed by administrator"
Displayed on the web interface	AP [{apName&&apMac}] {state} WLAN[{ssid}] on [{apTime}]. Reason: [{reason}].
Description	This event occurs when the WLAN state changes as per the service schedule or as per the service type setting.

## AP capacity reached

**TABLE 333** AP capacity reached event

Event	AP capacity reached
Event Type	apCapacityReached
Event Code	323
Severity	Informational



**TABLE 333** AP capacity reached event (continued)

Event	AP capacity reached
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "radio": "",
Displayed on the web interface	AP [{{apName&&apMac}}] radio [{{radio}}] stopped accepting clients because the client association threshold has been reached.
Description	This event occurs when an AP rejects a client due to the threshold limit reached by the client.

## AP capacity recovered

**TABLE 334** AP capacity recovered event

Event	AP capacity recovered
Event Type	apCapacityRecovered
Event Code	324
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "radio": "",
Displayed on the web interface	AP [{{apName&&apMac}}] radio [{{radio}}] started accepting clients again because current client association is now below the threshold.
Description	This event occurs when the AP starts accepting clients again because the current client association is below the threshold limit.

## AP cable modem interface up

**TABLE 335** AP cable modem interface up event

Event	AP cable modem interface up
Event Type	cableModemUp
Event Code	325
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{{apName&&apMac}}] cable modem interface is up.
Description	This event occurs when the AP cable modem interface is up.

## AP cable modem soft-rebooted by user

**TABLE 336** AP cable modem soft-rebooted by user event

Event	AP cable modem soft-rebooted by user
Event Type	cmResetByUser
Event Code	326
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxx"
Displayed on the web interface	AP [{{apName&&apMac}}] cable modem soft-reboot because of [{{reason}}].
Description	This event occurs when the AP cable modem is softly rebooted because the user executes the soft-reboot CLI command.

## AP cable modem set to factory default by user

**TABLE 337** AP cable modem set to factory default by user event

Event	AP cable modem set to factory default by user
Event Type	cmResetFactoryByUser
Event Code	327
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx";"reason"="xxxxx"
Displayed on the web interface	AP [{apName}&&apMac] cable modem set to factory default because of [{reason}]
Description	This event occurs when AP cable modem is reset to factory default because the user executes the set factory command line interface (CLI) command.

## AP health high latency flag

**TABLE 338** AP health high latency flag event

Event	AP health high latency flag
Event Type	apHealthLatencyFlag
Event Code	328
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current Value"="xxxxx", "configuredThreshold"="xxxxx", "radio" = "X.XG"
Displayed on the web interface	AP [{apName}&&apMac] flagged {{radio}} latency health [{currentValue}] because it crossed the threshold [{configuredThreshold}]
Description	This event occurs when the AP is flagged because the radio has crossed the latency health threshold configured by the administrator.

## AP health low capacity flag

**TABLE 339** AP health low capacity flag event

Event	AP health low capacity flag
Event Type	apHealthCapacityFlag
Event Code	329
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current Value"="xxxxx", "configuredThreshold"="xxxxx", "radio" = "X.XG"
Displayed on the web interface	AP [{apName}&&apMac] flagged {{radio}} capacity health [{currentValue}] because it crossed the threshold [{configuredThreshold}]
Description	This event occurs when the AP is flagged because the radio has crossed the capacity health threshold configured by the administrator.

## AP health high connection failure flag

**TABLE 340** AP health high connection failure flag event

Event	AP health high connection failure flag
Event Type	apHealthConnectionFailureFlag
Event Code	330
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current Value"="xxxxx", "configuredThreshold"="xxxxx", "radio" = "X.XG"
Displayed on the web interface	AP [{apName&&apMac}] flagged {{radio}} capacity health [{currentValue}] because it crossed the threshold [{configuredThreshold}]
Description	This event occurs when AP is flagged because the AP has crossed the connection failure health threshold configured by the administrator.

## AP health high client count flag

**TABLE 341** AP health high client count flag event

Event	AP health high client count flag
Event Type	apHealthClientCountFlag
Event Code	331
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current Value"="xxxxx", "configuredThreshold"="xxxxx",
Displayed on the web interface	AP [{apName&&apMac}] flagged client count health [{currentValue}] because it crossed the threshold [{configuredThreshold}]
Description	This event occurs when an AP is flagged because the AP has crossed the client count health threshold configured by the administrator.

## AP health high latency clear

**TABLE 342** AP health high latency clear event

Event	AP health high latency clear
Event Type	apHealthLatencyClear
Event Code	332
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current Value"="xxxxx", "configuredThreshold"="xxxxx", "radio" = "X.XG",
Displayed on the web interface	AP [{apName&&apMac}] cleared {{radio}} latency health [{currentValue}], which is no longer past the threshold [{configuredThreshold}]
Description	This event occurs when an AP health flag is cleared because it is no longer past the capacity threshold configured by the administrator.

## Events Types

### AP State Change Events

## AP health low capacity clear

**TABLE 343** AP health low capacity clear event

Event	AP health low capacity clear
Event Type	apHealthCapacityClear
Event Code	333
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current Value"="xxxxx", "configuredThreshold"="xxxxx", "radio" = "X.XG"
Displayed on the web interface	AP [{apName&&apMac}] cleared {{radio}} capacity health [{currentValue}], which is no longer past the threshold [{configuredThreshold]}.
Description	This event occurs when an AP's health flag is cleared because it is no longer past the capacity threshold configured by the administrator.

## AP health high connection failure clear

**TABLE 344** AP health high connection failure clear event

Event	AP health high connection failure clear
Event Type	apHealthConnectionFailureClear
Event Code	334
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "currentValue"="xxxxx", "configuredThreshold"="xxxxx", "radio" = "X.XG"
Displayed on the web interface	AP [{apName&&apMac}] flagged {{radio}} connection failure health [{currentValue}], which is no longer past the threshold [{configuredThreshold]}.
Description	This event occurs when an AP's health flag is cleared because it is no longer past the connection failure threshold configured by the administrator.

## AP health high client count clear

**TABLE 345** AP health high client count clear event

Event	AP health high client count clear
Event Type	apHealthClientCountClear
Event Code	335
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "currentValue"="xxxxx", "configuredThreshold"="xxxxx",
Displayed on the web interface	AP [{apName&&apMac}] cleared client count health [{currentValue}], which is no longer past the threshold [{configuredThreshold]}.
Description	This event occurs when an AP's health flag is cleared because it is no longer past the capacity threshold configured by the administrator.

## Primary DHCP AP is down

**TABLE 346** Primary DHCP AP is down event

Event	Primary DHCP AP is down detected by secondary DHCP AP. Starting DHCP service on secondary.
Event Type	apDHCPFailoverDetected
Event Code	336
Severity	Warning
Attribute	"primaryServerMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Primary DHCP server [{primaryServerMac}] is down detected by secondary DHCP server [{apMac}].
Description	This event occurs when the secondary DHCPAP detects that the primary DHCP service has failed and starts the DHCP service.

## Primary DHCP AP is up

**TABLE 347** Primary DHCP AP is up event

Event	Primary DHCP AP is up detected by secondary DHCP AP. Stopping DHCP service on secondary.
Event Type	apDHCPFallbackDetected
Event Code	337
Severity	Informational
Attribute	"primaryServerMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Primary DHCP server [{primaryServerMac}] is up detected by secondary DHCP server [{apMac}].
Description	This event occurs when the secondary DHCP AP detects that primary DHCP AP is UP and stops DHCP service.

## Secondary DHCP AP is down

**TABLE 348** Secondary DHCP AP is down event

Event	Secondary DHCP AP is down detected by primary DHCPAP.
Event Type	apSecondaryDHCPAPDown
Event Code	338
Severity	Major
Attribute	"secondaryServerMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Secondary DHCP server [{secondaryServerMac}] is down detected by primary DHCP server [{apMac}].
Description	This event occurs when the primary DHCP AP detects that the secondary DHCP AP is down.

## Events Types

### AP State Change Events

## Secondary DHCP AP is up

**TABLE 349** Secondary DHCP AP is up event

Event	Secondary DHCP AP is up detected by primary DHCP AP.
Event Type	apSecondaryDHCPAPUp
Event Code	339
Severity	Informational
Attribute	"secondaryServerMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Secondary DHCP server [{secondaryServerMac}] is up detected by primaryDHCP server [{primaryServerMac}].
Description	This event occurs when the primary DHCP AP detects that secondary DHCP AP is UP.

## Primary or secondary DHCP AP detects 90% of the configured total IPs

**TABLE 350** Primary or secondary DHCP AP detects 90% of the configured total IPs event

Event	Primary or secondary DHCP AP detects 90% of the configured total IPs
Event Type	apDHCIIPPoolMaxThresholdReached
Event Code	340
Severity	Warning
Attribute	"zoneName"="ZoneName", "poolId"="xxx", "vlanId"="1", "allocatedIPNum"="5", "totalIPNum"="10", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	In zone [{zoneName}] DHCP IP pool [{poolId}] reached 90% threshold detected by AP MAC [{apMac}]. VLAN ID: [{vlanId}] Allocated IPs: [{allocatedIPNum}], Total IPs: [{totalIPNum}].
Description	This event occurs when the primary or secondary DHCP AP reports that the IP pool has reached 90% of the total number of allocated IP addresses.

## Both primary and secondary DHCP server APs are down

**TABLE 351** Both primary and secondary DHCP server APs are down event

Event	Both primary and secondary DHCP server APs are down
Event Type	apDHCPServiceFailure
Event Code	341
Severity	Critical
Attribute	"primaryServerMac"="xx:xx:xx:xx:xx:xx", "secondaryServerMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP DHCP service failure . Both primary DHCP AP [{primaryServerMac}] and secondary DHCP server AP [{secondaryServerMac}] are down.
Description	This event occurs when the controller detects that the primary and secondary DHCP APs have failed.

## AP NAT gateway IP failover detected for particular VLAN pool

**TABLE 352** AP NAT gateway IP failover detected for particular VLAN pool event

Event	AP NAT gateway IP failover detected for particular VLAN pool
Event Type	apNATFailoverDetected

**TABLE 352** AP NAT gateway IP failover detected for particular VLAN pool event (continued)

Event	AP NAT gateway IP failover detected for particular VLAN pool
Event Code	342
Severity	Major
Attribute	"natGatewayIP"="10.1.2.2", "vlanId"="2", "natGatewayMac"="xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	NAT failover detected for {{natGatewayIP}}, VLAN {{vlanId}}, AP {{natGatewayMac}}. Bringing up interface and switching traffic to AP {{apMac}}.
Description	This event occurs when any NAT gateway AP detects that a monitored NAT gateway IP has failed.

## AP NAT gateway IP fall back detected for particular VLAN pool

**TABLE 353** AP NAT gateway IP fall back detected for particular VLAN pool event

Event	AP NAT gateway IP fall back detected for particular VLAN pool
Event Type	apNATFallbackDetected
Event Code	343
Severity	Informational
Attribute	"vlanId"="1", "natGatewayMac"="xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	NAT fallback detected for VLAN {{vlanId}} by AP {{apMac}}. Bringing down interface and switching traffic to AP {{natGatewayMac}}.
Description	This event occurs when any NAT gateway AP detects that other monitored NAT gateway AP IP is up.

## NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool

**TABLE 354** NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool event

Event	NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool
Event Type	apNATVlanCapacityAffected
Event Code	344
Severity	Critical
Attribute	"natGatewayIP1"=192.168.10.2", "natGatewayIP2"=192.168.10.3", "nat GatewayIP3"=192.168.10.4", "vlanId"="2", "apMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	NAT VLAN capacity affected is detected by NAT gateway AP {{apMac}} since three (3) consecutive NAT gateway IPs {{natGatewayIP1&&natGatewayIP2&&natGatewayIP3}} are down. The NAT traffic for some of the clients may get affected for VLAN {{vlanId}}.
Description	This event occurs when NAT VLAN capacity affected is detected by NAT gateway AP at zone. This is due to three (3) consecutive NAT gateway AP IP failure for a particular VLAN pool.

## NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up

**TABLE 355** NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up event

Event	NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up
Event Type	apNATVlanCapacityRestored
Event Code	345
Severity	Informational
Attribute	"natGatewayIP"="192.168.10.2", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	NAT VLAN capacity restored detected by DHCP NAT AP [{apMac}] one of the NAT gateway IPs [{natGatewayIP}] is now up, out of three (3) consecutive NAT gateway IPs which were down. The NAT traffic for affected clients is restored back.
Description	This event occurs when the AP detects at least one of the three (3) consecutive gateway APs IPs that had failed is now UP.

## AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down

**TABLE 356** AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down event

Event	AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down
Event Type	apNATFailureDetectedbySZ
Event Code	346
Severity	Critical
Attribute	"apMac1"="xx:xx:xx:xx:xx:xx", "apMac2"="xx:xx:xx:xx:xx:xx", "apMac3"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	NAT failure detected by SZ since three (3) consecutive NAT gateway IPs are down AP1=[{apMac1}] AP2=[{apMac2}] AP3=[{apMac3}] (All consecutive NAT APs are down in case of less than 3 NAT Gateway APs configured). The NAT traffic for some of the clients may get affected for the respective VLANs.
Description	This event occurs when the controller detects three (3) consecutive failures of NAT server APs.

## AP health high airtime utilization flag

**TABLE 357** AP health high airtime utilization flag event

Event	AP health high airtime utilization flag
Event Type	apHealthAirUtilizationFlag
Event Code	347
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "currentValue"="xxxxx", "configuredThreshold"="xxxxx", "radio"="X.XG"
Displayed on the web interface	AP [{apName}&&apMac}] flagged [{radio}] airtime utilization health [{currentValue}] because it crossed the threshold [{configuredThreshold}]



**TABLE 357** AP health high airtime utilization flag event (continued)

Event	AP health high airtime utilization flag
Description	This event occurs when an AP is flagged because the radio has crossed the latency health threshold configured by the administrator.

## AP health high airtime utilization clear

**TABLE 358** AP health high airtime utilization clear event

Event	AP health high airtime utilization clear
Event Type	apHealthAirUtilizationClear
Event Code	348
Severity	Informational
Attribute	"apName"="xxxx", "apMac"="xx:xx:xx:xx:xx:xx", "currentValue"="xxxx", "configuredThreshold"="xxxx", "radio"="X.XG"
Displayed on the web interface	AP [{apName}&&apMac]} cleared [{radio}] airtime utilization health [{currentValue}], which is no longer past the threshold [{configuredThreshold]}.
Description	This event occurs when an AP's health flag is cleared because it is no longer past the latency threshold configured by the administrator.

## AP cluster failover

**TABLE 359** AP cluster failover event

Event	AP cluster failover
Event Type	apClusterFailover
Event Code	349
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "oldWsgIP"="xxx.xxx.xxx.xxx", "newWsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName}&&apMac]} on zone [{zoneName}] is failover from {produce.short.name} [{oldCpName}   {oldWsgIP}] to {produce.short.name} [{cpName}   {newWsgIP}].
Description	This event occurs when an AP executes the failover from the original cluster to a new cluster.

## AP cluster rehome

**TABLE 360** AP cluster rehome event

Event	AP cluster rehome
Event Type	apRehomeFailover
Event Code	350
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "oldWsgIP"="xxx.xxx.xxx.xxx", "newWsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName}&&apMac]} on zone [{zoneName}] is rehomed from {produce.short.name} [{oldCpName}   {oldWsgIP}] to {produce.short.name} [{cpName}   {newWsgIP}].

## Events Types

### AP State Change Events

**TABLE 360** AP cluster rehome event (continued)

Event	AP cluster rehome
Description	This event occurs when an AP is rehomed from a standby to a primary cluster.

## AP switchover cluster failed

**TABLE 361** AP switchover cluster failed event

Event	AP switchover cluster failed
Event Type	apSwitchoverFailed
Event Code	352
Severity	Minor
Attribute	apName="xxxx" apMac="xx:xx:xx:xx:xx:xx" ip="xx.xx.xx.xx" reason="xxxxxxxxx"
Displayed on the web interface	AP [{apName&&apMac}] failed to switchover to another cluster [{ip}] because of [{reason}]
Description	This event occurs when an AP fails to switchover to the target cluster.

## AP MAC OUI violation

**TABLE 362** AP MAC OUI violation

Event	AP MAC OUI violation
Event Type	AP MAC OUI violation
Event Code	1294
Severity	Major
Attribute	AP Name, AP MAC
Displayed on the web interface	APName @ AP MAC
Description	This event occurs when an approved AP is rejected due to violation of AP MAC OUI (Organization Unique ID) rule.

## Backhaul switched to primary

**TABLE 363** Backhaul switched to primary event

Event	Backhaul switched to primary
Event Type	changeToPrimaryBackhaul
Event Code	9100
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currBackhaul = "eth0"
Displayed on the web interface	AP [{apName&&apMac}] Backhaul switched to primary - [{currBackhaul}]
Description	This event occurs when Backhaul switched to primary.

## Backhaul switched to secondary

**TABLE 364** Backhaul switched to secondary event

Event	Backhaul switched to secondary
Event Type	changeToSecondaryBackhaul
Event Code	9101
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currBackhaul = "SIM 1"
Displayed on the web interface	AP [{apName&&apMac}] Backhaul switched to secondary - [{currBackhaul}]
Description	This event occurs when Backhaul switched to secondary.

## LTE network connectivity lost

**TABLE 365** LTE network connectivity lost event

Event	LTE network connectivity lost
Event Type	lteConnectivityFailed
Event Code	9102
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0"
Displayed on the web interface	AP [{apName&&apMac}] LTE network connectivity lost on [{currSim}]
Description	This event occurs when LTE network connectivity is lost.

## Ethernet network connectivity lost

**TABLE 366** Ethernet network connectivity lost vent

Event	Ethernet network connectivity lost
Event Type	ethernetConnectivityFailed
Event Code	9103
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", curriface = "eth0"
Displayed on the web interface	AP [{apName&&apMac}] Ethernet network connectivity lost on [{curriface}]
Description	This event occurs when Ethernet network connectivity is lost.

## LTE DHCP timeout

**TABLE 367** LTE DHCP timeout event

Event	LTE DHCP timeout
Event Type	lteDhcpTimeout
Event Code	9104
Severity	Informational

## Events Types

### AP State Change Events

**TABLE 367** LTE DHCP timeout event (continued)

Event	LTE DHCP timeout
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 1"
Displayed on the web interface	AP [{apName&&apMac}] LTE DHCP timeout on [{currSim}]
Description	This event occurs when LTE DHCP timeout.

## Ethernet link down

**TABLE 368** Ethernet link down event

Event	Ethernet link down
Event Type	ethernetLinkDown
Event Code	9105
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", curriface = "eth1"
Displayed on the web interface	AP [{apName&&apMac}] Ethernet link down on [{curriface}]
Description	This event occurs when Ethernet link is down.

## Ethernet link up

**TABLE 369** Ethernet link up event

Event	Ethernet link up
Event Type	ethernetLinkUp
Event Code	9106
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", curriface = "eth0"
Displayed on the web interface	AP [{apName&&apMac}] Ethernet link up on [{curriface}]
Description	This event occurs when Ethernet link is up.

## SIM switch

**TABLE 370** SIM switch event

Event	SIM switch
Event Type	simSwitch
Event Code	9107
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 1"
Displayed on the web interface	AP [{apName&&apMac}] Cellular connection switched to [{currSim}]
Description	This event occurs when SIM is switched.

## Remote host blacklisted

**TABLE 371** Remote host blacklisted event

Event	Remote host blacklisted
Event Type	remoteHostBlacklisted
Event Code	9108
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", remotehosturl = "www.ruckus.wireless.com", remotehostport = "8443"
Displayed on the web interface	AP [{apName&&apMac}] Unable to reach [{remotehosturl}]/[{remotehostport}] and hence blacklisted
Description	This event occurs when remote host is blacklisted.

## SIM removal

**TABLE 372** SIM removal event

Event	SIM removal
Event Type	simRemoval
Event Code	9109
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0"
Displayed on the web interface	AP [{apName&&apMac}] [{currSim}] removed
Description	This event occurs when SIM is removed.

## LTE network registration status

**TABLE 373** LTE network registration status event

Event	LTE network registration status
Event Type	lteNetworkRegistrationStatus
Event Code	9110
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currNwRegStatus = "Registered with home network"
Displayed on the web interface	AP [{apName&&apMac}] [{currSim}] Cellular network status - [{currNwRegStatus}]
Description	This event occurs whenever there is a change in the LTE network registration status.

## LTE connection status

**TABLE 374** LTE connection status event

Event	LTE connection status
Event Type	lteConnectionStatus
Event Code	9111

## Events Types

### AP State Change Events

**TABLE 374** LTE connection status event (continued)

Event	LTE connection status
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currConnStatus = "3G"
Displayed on the web interface	AP [{apName}&&apMac] [{currSim}] Cellular connection status - [{currConnStatus}]
Description	This event occurs whenever there is a change in the LTE connection status.

## LTE good rssi status

**TABLE 375** LTE good rssi status event

Event	LTE good rssi status
Event Type	lteGoodRssiStatus
Event Code	9112
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currRssiStatus = "good"
Displayed on the web interface	AP [{apName}&&apMac] [{currSim}] Cellular signal strength is [{currRssiStatus}] now
Description	This event occurs whenever there is a change in the RSSI from weak to good.

## LTE weak rssi status

**TABLE 376** LTE weak rssi status event

Event	LTE weak rssi status
Event Type	lteWeakRssiStatus
Event Code	9113
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currRssiStatus = "weak"
Displayed on the web interface	AP [{apName}&&apMac] [{currSim}] Cellular signal strength is [{currRssiStatus}] now
Description	This event occurs whenever there is a change in the RSSI from good to weak.

## AP client load balancing limit reached

**TABLE 377** AP client load balancing limit reached event

Event	AP client load balancing limit reached
Event Type	apCLBCapacityLimitReached
Event Code	9114
Severity	Informational
Attribute	"apMac" = "xx:xx:xx:xx:xx:xx", "nbrAvlCapAvg" = "1000", "localAvlCap" = "1100", "wifiInterface"="2.4G WLANs"
Displayed on the web interface	AP [RuckusAP@EC:8C:A2:26:06:F0] reached the capacity limit, localAvlCap=1000, nbrAvlCapAvg=900 on WLAN [2.4G WLANs]

**TABLE 377** AP client load balancing limit reached event (continued)

Event	AP client load balancing limit reached
Description	This event is raised by AP when the capacity of the AP is less than the average of the neighbor AP's capacity.

## AP client load balancing limit recovered

**TABLE 378** AP client load balancing limit recovered event

Event	AP client load balancing limit recovered
Event Type	apCLBCapacityLimitRecovered
Event Code	9115
Severity	Informational
Attribute	apMac = "xx:xx:xx:xx:xx:xx", "nbrAvlCapAvg" = "1100", "localAvlCap" = "1000", "wifiInterface"="2.4G WLANs"
Displayed on the web interface	AP [RuckusAP@EC:8C:A2:26:06:F0] recovered the capacity limit, localAvlCap=800, nbrAvlCapAvg=1000 on WLAN [2.4G WLANs].
Description	This event is raised by AP when the capacity of the AP is more than the average of the neighbor AP's capacity.

## AP System Anomaly

**TABLE 379** AP System Anomaly event

Event	AP System Anomaly
Event Type	apWritableRO
Event Code	285
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "apName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] /writable partition is mounted as Read-Only
Description	This event is triggered when AP /writable partition is mounted as Read-Only

## AP USB Events

Following are the events related to AP USB (Universal Serial Bus).

- [AP USB software package downloaded](#) on page 191
- [AP USB software package download failed](#) on page 192

## AP USB software package downloaded

**TABLE 380** AP USB software package downloaded event

Event	AP USB software package downloaded
Event Type	apUsbSoftwarePackageDownloaded
Event Code	370

## Events Types

### Authentication Events

**TABLE 380** AP USB software package downloaded event (continued)

Event	AP USB software package downloaded
Severity	Informational
Attribute	"apMac="xx:xx:xx:xx:xx:xx", "usbSoftwareName="19d2-fff5(v1.0)"
Displayed on the web interface	AP [{apName&&apMac}] downloaded USB software package [{usbSoftwareName}] successfully.
Description	This event occurs when AP successfully downloads its USB software package.

## AP USB software package download failed

**TABLE 381** AP USB software package download failed event

Event	AP USB software package download failed
Event Type	apUsbSoftwarePackageDownloadFailed
Event Code	371
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx", usbSoftwareName="19d2-fff5(v1.0)"
Displayed on the web interface	AP [{apName&&apMac}] failed to download USB software package [{usbSoftwareName}]
Description	This event occurs when the AP fails to download its USB software package.

## Authentication Events

The following are the events related to authentication.

- [Authentication server not reachable](#) on page 193
- [Unknown realm](#) on page 193
- [Authentication succeeded](#) on page 193
- [Authentication failed](#) on page 194
- [Pseudonym authentication succeeded](#) on page 194
- [Pseudonym authentication failed](#) on page 194
- [Fast re-authentication succeeded](#) on page 195
- [Fast re-authentication failed](#) on page 195
- [Authentication failed over to secondary](#) on page 196
- [Authentication fallback to primary](#) on page 196
- [AD/LDAP connected successfully](#) on page 196
- [AD/LDAP connectivity failure](#) on page 197
- [Bind fails with AD/LDAP](#) on page 197
- [Bind success with LDAP, but unable to find clear text password for the user](#) on page 197
- [RADIUS fails to connect to AD NPS server](#) on page 198
- [RADIUS fails to authenticate with AD NPS server](#) on page 198
- [Successfully established the TLS tunnel with AD/LDAP](#) on page 198
- [Fails to establish TLS tunnel with AD/LDAP](#) on page 199



## Authentication server not reachable

**TABLE 382** Authentication server not reachable event

Event	Authentication server not reachable
Event Type	authSrvrNotReachable
Event Code	1601
Severity	Major
Attribute	"mvnold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.3gppnetwork.org" "radProxyIp"="7.7.7.7" "authSrvrIp"="20.20.20.20" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the authentication fails since the primary or secondary servers are not reachable.

## Unknown realm

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 383** Unknown realm event

Event	Unknown realm
Event Type	unknownRealm
Event Code	1603
Severity	Debug
Attribute	"mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.3gppnetwork.org"
Displayed on the web interface	Realm [{realm}] could not be resolved to a AAA server
Description	This event occurs when the authentication realm resolution fails.

## Authentication succeeded

**TABLE 384** Authentication succeeded event

Event	Authentication succeeded
Event Type	authSuccess
Event Code	1604
Severity	Debug
Attribute	"mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdN"="98787" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdN}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS accept is sent back to the AP. This event applies only for TTG/PDG session.  Note: The attribute Permanent ID is used for authentication.

## Authentication failed

**TABLE 385** Authentication failed event

Event	Authentication failed
Event Type	authFailed
Event Code	1605
Severity	Debug
Attribute	"mvpnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImei"="12345", "ueMsisdn"="98787", "cause"="<Cause of failure>" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Authentication failed for UE with IMSI [{ueImei}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back and the MS-ISDN is provided (if available).  Note: The attribute Permanent ID is used for authentication.

## Pseudonym authentication succeeded

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 386** Pseudonym authentication succeeded event

Event	Pseudonym authentication succeeded
Event Type	pseudonymAuthSuccess
Event Code	1606
Severity	Debug
Attribute	"mvpnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImei"="12345", "ueMsisdn"="98787" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Pseudonym ID based authentication successful for UE with IMSI [{ueImei}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS accept is sent back to the AP. This event is applicable when the controller acts as a host AAA server and is applicable only for TTG/PDG session.  <b>Note:</b> The attribute <b>Pseudonym ID</b> is used for authentication.

## Pseudonym authentication failed

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 387** Pseudonym authentication failed event

Event	Pseudonym authentication failed
Event Type	pseudonymAuthFailed
Event Code	1607
Severity	Debug

**TABLE 387** Pseudonym authentication failed event (continued)

Event	Pseudonym authentication failed
Attribute	"mvsidn"=12 "wlanid"=1 "zoneid"=10 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"= radiusd "realm"=wlan.3gppnetwork.org "SCGMgmtIp"=2.2.2.2 "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "cause"="<Cause of failure>" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Pseudonym ID based authentication failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back for pseudonym authentication. This event is applicable when the controller acts as a host AAA server. The mobile subscriber integrated services digital network number (MS-ISDN) is provided (if available).  <b>Note:</b> The attribute <b>Pseudonym ID</b> is used for authentication.

## Fast re-authentication succeeded

### NOTE

This event is not applicable for vSZ-H.

**TABLE 388** Fast re-authentication succeeded event

Event	Fast re-authentication succeeded
Event Type	fastReauthSuccess
Event Code	1608
Severity	Debug
Attribute	"mvsidn"=12 "wlanid"=1, "zoneid"=10 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"= radiusd "realm"=wlan.3gppnetwork.org "SCGMgmtIp"=2.2.2.2 "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Fast re-auth ID based authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs after resending RADIUS accept back to AP. This event is applicable when, the {produce.short.name} acts as a hosted AAA server and for TTG/PDG session.  <b>Note:</b> <b>FastReauth ID</b> is used for authentication.

## Fast re-authentication failed

### NOTE

This event is not applicable for vSZ-H.

**TABLE 389** Fast re-authentication failed event

Event	Fast re-authentication failed
Event Type	fastReauthFailed
Event Code	1609
Severity	Debug
Attribute	"mvsidn"=12 "wlanid"=1, "zoneid"=10 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"= radiusd "realm"=wlan.3gppnetwork.org "SCGMgmtIp"=2.2.2.2 "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "cause"="<Cause of failure>" "authType"="EAP-SIM/AKA"

## Events Types

### Authentication Events

**TABLE 389** Fast re-authentication failed event (continued)

Event	Fast re-authentication failed
Displayed on the web interface	Fast re-auth ID based authentication failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back for fast reauthentication. This event applies when the controller acts as a host AAA server. The MS-ISDN is provided (if available). <b>Note:</b> Attribute <b>FastReauthID</b> is used for reauthentication.

## Authentication failed over to secondary

**TABLE 390** Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651
Severity	Major
Attribute	"mvsold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the secondary authentication RADIUS server is available after the primary server becomes zombie or dead.

## Authentication fallback to primary

**TABLE 391** Authentication fallback to primary event

Event	Authentication fallback to primary
Event Type	authFallbackToPrimary
Event Code	1652
Severity	Major
Attribute	"mvsold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the automatic fallback is enabled. The authentication failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.

## AD/LDAP connected successfully

**TABLE 392** AD/LDAP connected successfully event

Event	AD/LDAP connected successfully
Event Type	racADLDAPSuccess
Event Code	1751

**TABLE 392** AD/LDAP connected successfully event (continued)

Event	AD/LDAP connected successfully
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1"  "SCGMgmtIp"="2.2.2.2", "desc"="Successful connection to AD/LDAP"
Displayed on the web interface	{{srcProcess}} Connect to AD/LDAP{{authSrvrIp}} successfully from SCG{{SCGMgmtIp}}
Description	This event occurs when RADIUS connection to AD/LDAP server is successful.

## AD/LDAP connectivity failure

**TABLE 393** AD/LDAP connectivity failure event

Event	AD/LDAP connectivity failure
Event Type	racADLDAPFail
Event Code	1752
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "SCGMgmtIp"="2.2.2.2"  "desc"="Connection to AD/LDAP fails"
Displayed on the web interface	{{srcProcess}} Connect to AD/LDAP{{authSrvrIp}} fails from SCG{{SCGMgmtIp}}
Description	This event occurs when RADIUS fails to connect to AD/LDAP server.

## Bind fails with AD/LDAP

**TABLE 394** Bind fails with AD/LDAP event

Event	Bind fails with AD/LDAP
Event Type	racADLDAPBindFail
Event Code	1753
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Bind to AD/LDAP fails"
Displayed on the web interface	{{srcProcess}} Bind to AD/LDAP{{authSrvrIp}} fails from SCG{{SCGMgmtIp}} for User{{userName}}
Description	This event occurs when RADIUS binding fails to AD/LDAP server.

## Bind success with LDAP, but unable to find clear text password for the user

**TABLE 395** Bind success with LDAP, but unable to find clear text password for the user event

Event	Bind success with LDAP but unable to find clear text password for the user
Event Type	racLDAPFailToFindPassword
Event Code	1754

## Events Types

### Authentication Events

**TABLE 395** Bind success with LDAP, but unable to find clear text password for the user event (continued)

Event	Bind success with LDAP but unable to find clear text password for the user
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Fail to find password"
Displayed on the web interface	{{srcProcess}} failed to find password from LDAP {{authSrvrIp}} for SCG{{SCGMgmtIp}} for User{{userName}}
Description	This event occurs when binding is successful with LDAP using root credential but is unable to retrieve the clear text password for the user.

## RADIUS fails to connect to AD NPS server

**TABLE 396** RADIUS fails to connect to AD NPS server event

Event	RADIUS fails to connect to AD NPS server
Event Type	racADNPSFail
Event Code	1755
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Fails to connect to AD NPS server"
Displayed on the web interface	{{srcProcess}} Fails to connect to AD NPS {{authSrvrIp}} from SCG{{SCGMgmtIp}}
Description	This event occurs when RADIUS fails to connect to AD NPS server.

## RADIUS fails to authenticate with AD NPS server

**TABLE 397** RADIUS fails to authenticate with AD NPS server event

Event	RADIUS fails to authenticate with AD NPS server
Event Type	racADNPSFailToAuthenticate
Event Code	1756
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SCGMgmtIp"="2.2.2.2", "desc"="Fails to authenticate with AD NPS"
Displayed on the web interface	{{srcProcess}} Fails to authenticate AD NPS{{authSrvrIp}} on SCG {{SCGMgmtIp}} for User{{userName}}
Description	This event occurs when RADIUS fails to authenticate with AD NPS server.

## Successfully established the TLS tunnel with AD/LDAP

**TABLE 398** Successfully established the TLS tunnel with AD/LDAP event

Event	Successfully established the TLS tunnel with AD/LDAP
Event Type	racADNPSFailToAuthenticate

**TABLE 398** Successfully established the TLS tunnel with AD/LDAP event (continued)

Event	Successfully established the TLS tunnel with AD/LDAP
Event Code	1761
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="radiusd", "authSrvrIp"="1.1.1.1", "authSrvrPort"="636" "SCGMgmtIp"="2.2.2.2", "desc"="Successfully established TLS Tunnel with LDAP/AD"
Displayed on the web interface	{{srcProcess}} Established the TLS connection with AD/LDAP{{authSrvrIp}} successfully from SCG{{SCGMgmtIp}}
Description	This event occurs when the TLS connection between the controller and AD/LDAP is successfully established.

## Fails to establish TLS tunnel with AD/LDAP

**TABLE 399** Fails to establish TLS tunnel with AD/LDAP event

Event	Fails to establish TLS tunnel with AD/LDAP
Event Type	racADLDAPTLSFailed
Event Code	1762
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12 "srcProcess"="radiusd", "authSrvrIp"="1.1.1.1" "authSrvrPort"="636", "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish TLS Tunnel with LDAP/AD"
Displayed on the web interface	{{srcProcess}} Establishes the TLS connection with AD/LDAP{{authSrvrIp}} fails from SCG{{SCGMgmtIp}}
Description	This event occurs when the TLS connection between the controller and AD/LDAP fails.
Auto Clearance	This event triggers the alarm 1762, which is auto cleared by the event code 1761.

## TLS Establishment Failed between SZ and external AAA Server

**TABLE 400** TLS Establishment Failed between SZ and external AAA Server event

Event	TLS Establishment Failed between SZ and external AAA Server
Event Type	racTLSEstablishmentFailedBetweenSZandExternalAAAServer
Event Code	1763
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish "
Displayed on the web interface	{{srcProcess}} Establishes the TLS connection fails between SZ and external AAA Server from SCG{{SCGMgmtIp}}
Description	This event is triggered when TLS connection between the controller and AD/LDAP fails.

## Authorization Events

The following are the events related to authorization (DM/CoA).

- [DM received from AAA](#) on page 200
- [DM NACK sent to AAA](#) on page 200
- [DM sent to NAS](#) on page 201
- [DM NACK received from NAS](#) on page 201
- [CoA received from AAA](#) on page 201
- [CoA NACK sent to AAA](#) on page 202
- [CoA sent NAS](#) on page 202
- [CoA NAK received NAS](#) on page 202
- [CoA authorize only access reject](#) on page 203
- [CoA RWSG MWSG notification failure](#) on page 203

### DM received from AAA

**TABLE 401** DM received from AAA event

Event	DM received from AAA
Event Type	dmRcvdAAA
Event Code	1641
Severity	Debug
Attribute	"mvnoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "rmtRadSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM received by RAC [{radSrvrIp}] from AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when the radio access controller (RAC) receives a disconnected message from the AAA server.

### DM NACK sent to AAA

**TABLE 402** DM NACK sent to AAA event

Event	DM NACK sent to AAA
Event Type	dmNackSntAAA
Event Code	1642
Severity	Debug
Attribute	"mvnoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "rmtRadSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected not acknowledged message to the AAA server.



## DM sent to NAS

**TABLE 403** DM sent to NAS event

Event	DM sent to NAS
Event Type	dmSntNAS
Event Code	1643
Severity	Debug
Attribute	"mvnoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "nasIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM sent to NAS [{rmtRadSrvrIp}] by RAC [{radSrvrIp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected message to the network access server [proxy of received disconnected message or the disconnected message as initiated by the controller].

## DM NACK received from NAS

**TABLE 404** DM NACK received from NAS event

Event	DM NACK received from NAS
Event Type	dmNackRcvdNAS
Event Code	1644
Severity	Debug
Attribute	"mvnoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "nasIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2", "cause"=""
Displayed on the web interface	RADIUS DM NACK received by RAC [{radSrvrIp}] from NAS [{nasIp}] for [{userName}]
Description	This event occurs when the radio access control receives disconnect message, which is not acknowledged from the NAS server.

## CoA received from AAA

**TABLE 405** CoA received from AAA event

Event	CoA received from AAA
Event Type	coaRcvdAAA
Event Code	1645
Severity	Debug
Attribute	"mvnoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "rmtRadSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA received by RAC [{radSrvrIp}] from AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control receives a change of authorization message from the AAA server.

## CoA NACK sent to AAA

**TABLE 406** CoA NACK sent to AAA event

Event	CoA NACK sent to AAA
Event Type	coaNackSntAAA
Event Code	1646
Severity	Debug
Attribute	"mvpnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "rmtRadSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control sends a change of authorization, not acknowledged to the AAA server.

## CoA sent NAS

**TABLE 407** CoA sent NAS event

Event	CoA sent NAS
Event Type	coaSentNas
Event Code	1647
Severity	Debug
Attribute	"mvpnold"="12" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "userName"="abc@xyz.com" "radSrvrIp"="1.1.1.1" "nasIp"="3.3.3.3" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA requests proxied/forwarded to NAS(AP) [{nasIp]}.
Description	This event occurs when the controller forwards/proxy of change of authorization to the NAS server.

## CoA NAK received NAS

**TABLE 408** CoA NAK received NAS event

Event	CoA NAK received NAS
Event Type	coaNakRcvdNas
Event Code	1648
Severity	Debug
Attribute	"mvpnold"="12" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "userName"="abc@xyz.com" "radSrvrIp"="1.1.1.1" "nasIp"="3.3.3.3" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA NAK received from NAS(AP) for forwarded/proxied CoA [{radSrvrIp}]
Description	This event occurs when a change of authorization, not acknowledged is received from the NAS server.

## CoA authorize only access reject

**TABLE 409** CoA authorize only access reject event

Event	CoA authorize only access reject
Event Type	coaAuthorizeOnlyAccessReject
Event Code	1649
Severity	Critical
Attribute	"mvnold"="12" "wlanId"="1", "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787", "rmtRadSrvrIp"="40.40.40.40"
Displayed on the web interface	CoA Authorize Only unsuccessful for AAA Server [rmtRadSrvrIp] for UE [ueMacAddr]
Description	This event occurs when the change of authorization is rejected.

## CoA RWSG MWSG notification failure

**TABLE 410** CoA RWSG MWSG notification failure event

Event	CoA RWSG MWSG notification failure
Event Type	coaRWSGMWSGNotifFailure
Event Code	1650
Severity	Major
Attribute	mvnold"=12 "wlanId"=1 "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "userName"=abc@xyz.com "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "apType" =" " "ueMacAddr"="aa:bb:cc:gg:hh:ii"
Displayed on the web interface	Session Modify MWSG-RWSG Notification Failure/No response received
Description	This event occurs when the change of authorization in RADIUS /metro wireless service gateway notification fails.

## Control and Data Plane Interface

### NOTE

This event is not applicable for vSZ-H.

Following are the events related to control and data plane events.

- [DP connected](#) on page 204
- [GtpManager \(DP\) disconnected](#) on page 204
- [Session updated at DP](#) on page 204
- [Session update at DP failed](#) on page 205
- [Session deleted at DP](#) on page 205
- [Session delete at DP failed](#) on page 205
- [C2d configuration failed](#) on page 206

## DP connected

**TABLE 411** DP connected event

Event	DP connected
Event Type	connectedToDblade
Event Code	1201
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="NA", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	The connectivity between Control plane {{ctrlBladeIp}} and Data plane {{dataBladeIp}} is established at {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when control plane completes the configuration procedure successfully.

## GtpManager (DP) disconnected

**TABLE 412** GtpManager (DP) disconnected event

Event	GtpManager (DP) disconnected
Event Type	lostCnxnToDblade
Event Code	1202
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="NA", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	The connectivity between Control plane {{ctrlBladeIp}} and Data plane {{dataBladeIp}} is lost at {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when either the transmission control protocol connection is lost or when the control plane is unable to complete the configuration procedure.
Auto Clearance	This event triggers the alarm 1202, which is auto cleared by the event code 1201.

## Session updated at DP

**TABLE 413** Session updated at DP event

Event	Session updated at DP
Event Type	sessUpdatedAtDblade
Event Code	1205
Severity	Debug
Attribute	"mvsid"="12", "wlanId"="1", "zoneId"="10", "srcProcess"="aut", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "realm"="realm sent by UE", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI {{ueImsi}} and MSISDN {{ueMsisdn}} has been updated at Data plane {{dataBladeIp}} by Control plane {{ctrlBladeIp}} at {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when the session updates the request (C-D-SESS-UPD-REQ) successfully.

## Session update at DP failed

**TABLE 414** Session update at DP failed event

Event	Session update at DP failed
Event Type	sessUpdateErrAtDblade
Event Code	1206
Severity	Debug
Attribute	"mvnoid"="12", "wlanId"="1", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "zoneId"="10", "realm"="realm sent by UE", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to update at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session update request fails (C-D-SESS-UPD-REQ). This is either due to a request timeout or a failed response.

## Session deleted at DP

**TABLE 415** Session deleted at DP event

Event	Session deleted at DP
Event Type	sessDeletedAtDblade
Event Code	1207
Severity	Debug
Attribute	"mvnoid"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="realm sent by UE", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been deleted from Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session deletes request (C-D-SESS-DEL-REQ) is successfully acknowledged.

## Session delete at DP failed

**TABLE 416** Session delete at DP failed event

Event	Session delete at DP failed
Event Type	sessDeleteErrAtDblade
Event Code	1208
Severity	Debug
Attribute	"mvnoid"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="realm sent by UE", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"

**TABLE 416** Session delete at DP failed event (continued)

Event	Session delete at DP failed
Displayed on the web interface	TTG/PDG session for UE with IMSI [{{ueImsi}}] and MSISDN [{{ueMsisdn}}] has failed to delete from Data plane [{{dataBladeIp}}] by Control plane [{{ctrlBladeIp}}] at {produce.short.name} [{{SCGMgmtIp}}]
Description	This event occurs when the session delete request (C-D-SESS-DEL-REQ) results in a timeout or a failed response.

## C2d configuration failed

**TABLE 417** C2d configuration failed event

Event	C2d configuration failed
Event Type	c2dCfgFailed
Event Code	1209
Severity	Warning
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="NA" "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "cause"="<what was configured>"
Displayed on the web interface	Configuration [{{cause}}] from Control plane [{{ctrlBladeIp}}] failed to apply on Data plane [{{dataBladeIp}}] at {produce.short.name} [{{SCGMgmtIp}}]
Description	This event occurs when the configuration request (C-D-CFG-REQ) results in a timeout or a failed response.

## Client Events

All client events from the AP will be appended with tenant ID ("tenantUUID":"xxxx"). Following are the events related to clients:

- [Client authentication failed](#) on page 207
- [Client joined](#) on page 208
- [Client failed to join](#) on page 208
- [Client disconnected](#) on page 208
- [Client connection timed out](#) on page 209
- [Client authorization successfully](#) on page 209
- [Client authorization failed](#) on page 210
- [Client session expired](#) on page 210
- [Client roaming](#) on page 210
- [Client logged out](#) on page 211
- [3rd party client join](#) on page 211
- [3rd party client inactivity timeout](#) on page 212
- [3rd party client authorization](#) on page 212
- [3rd party client authorization failure](#) on page 212
- [3rd party client session expiration](#) on page 213
- [3rd party client roaming](#) on page 213

- [3rd party client session logout](#) on page 214
- [Client roaming disconnected](#) on page 214
- [Client blocked](#) on page 214
- [Client grace period](#) on page 215
- [Onboarding registration succeeded](#) on page 215
- [Onboarding registration failed](#) on page 215
- [Remediation succeeded](#) on page 216
- [Remediation failed](#) on page 216
- [Force DHCP disconnected](#) on page 216
- [WDS device joined](#) on page 217
- [WDS device left](#) on page 217
- [Client is blocked because of barring UE rule](#) on page 217
- [Client is unblocked by barring UE rule](#) on page 218
- [Start CALEA mirroring client](#) on page 218
- [Stop CALEA mirroring client](#) on page 218
- [Wired client joined](#) on page 219
- [Wired client failed to join](#) on page 219
- [Wired client disconnected](#) on page 219
- [Wired client authorization successfully](#) on page 220
- [Wired client session expired](#) on page 220
- [Application identified](#) on page 220
- [Application denied](#) on page 221
- [URL filtering server unreachable](#) on page 221
- [URL filtering server reachable](#) on page 221
- [Packet spoofing detected](#) on page 222
- [Packet spoofing detected](#) on page 222
- [Packet spoofing detected](#) on page 222
- [Packet spoofing detected](#) on page 223

## Client authentication failed

**TABLE 418** Client authentication failed event

Event	Client authentication failed
Event Type	clientAuthFailure
Event Code	201
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx","userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join WLAN [{ssid}] from AP [{apName&&apMac}] due to authentication failure.

**TABLE 418** Client authentication failed event (continued)

Event	Client authentication failed
Description	This event occurs when the client fails to join WLAN on the AP due to an authentication failure.

## Client joined

**TABLE 419** Client joined event

Event	Client joined
Event Type	clientJoin
Event Code	202
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] joined WLAN [{ssid}] from AP [{apName}&&apMac}].
Description	This event occurs when the client session joins the WLAN on AP.

## Client failed to join

**TABLE 420** Client failed to join event

Event	Client failed to join
Event Type	clientJoinFailure
Event Code	203
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx" "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join WLAN [{ssid}] from AP [{apName}&&apMac}].
Description	This event occurs when the client fails to connect to the WLAN on the AP.

## Client disconnected

**TABLE 421** Client disconnected event

Event	Client disconnected
Event Type	clientDisconnect
Event Code	204
Severity	Informational



**TABLE 421** Client disconnected event (continued)

Event	Client disconnected
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] disconnected from WLAN [{ssid}] on AP [{apName}&&apMac]
Description	This event occurs when the client disconnects from WLAN on AP.

## Client connection timed out

**TABLE 422** Client connection timed out event

Event	Client connection timed out
Event Type	clientInactivityTimeout
Event Code	205
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"=", "sessionDuration"=", "txBytes"=", "rxBytes"=", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] disconnected from WLAN [{ssid}] on AP [{apName}&&apMac] due to inactivity
Description	This event occurs when client disconnects from WLAN on AP due to inactivity.

## Client authorization successfully

**TABLE 423** Client authorization successfully event

Event	Client authorization successfully
Event Type	clientAuthorization
Event Code	206
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] of WLAN [{ssid}] from AP [{apName}&&apMac] was authorized.

**TABLE 423** Client authorization successfully event (continued)

Event	Client authorization successfully
Description	This event occurs when the client on WLAN AP is authorized.

## Client authorization failed

**TABLE 424** Client authorization failed event

Event	Client authorization failed
Event Type	clientAuthorizationFailure
Event Code	207
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x" "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] of WLAN [{ssid}] from AP [{apName}&&apMac}] was not authorized.
Description	This event occurs when the client on WLAN AP authorization fails.

## Client session expired

**TABLE 425** Client session expired event

Event	Client session expired
Event Type	clientSessionExpiration
Event Code	208
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="" "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] exceeded the session time limit. Session terminated.
Description	This event occurs when the client exceeds the session time limit resulting in a session termination.

## Client roaming

**TABLE 426** Client roaming event

Event	Client roaming
Event Type	clientRoaming
Event Code	209
Severity	Informational

**TABLE 426** Client roaming event (continued)

Event	Client roaming
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x" "userId"="uuid"
Displayed on the web interface	AP [{apName&&apMac}] radio [{toRadio}] detected client [{userName    IP     clientMac}] in WLAN [{ssid}] roam from AP [{fromApName&&fromApMac}].
Description	This event occurs when the AP radio detects a client.

## Client logged out

**TABLE 427** Client logged out event

Event	Client logged out
Event Type	clientSessionLogout
Event Code	210
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "assoicationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="" "userId"="uuid"
Displayed on the web interface	Client [{userName    IP     clientMac}] session logout.
Description	This event occurs when a client session is logged out.

## 3rd party client join

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 428** 3rd party client join event

Event	3rd party client join
Event Type	3rdPtyClientJoin
Event Code	211
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd party client [{clientIP   clientMac}] joined Zone [{zoneName}] on DP [{dpName&&dpKey}].
Description	This event occurs when a 3rd party client joins the AP zone session on the data plane.

## 3rd party client inactivity timeout

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 429** 3rd party client inactivity timeout event

Event	3rd party client inactivity timeout
Event Type	3rdPtyClientInactivityTimeout
Event Code	212
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd party client [{clientIP}   clientMac] disconnected from Zone [{zoneName}] on DP [{dpName&&dpKey}] due to inactivity.
Description	This event occurs when 3rd party client disconnects from an AP zone session on the data plane due to inactivity.

## 3rd party client authorization

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 430** 3rd party client authorization event

Event	3rd party client authorization
Event Type	3rdPtyClientAuthorization
Event Code	213
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd Party client [{clientIP}   clientMac] of Zone [{zoneName}] on DP [{dpName&&dpKey}] was authorized.
Description	This event occurs when 3rd party client on AP zone session is authorized.

## 3rd party client authorization failure

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 431** 3rd party client authorization failure event

Event	3rd party client authorization failure
Event Type	3rdPtyClientAuthorizationFailure
Event Code	214
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"

**TABLE 431** 3rd party client authorization failure event (continued)

Event	3rd party client authorization failure
Displayed on the web interface	3rd party client [{clientIP}   clientMac] of Zone [{zoneName}] on DP [{dpName}&{dpKey}] was not authorized.
Description	This event occurs when the 3rd party client on the AP zone session is not authorized.

## 3rd party client session expiration

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 432** 3rd party client session expiration event

Event	3rd party client session expiration
Event Type	3rdPtyClientSessionExpiration
Event Code	215
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd party client [{clientIP}   clientMac] of Zone [{zoneName}] on DP [{dpName}   dpKey] exceeded the session time limit. Session terminated.
Description	This event occurs when the 3rd party client on the AP zone exceeds the session time limit, resulting in session termination.

## 3rd party client roaming

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 433** 3rd party client roaming event

Event	3rd party client roaming
Event Type	3rdPtyClientRoaming
Event Code	216
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	DataPlane [{dpName}   dpKey] detected 3rd party client [{clientIP}   clientMac] in Zone [{zoneName}] on DP [{dpName}   fromDpMac].
Description	This event occurs when the data plane detects a 3rd party client in the AP zone.

## 3rd party client session logout

### NOTE

This event is not applicable for vSZ-H.

**TABLE 434** 3rd party client session logout event

Event	3rd party client session logout
Event Type	3rdPtyClientSessionLogout
Event Code	217
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd party client [{clientIP   clientMac}] of Zone [{zoneName}] on DP [{dpName   dpKey}] occurred session logout.
Description	This event occurs when 3rd party client on AP zone data plane occurs. This results in a session logs out.

## Client roaming disconnected

**TABLE 435** Client roaming disconnected event

Event	Client roaming disconnected
Event Type	smartRoamDisconnect
Event Code	218
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "assoicationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="", "ni_rx_rssilo_cnt"="", "ni_rx_tot_cnt"="", "ns_rx_rssilo_cnt"="", "ns_rx_tot_cnt"="", "ni_tx_xput_lo_cnt"="", "ni_tx_xput_lo_dur"="", "Instantaneous rssi"="", "Xput"="", "userId"="uuid"
Displayed on the web interface	Client [{userName   IP   clientMac}] disconnected from WLAN [{ssid}] on AP [{apName&&apMac}] due to SmartRoam policy.
Description	This event occurs when the client disconnects from the WLALN due to a smart roam policy.

## Client blocked

**TABLE 436** Client blocked event

Event	Client blocked
Event Type	clientBlockByDeviceType
Event Code	219
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "deviceType"="xxxxx", "ssid"="xxxxx", "wlanId"="xxxxx",

**TABLE 436** Client blocked event (continued)

Event	Client blocked
Displayed on the web interface	Client [{clientMac}] was recognized as [{deviceType}], and blocked by a device policy in AP [{apMac}]
Description	This event occurs when a client is blocked by a device policy.

## Client grace period

**TABLE 437** Client grace period event

Event	Client grace period
Event Type	clientGracePeriod
Event Code	220
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x"
Displayed on the web interface	Client [{userName   clientIP   clientMac}] reconnects WLAN [{ssid}] on AP [{apName&&apMac}] within grace period. No additional authentication is required.
Description	This event occurs when the when the STa interface reconnects and authorizes due to the grace period.

## Onboarding registration succeeded

**TABLE 438** Onboarding registration succeeded event

Event	Onboarding registration succeeded
Event Type	onboardingRegistrationSuccess
Event Code	221
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid", "apLocation"="xxxxx", "groupName"="xxxxx", "vlanId"="xxxxx", "osType"="xxxxx", "userAgent"="xxxxx"
Displayed on the web interface	Client [{userName   clientIP   clientMac}] of WLAN [{ssid}] on AP [{apName&&apMac}] on boarding registration succeeded.
Description	This event occurs when the client on boarding registration is successful.

## Onboarding registration failed

**TABLE 439** Onboarding registration failed event

Event	Onboarding registration failed
Event Type	onboardingRegistrationFailure
Event Code	222
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid", "apLocation"="xxxxx", "groupName"="xxxxx", "vlanId"="xxxxx", "osType"="xxxxx", "userAgent"="xxxxx", "reason"="xxxxx"

**TABLE 439** Onboarding registration failed event (continued)

Event	Onboarding registration failed
Displayed on the web interface	Client [{userName}   {clientIP}   {clientMac}] of WLAN [{ssid}] on AP [{apName}&&apMac}] on boarding registration failed because of [{reason}].
Description	This event occurs when the client onboarding registration fails.

## Remediation succeeded

**TABLE 440** Remediation succeeded event

Event	Remediation succeeded
Event Type	remediationSuccess
Event Code	223
Severity	Informational
Attribute	"remediationType"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "userName"="xxxxx", "userId"="uuid", "reason"="xxxxx"
Displayed on the web interface	Remediation of type [{remediationType}] finished successfully on client [{clientIP}   {clientMac}] for user [{userName}].
Description	This event occurs when the client remediation is successful.

## Remediation failed

**TABLE 441** Remediation failed event

Event	Remediation failed
Event Type	remediationFailure
Event Code	224
Severity	Informational
Attribute	"remediationType"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "userName"="xxxxx", "userId"="uuid"
Displayed on the web interface	Remediation of type [{remediationType}] failed on client [{clientIP}   {clientMac}] for user [{userName}].
Description	This event occurs when the client remediation fails.

## Force DHCP disconnected

**TABLE 442** Force DHCP disconnected event

Event	Force DHCP disconnected
Event Type	forceDHCPDisconnect
Event Code	225
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "bssid"="", "wlanId"="xxxxx", "tenantUUID"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "vlanId"="", "radio"="", "encryption"=""
Displayed on the web interface	Client [{userName}   {IP}   {clientMac}] disconnected from WLAN [{ssid}] on AP [{apName}&&apMac}] due to force-dhcp.



**TABLE 442** Force DHCP disconnected event (continued)

Event	Force DHCP disconnected
Description	This event occurs when the client disconnects by force from the dynamic host configuration protocol.

## WDS device joined

**TABLE 443** WDS device joined event

Event	WDS device joined
Event Type	wdsDeviceJoin
Event Code	226
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "wdsDeviceMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Device [{wdsDeviceMac}] sends traffic via Client [{clientMac}] in AP [{apName&&apMac}].
Description	This event occurs when a subscriber device joins the network provided by a Customer-Premises Equipment (CPE) of a client associated AP through a wireless distribution system (WDS) mode.

## WDS device left

**TABLE 444** WDS device left event

Event	WDS device left
Event Type	wdsDeviceLeave
Event Code	227
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "wdsDeviceMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Device [{wdsDeviceMac}] stops traffic via Client [{clientMac}] in AP [{apName&&apMac}].
Description	This event occurs when a subscriber device leaves the network provided by a CPE client associated to an AP through WDS.

## Client is blocked because of barring UE rule

**TABLE 445** Client is blocked because of barring UE rule event

Event	Client is blocked because of barring UE rule
Event Type	clientBlockByBarringUERule
Event Code	228
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Client [clientMac] of WLAN [ssid] from AP [apName&&apMac] was blocked because of barring UE rule.
Description	This event occurs when a client is temporarily blocked by the UE barring rule.

## Client is unblocked by barring UE rule

**TABLE 446** Client is unblocked by barring UE rule event

Event	Client is unblocked by barring UE rule
Event Type	clientUnblockByBarringUERule
Event Code	229
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Client [clientMac] of WLAN [ssid] from AP [apName&&apMac] was unblocked
Description	This event occurs when a client is unblocked by the UE barring rule.

## Start CALEA mirroring client

**TABLE 447** Start CALEA mirroring client event

Event	Start CALEA mirroring client
Event Type	caleaMirroringStart
Event Code	230
Severity	Informational
Attribute	"userName"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Start CALEA mirroring client [userName   IP   clientMac] on WLAN [ssid] from AP [apName&&apMac].
Description	This event occurs when CALEA is started for mirroring the client image.

## Stop CALEA mirroring client

**TABLE 448** Stop CALEA mirroring client event

Event	Stop CALEA mirroring client
Event Type	caleaMirroringStop
Event Code	231
Severity	Informational
Attribute	"userName"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "authType"="xxxxx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	Stop CALEA mirroring client [userName   IP   clientMac] on WLAN [ssid] with authentication type [authType] from AP [apName&&apMac]. TxBytes[txBytes], RxBytes[rxBytes].
Description	This event occurs when CALEA stops mirroring the client image.

## Client information updated

**TABLE 449** Client information updated event

Event	Client Info Update
Event Type	clientInfoUpdate

**TABLE 449** Client information updated event (continued)

Event	Client Info Update
Event Code	236
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] info update on WLAN [{ssid}] from AP [{apName}&&apMac}].
Description	This event occurs when a client obtains IP address.

## Wired client joined

**TABLE 450** Wired client joined event

Event	Wired client joined
Event Type	wiredClientJoin
Event Code	2802
Severity	Informational
Attribute	apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ethProfileId"="xxxxx", "ethPort"="x", "iface"="xxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxx", "vlanId"="x"
Displayed on the web interface	Client [{userName}   IP   clientMac] joined LAN [{ethPort}] from AP [{apName}&&apMac}].
Description	This event occurs when a client joins the LAN AP.

## Wired client failed to join

**TABLE 451** Wired client failed to join event

Event	Wired client failed to join
Event Type	wiredClientJoinFailure
Event Code	2803
Severity	Informational
Attribute	apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ethProfileId"="xxxxx", "ethPort"="x", "iface"="xxx", "userName"="xxxxx", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join LAN [{ethPort}] from AP [{apName}&&apMac}].
Description	This event occurs when a client fails to join the LAN AP.

## Wired client disconnected

**TABLE 452** Wired client disconnected event

Event	Wired client disconnected
Event Type	wiredClientDisconnect
Event Code	2804
Severity	Informational

**TABLE 452** Wired client disconnected event (continued)

Event	Wired client disconnected
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxxx", tenantUUID="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", apName="xxxx", vlanId="x", rxBytes="x", txFrames="x", txBytes="x", disconnectTime="x", sessionDuration="x", disconnectReason="x"
Displayed on the web interface	Client [{userName}   IP   clientMac] disconnected from LAN [ethPort] on AP [apName&&apMac].
Description	This event occurs when a client disconnect from the LAN AP.

## Wired client authorization successfully

**TABLE 453** Wired client authorization successfully event

Event	Wired client authorization successfully
Event Type	wiredClientAuthorization
Event Code	2806
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxxx", tenantUUID="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", apName="xxxx", vlanId="x", rxBytes="x", txFrames="x", txBytes="x", userName="xxxx"
Displayed on the web interface	Client [{userName}   IP   clientMac] of LAN [ethPort] from AP [apName&&apMac] was authorized.
Description	This event occurs when a client on WLAN AP is authorized.

## Wired client session expired

**TABLE 454** Wired client session expired event

Event	Wired client session expired
Event Type	wiredClientSessionExpiration
Event Code	2808
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxxx", tenantUUID="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", apName="xxxx", vlanId="x", rxBytes="x", txFrames="x", txBytes="x", disconnectTime="x", sessionDuration="x", disconnectReason="x"
Displayed on the web interface	Client [{userName}   IP   clientMac] exceeded the session time limit. Session terminated.
Description	This event occurs when a client exceeds the session time limit, which results in a session termination.

## Application identified

**TABLE 455** Application identified event

Event	Application identified
Event Type	application of user is identified
Event Code	8001

**TABLE 455** Application identified event (continued)

Event	Application identified
Severity	Informational
Attribute	
Displayed on the web interface	APP[APP] identified from AP[apMac] for client [STA_MAC] with source[SRC_IP]:[SRC_PORT] destination[DST_IP]:[DST_PORT] Proto[PROTO]
Description	This event occurs when the user of the application is identified.

## Application denied

**TABLE 456** Application denied event

Event	Application denied
Event Type	application of user is denied
Event Code	8002
Severity	Informational
Attribute	
Displayed on the web interface	APP[APP] denied from AP[apMac] for client [STA_MAC] with source[SRC_IP]:[SRC_PORT] destination[DST_IP]:[DST_PORT] Proto[PROTO]
Description	This event occurs when the application of the user is denied.

## URL filtering server unreachable

**TABLE 457** URL filtering server unreachable event

Event	URL filtering server unreachable
Event Type	urlFilteringServerUnreachable
Event Code	8003
Severity	Major
Attribute	apMac = "xx:xx:xx:xx:xx:xx", serverUrl = "xxxxxx"
Displayed on the web interface	AP [apMac] cannot reach the URL Filtering server [serverUrl].
Description	This event occurs when URL filtering server is unreachable.

## URL filtering server reachable

**TABLE 458** URL filtering server reachable event

Event	URL filtering server reachable
Event Type	urlFilteringServerReachable
Event Code	8004
Severity	Major
Attribute	apMac = "xx:xx:xx:xx:xx:xx", serverUrl = "xxxxxx"
Displayed on the web interface	AP [apMac] can reach the URL Filtering server [serverUrl].
Description	This event occurs when URL filtering server is reachable.

## Packet spoofing detected

**TABLE 459** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWireless
Event Code	232
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "ssid"="xxxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}] from client [{clientMac&&clientIP}] on WLAN [{ssid}] [{networkInterface}] from AP [{apName&&apMac}]
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature.

## Packet spoofing detected

**TABLE 460** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWirelessSourceMacSpoofed
Event Code	233
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "ssid"="xxxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}], packets [{packetDropCount}] were dropped on WLAN [{ssid}] [{networkInterface}] from AP [{apName&&apMac}]
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature. It is a source MAC address spoof.

## Packet spoofing detected

**TABLE 461** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWired
Event Code	234
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}] from client [{clientMac&&clientIP}] on [{networkInterface}] from AP [{apName&&apMac}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature.

## Packet spoofing detected

**TABLE 462** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWiredSourceMacSpoofed
Event Code	235
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{{desc}}], packets [{{packetDropCount}}] were dropped on [{{networkInterface}}] from AP [{{apName&&apMac}}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature. It is a source MAC address spoof.

## Cloud Events

The following are the events related to Cloud Based Service.

- [Cloud Services Enabled](#) on page 223
- [Cloud Services Disabled](#) on page 223
- [Cloud Analytics Enabled](#) on page 224
- [Cloud Analytics Disabled](#) on page 224
- [Cloud Services Token Refreshed](#) on page 224
- [Cloud Analytics Token Renewed](#) on page 225

## Cloud Services Enabled

**TABLE 463** Cloud services enabled event

Event	Cloud services enabled
Event Type	CloudServicesEnabled
Event Code	4501
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services have been enabled successfully.
Description	This event occurs when the controller successfully enables the Cloud Services.

## Cloud Services Disabled

**TABLE 464** Cloud services disabled event

Event	Cloud services disabled
Event Type	CloudServicesdisabled
Event Code	4502
Severity	Informational

**TABLE 464** Cloud services disabled event (continued)

Event	Cloud services disabled
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services have been disabled successfully.
Description	This event occurs when controller successfully disables the Cloud Services.

## Cloud Analytics Enabled

**TABLE 465** Cloud analytics enabled event

Event	Cloud analytics enabled
Event Type	CloudAnalyticsEnabled
Event Code	4503
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics service has been enabled successfully.
Description	This event occurs when the controller successfully enables Cloud Analytics service.

## Cloud Analytics Disabled

**TABLE 466** Cloud analytics disabled event

Event	Cloud analytics disabled
Event Type	CloudAnalyticsDisabled
Event Code	4504
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This event occurs when the controller successfully disables Cloud Analytics service.

## Cloud Services Token Refreshed

**TABLE 467** Cloud services token refreshed event

Event	Cloud services token refreshed
Event Type	CloudServicesTokenRefreshed
Event Code	4601
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services token has been refreshed successfully.
Description	This event occurs when the controller successfully refreshes the Cloud Services access token.



## Cloud Analytics Token Renewed

**TABLE 468** Cloud analytics token renewed event

Event	Cloud analytics token renewed
Event Type	cloudAnalyticsTokenRenewed
Event Code	4602
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics token has been renewed successfully.
Description	This event occurs when the controller successfully renews Cloud Analytics access token.

## Cloud Analytics Service has been Enabled

**TABLE 469** Cloud Analytics Service has been Enabled event

Event	Cloud Analytics Service has been Enabled
Event Type	cloudAnalyticsEnabled
Event Code	4503
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service has been enabled successfully.
Description	This event occurs when Smart Zone successfully enables cloud analytics service.

## Cloud Analytics service has been disabled

**TABLE 470** Cloud Analytics service has been disabled event

Event	Cloud Analytics service has been disabled
Event Type	cloudAnalyticsDisabled
Event Code	4504
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This event occurs when SZ successfully disabled Cloud Analytics service.

## Cloud Analytics Disconnected

**TABLE 471** Cloud Analytics Disconnected event

Event	Cloud Analytics Disconnected
Event Type	cloudAnalyticsDisconnected
Event Code	4505
Severity	Major

**TABLE 471** Cloud Analytics Disconnected event (continued)

Event	Cloud Analytics Disconnected
Attribute	
Displayed on the web interface	Cloud Analytics service cannot be connected.
Description	This event occurs when Smart Zone can't send heartbeat to Cloud Analytics service.

## Cluster Events

Following are the events related to clusters.

Event	Event	Event
<a href="#">Cluster created successfully</a> on page 227	<a href="#">New node joined successfully</a> on page 227	<a href="#">New node failed to join</a> on page 227
<a href="#">Node removal completed</a> on page 228	<a href="#">Node removal failed</a> on page 228	<a href="#">Node out of service</a> on page 228
<a href="#">Cluster in maintenance state</a> on page 229	<a href="#">Cluster back in service</a> on page 229	<a href="#">Cluster backup completed</a> on page 229
<a href="#">Cluster backup failed</a> on page 229	<a href="#">Cluster restore completed</a> on page 230	<a href="#">Cluster restore failed</a> on page 230
<a href="#">Cluster node upgrade completed</a> on page 230	<a href="#">Entire cluster upgraded successfully</a> on page 231	<a href="#">Cluster upgrade failed</a> on page 231
<a href="#">Cluster application stopped</a> on page 231	<a href="#">Cluster application started</a> on page 232	<a href="#">Cluster backup started</a> on page 232
<a href="#">Cluster upgrade started</a> on page 232	<a href="#">Cluster leader changed</a> on page 233	<a href="#">Node bond interface down</a> on page 233
<a href="#">Node bond interface up</a> on page 233	<a href="#">Node IP address changed</a> on page 234	<a href="#">Node physical interface down</a> on page 234
<a href="#">Node physical interface up</a> on page 234	<a href="#">Cluster node rebooted</a> on page 234	<a href="#">NTP time synchronized</a> on page 235
<a href="#">Cluster node shutdown</a> on page 235	<a href="#">Cluster upload started</a> on page 235	<a href="#">Cluster upload completed</a> on page 236
<a href="#">Cluster upload failed</a> on page 236	<a href="#">SSH tunnel switched</a> on page 236	<a href="#">Cluster remove node started</a> on page 237
<a href="#">Node back in service</a> on page 237	<a href="#">Disk usage exceed threshold</a> on page 237	<a href="#">Cluster out of service</a> on page 237
<a href="#">Initiated moving APs in node to a new cluster</a> on page 238	<a href="#">Cluster upload vSZ-D firmware started</a> on page 238	<a href="#">Cluster upload vSZ-D firmware completed</a> on page 238
<a href="#">Cluster upload vSZ-D firmware failed</a> on page 239	<a href="#">Cluster upload AP firmware started</a> on page 239	<a href="#">Cluster upload AP firmware completed</a> on page 239
<a href="#">Cluster upload AP firmware failed</a> on page 240	<a href="#">Cluster add AP firmware started</a> on page 240	<a href="#">Cluster add AP firmware completed</a> on page 240
<a href="#">Cluster add AP firmware failed</a> on page 240	<a href="#">Cluster name is changed</a> on page 241	<a href="#">Unsync NTP Time</a> on page 241
<a href="#">Cluster upload KSP file started</a> on page 241	<a href="#">Cluster upload KSP file completed</a> on page 242	<a href="#">Cluster upload KSP file failed</a> on page 242
<a href="#">NTP unreachable server</a> on page 242	<a href="#">Configuration backup started</a> on page 243	<a href="#">Configuration backup succeeded</a> on page 243
<a href="#">Configuration backup failed</a> on page 243	<a href="#">Configuration restore succeeded</a> on page 243	<a href="#">Configuration restore failed</a> on page 244
<a href="#">AP Certificate Expired</a> on page 244	<a href="#">AP Certificate Updated</a> on page 244	<a href="#">Configuration restore started</a> on page 245
<a href="#">Upgrade SSTable failed</a> on page 245	<a href="#">Reindex elastic search finished</a> on page 245	<a href="#">Initiated APs contact APR</a> on page 246
<a href="#">All nodes back in service</a> on page 246	<a href="#">Not management service ready</a> on page 246	<a href="#">Management service ready</a> on page 246
<a href="#">Configuration sync failed</a> on page 247	<a href="#">Node IPv6 address deleted</a> on page 248	<a href="#">Node IPv6 address added</a> on page 247
<a href="#">AP is connected to standby cluster over the expiration date</a> on page 247	<a href="#">Sync Configuration Success for Cluster Redundancy</a> on page 248	<a href="#">Standby Cluster Restores a Configuration for Cluster Redundancy</a> on page 249
<a href="#">Standby Cluster Back to Monitoring Mode for Cluster Redundancy</a> on page 249	<a href="#">Standby Cluster Restored a Configuration Success for Cluster Redundancy</a> on page 249	<a href="#">AP Connected to Standby Cluster after Rehome Timeout</a> on page 250
<a href="#">External DP Connected to Standby Cluster after Rehome Timeout</a> on page 250	<a href="#">Sync Configuration started for Cluster Redundancy</a> on page 248	<a href="#">Standby Cluster Restored a Configuration Success for Cluster Redundancy</a> on page 249
<a href="#">Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy</a> on page 250		

## Cluster created successfully

**TABLE 472** Cluster created successfully event

Event	Cluster created successfully
Event Type	clusterCreatedSuccess
Event Code	801
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Cluster [{clusterName}] created with node [{nodeName}]
Description	This event occurs when a cluster and a node are created.

## New node joined successfully

**TABLE 473** New node joined successfully event

Event	New node joined successfully
Event Type	newNodeJoinSuccess
Event Code	802
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	New node [{nodeName}] joined cluster [{clusterName}]
Description	This event occurs when a node joins a cluster session.

## New node failed to join

**TABLE 474** New node failed to join event

Event	New node failed to join
Event Type	newNodeJoinFailed
Event Code	803
Severity	Critical
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	New node [{nodeName}] failed to join cluster [{clusterName}]
Description	This event occurs when a node fails to join a cluster session. The controller web interface displays the error message.
Auto Clearance	This event triggers the alarm 801, which is auto cleared by the event code 802.

## Node removal completed

**TABLE 475** Node removal completed event

Event	Node removal completed
Event Type	removeNodeSuccess
Event Code	804
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] removed from cluster [{clusterName}]
Description	This event occurs when a node is removed from the cluster session.

## Node removal failed

**TABLE 476** Node removal failed event

Event	Node removal failed
Event Type	removeNodeFailed
Event Code	805
Severity	Major
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] failed to remove from cluster [{clusterName}].
Description	This event occurs when a node cannot be removed from the cluster.
Auto Clearance	This event triggers the alarm 802, which is auto cleared by the event code 804.

## Node out of service

**TABLE 477** Node out of service event

Event	Node out of service
Event Type	nodeOutOfService
Event Code	806
Severity	Critical
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service. Reason:[{reason}].
Description	This event occurs when a node is out of service.
Auto Clearance	This event triggers the alarm 803, which is auto cleared by the event code 835.

## Cluster in maintenance state

**TABLE 478** Cluster in maintenance state event

Event	Cluster in maintenance state
Event Type	clusterInMaintenanceState
Event Code	807
Severity	Critical
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}} is in maintenance state
Description	This event occurs when a node is in a maintenance state.
Auto Clearance	This event triggers the alarm 804, which is auto cleared by the event code 808.

## Cluster back in service

**TABLE 479** Cluster back in service event

Event	Cluster back in service
Event Type	clusterBackToInService
Event Code	808
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}} is now in service
Description	This event occurs when a cluster is back in service.

## Cluster backup completed

**TABLE 480** Cluster backup completed event

Event	Cluster backup completed
Event Type	backupClusterSuccess
Event Code	809
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} backup completed
Description	This event occurs when a cluster backup is complete.

## Cluster backup failed

**TABLE 481** Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810

**TABLE 481** Cluster backup failed event (continued)

Event	Cluster backup failed
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason[{reason}].
Description	This event occurs when a cluster backup fails.
Auto Clearance	This event triggers the alarm 805, which is auto cleared by the event code 809.

## Cluster restore completed

**TABLE 482** Cluster restore completed event

Event	Cluster restore completed
Event Type	restoreClusterSuccess
Event Code	811
Severity	Informational
Attribute	"nodeName"="xxx", "clusterName"="xxx",
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] restore completed
Description	This event occurs when restoration of a node to a cluster is successful.

## Cluster restore failed

**TABLE 483** Cluster restore failed event

Event	Cluster restore failed
Event Type	restoreClusterFailed
Event Code	812
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] restore failed. Reason [{reason}].
Description	This event occurs when restoration of a node in a cluster fails.
Auto Clearance	This event triggers the alarm 806, which is auto cleared by the event code 811.

## Cluster node upgrade completed

**TABLE 484** Cluster node upgrade completed event

Event	Cluster node upgrade completed
Event Type	upgradeClusterNodeSuccess
Event Code	813
Severity	Informational

**TABLE 484** Cluster node upgrade completed event (continued)

Event	Cluster node upgrade completed
Attribute	clusterName="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "fromVersion"="x.x", "toVersion"="x.x"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] upgraded from [{fromVersion}] to [{toVersion}]
Description	This event occurs when version upgrade of a node is successful.

## Entire cluster upgraded successfully

**TABLE 485** Entire cluster upgraded successfully event

Event	Entire cluster upgraded successfully
Event Type	upgradeEntireClusterSuccess
Event Code	814
Severity	Informational
Attribute	clusterName="xxx", "fromVersion"="x.x", "toVersion"="x.x"
Displayed on the web interface	Cluster [{clusterName}] upgraded from [{fromVersion}] to [{toVersion}].
Description	This event occurs when version upgrade of a cluster is successful.

## Cluster upgrade failed

**TABLE 486** Cluster upgrade failed event

Event	Cluster upgrade failed
Event Type	upgradeClusterFailed
Event Code	815
Severity	Major
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "fromVersion"="x.x", "toVersion"="x.x"
Displayed on the web interface	Cluster [{clusterName}] could not be upgraded from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the version upgrade of a cluster fails.
Auto Clearance	This event triggers the alarm 807, which is auto cleared by the event code 814.

## Cluster application stopped

**TABLE 487** Cluster application stopped event

Event	Cluster application stopped
Event Type	clusterAppStop
Event Code	816
Severity	Critical

**TABLE 487** Cluster application stopped event (continued)

Event	Cluster application stopped
Attribute	"appName"="xxxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Application [{appName}] on node [{nodeName}] stopped
Description	This event occurs when an application on node is stopped.
Auto Clearance	This event triggers the alarm 808, which is auto cleared by the event code 817.

## Cluster application started

**TABLE 488** Cluster application started event

Event	Cluster application started
Event Type	clusterAppStart
Event Code	817
Severity	Informational
Attribute	"appName"="xxxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Application [{appName}] on node [{nodeName}] started
Description	This event occurs when an application on node starts.

## Cluster backup started

**TABLE 489** Cluster backup started event

Event	Cluster backup started
Event Type	clusterBackupStart
Event Code	818
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Starting backup in cluster[{clusterName}]...
Description	This event occurs when a backup for a node commences.

## Cluster upgrade started

**TABLE 490** Cluster upgrade started event

Event	Cluster upgrade started
Event Type	clusterUpgradeStart
Event Code	819
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",



**TABLE 490** Cluster upgrade started event (continued)

Event	Cluster upgrade started
Displayed on the web interface	Starting upgrade in cluster[{clusterName}]
Description	This event occurs when an upgrade for a node commences.

## Cluster leader changed

**TABLE 491** Cluster leader changed event

Event	Cluster leader changed
Event Type	clusterLeaderChanged
Event Code	820
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] promoted to leader
Description	This event occurs when a node is changed to a lead node.

## Node bond interface down

**TABLE 492** Node bond interface down event

Event	Node bond interface down
Event Type	nodeBondInterfaceDown
Event Code	821
Severity	Major
Attribute	"nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Network interface [{networkInterface}   {ifName}] on node [{nodeName}] is down.
Description	This event occurs when the network interface of a node is down.
Auto Clearance	This event triggers the alarm 809, which is auto cleared by the event code 822.

## Node bond interface up

**TABLE 493** Node bond interface up event

Event	Node bond interface up
Event Type	nodeBondInterfaceUp
Event Code	822
Severity	Informational
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Network interface [{networkInterface}   {ifName}] on node [{nodeName}] is up.
Description	This event occurs when the network interface of a node is up.

## Node IP address changed

**TABLE 494** Node IP address changed event

Event	Node IP address changed
Event Type	nodeIPChanged
Event Code	823
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx", "ip"="xxx.xxx.xxx.xxx"
Displayed on the web interface	IP address of network interface [{networkInterface}   {ifName}] on node [{nodeName}] changed to [{ip}].
Description	This event occurs when the node's network interface IP address changes.

## Node physical interface down

**TABLE 495** Node physical interface down event

Event	Node physical interface down
Event Type	nodePhyInterfaceDown
Event Code	824
Severity	Critical
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Physical network interface [{networkInterface}   {ifName}] on node [{nodeName}] is down.
Description	This event occurs when the node's physical interface is down.
Auto Clearance	This event triggers the alarm 810, which is auto cleared by the event code 825.

## Node physical interface up

**TABLE 496** Node physical interface up event

Event	Node physical interface up
Event Type	nodePhyInterfaceUp
Event Code	825
Severity	Informational
Attribute	"nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Physical network interface [{networkInterface}   {ifName}] on node [{nodeName}] is up.
Description	This event occurs when the node's physical interface is up.

## Cluster node rebooted

**TABLE 497** Cluster node rebooted event

Event	Cluster node rebooted
Event Type	nodeRebooted
Event Code	826

**TABLE 497** Cluster node rebooted event (continued)

Event	Cluster node rebooted
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "clusterName"="xxx",
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] rebooted
Description	This event occurs when the node, belonging to a cluster reboots.

## NTP time synchronized

**TABLE 498** NTP time synchronized event

Event	NTP time synchronized
Event Type	ntpTimeSynched
Event Code	827
Severity	Informational
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Date and time settings on node [{nodeName}] synchronized with NTP server
Description	This event occurs when the date and time settings of a node synchronizes with the NTP server.

## Cluster node shutdown

**TABLE 499** Cluster node shutdown event

Event	Cluster node shutdown
Event Type	nodeShutdown
Event Code	828
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx "
Displayed on the web interface	Node [{nodeName}] has been shut down
Description	This event occurs when the node is shut down.
Auto Clearance	This event triggers the alarm 813, which is auto cleared by the event code 826.

## Cluster upload started

**TABLE 500** Cluster upload started event

Event	Cluster upload started
Event Type	clusterUploadStart
Event Code	830
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting upload in cluster [{clusterName}].

**TABLE 500** Cluster upload started event (continued)

Event	Cluster upload started
Description	This event occurs when the cluster upload process starts.

## Cluster upload completed

**TABLE 501** Cluster upload completed event

Event	Cluster upload completed
Event Type	uploadClusterSuccess
Event Code	831
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload completed
Description	This event occurs when the cluster upload process is successful.

## Cluster upload failed

**TABLE 502** Cluster upload failed event

Event	Cluster upload failed
Event Type	uploadClusterFailed
Event Code	832
Severity	Major
Attribute	"clusterName"="xxx", "reason"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload failed. Reason:{{reason}}
Description	This event occurs when the cluster upload process fails.

## SSH tunnel switched

**TABLE 503** SSH tunnel switched event

Event	SSH tunnel switched
Event Type	sshTunnelSwitched
Event Code	833
Severity	Major
Attribute	"clusterName"="xx", "nodeName"="xx", "nodeMac"="xx.xx.xx.xx.xx", "wsgMgmtIp"="xx.xx.xx.xx", "status"="ON->OFF", "sourceBladeUUID"="054ee469"
Displayed on the web interface	Node {{nodeName}} SSH tunnel switched {{status}}
Description	This event occurs when the SSH tunnel is switched.

## Cluster remove node started

**TABLE 504** Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName" ="xxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Start to remove node [{nodeName}] from cluster [{clusterName}]
Description	This event occurs when the node start is removed.

## Node back in service

**TABLE 505** Node back in service event

Event	Node back in service
Event Type	nodeBackToInService
Event Code	835
Severity	Informational
Attribute	"clusterName"="xx", "nodeName" ="xxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is in service
Description	This event occurs when a node status changes to 'in service'.

## Disk usage exceed threshold

**TABLE 506** Disk usage exceed threshold

Event	Disk usage exceed threshold
Event Type	diskUsageExceed
Event Code	838
Severity	Critical
Attribute	"nodeName"="xx", "status"="xx"
Displayed on the web interface	The disk usage of node [{nodeName}] is over {status}%.
Description	This event occurs when the disk usage exceeds the threshold limit of 96%. For event 838, the threshold is 95%.

## Cluster out of service

**TABLE 507** Cluster out of service event

Event	Cluster out of service
Event Type	clusterOutOfService
Event Code	843
Severity	Critical

**TABLE 507** Cluster out of service event (continued)

Event	Cluster out of service
Attribute	"clusterName"="xx"
Displayed on the web interface	Cluster [{clusterName}] is out of service.
Description	This event occurs when the cluster is out of service.
Auto Clearance	This event triggers the alarm 843, which is auto cleared by the event code 808.

## Initiated moving APs in node to a new cluster

**TABLE 508** Initiated moving APs in node to a new cluster event

Event	Initiated moving APs in node to a new cluster
Event Type	clusterInitiatedMovingAp
Event Code	844
Severity	Informational
Attribute	"nodeName"="xxx" "clusterName"="xxx"
Displayed on the web interface	Initiated moving APs in node [{nodeName}] of cluster [{clusterName}] to a new cluster.
Description	This event occurs when the command to move the APs in the node to another cluster is received.

**NOTE**

Events 845, 846 and 847 are not applicable for SZ300/SZ100.

## Cluster upload vSZ-D firmware started

**TABLE 509** Cluster upload vSZ-D firmware started event

Event	Cluster upload vSZ-D firmware started
Event Type	clusterUploadVDPFirmwareStart
Event Code	845
Severity	Informational
Attribute	"clusterName"="xx"
Displayed on the web interface	Starting upload vSZ-D firmware in cluster [{clusterName}]
Description	This event occurs when the cluster starts and uploads vSZ-data plane firmware.

## Cluster upload vSZ-D firmware completed

**TABLE 510** Cluster upload vSZ-D firmware completed event

Event	Cluster upload vSZ-D firmware completed
Event Type	uploadClusterVDPFirmwareSuccess
Event Code	846
Severity	Informational

**TABLE 510** Cluster upload vSZ-D firmware completed event (continued)

Event	Cluster upload vSZ-D firmware completed
Attribute	"clusterName"="xxx" "status"="StartTime:yyyy-MM-dd hh:mm:ss, EndTime:yyyy-MM-dd hh:mm:ss, Duration:hh:mm:ss"
Displayed on the web interface	Cluster {{clusterName}} upload vSZ-D firmware completed. {{status}}
Description	This event occurs when the cluster upload process of vSZ-data plane firmware is successful.

## Cluster upload vSZ-D firmware failed

**TABLE 511** Cluster upload vSZ-D firmware failed event

Event	Cluster upload vSZ-D firmware failed
Event Type	uploadClusterVDPFirmwareFailed
Event Code	847
Severity	Informational
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload vSZ-D firmware failed. Reason:{{reason}}.
Description	This event occurs when the cluster upload process of vSZ-data plane firmware fails.

## Cluster upload AP firmware started

**TABLE 512** Cluster upload AP firmware started event

Event	Cluster upload AP firmware started
Event Type	clusterUploadAPFirmwareStart
Event Code	848
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting upload AP firmware in cluster {{clusterName}}
Description	This event occurs when the cluster upload process to the AP firmware starts.

## Cluster upload AP firmware completed

**TABLE 513** Cluster upload AP firmware completed event

Event	Cluster upload AP firmware completed
Event Type	clusterUploadAPFirmwareSuccess
Event Code	849
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload AP firmware completed.
Description	This event occurs when the cluster upload process to the AP firmware is successful.

## Cluster upload AP firmware failed

**TABLE 514** Cluster upload AP firmware failed event

Event	Cluster upload AP firmware failed
Event Type	clusterUploadAPFirmwareFailed
Event Code	850
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload AP firmware failed. Reason:{{reason}}.
Description	This event occurs when the cluster upload process to the AP firmware fails.

## Cluster add AP firmware started

**TABLE 515** Cluster add AP firmware started event

Event	Cluster add AP firmware started
Event Type	clusterAddAPFirmwareStart
Event Code	851
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting add AP firmware in cluster {{clusterName}}
Description	This event occurs when the cluster add process to the AP firmware process starts.

## Cluster add AP firmware completed

**TABLE 516** Cluster add AP firmware completed event

Event	Cluster add AP firmware completed
Event Type	clusterAddAPFirmwareSuccess
Event Code	852
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting add AP firmware in cluster {{clusterName}}
Description	This event occurs when the cluster add process to the AP firmware is successful.

## Cluster add AP firmware failed

**TABLE 517** Cluster add AP firmware failed event

Event	Cluster add AP firmware failed
Event Type	clusterAddAPFirmwareFailed
Event Code	853
Severity	Major



**TABLE 517** Cluster add AP firmware failed event (continued)

Event	Cluster add AP firmware failed
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] add AP firmware failed. Reason:[{reason}].
Description	This event occurs when the cluster add process to the AP firmware fails.

## Cluster name is changed

**TABLE 518** Cluster name is changed event

Event	Cluster name is changed
Event Type	clusterNameChanged
Event Code	854
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster name is changed to [{clusterName}]
Description	<p>This event occurs when the cluster node name is modified. By enabling email and SNMP notification in the controller user interface (<b>Configuration &gt; System &gt; Event Management</b>) of the event, SNMP trap and email will be generated on successful cluster-name modification.</p> <p>Cluster name change will fail if any node in either a two, three or four node cluster is out of service. For example, if in a three node cluster, any one node is powered off or the Ethernet cable is unplugged, cluster name change will fail.</p>

## Unsync NTP Time

**TABLE 519** Unsync NTP Time event

Event	Unsync NTP Time
Event Type	unsyncNTPTIME
Event Code	855
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx", "status"="xxx"
Displayed on the web interface	Node [{nodeName}] time is not synchronized because of [{reason}]. The time difference is [{status}] seconds.
Description	This event occurs when the cluster time is not synchronized.

## Cluster upload KSP file started

**TABLE 520** Cluster upload KSP file started event

Event	Cluster upload KSP file started
Event Type	clusterUploadKspFileStart
Event Code	856
Severity	Informational
Attribute	"clusterName"="xxx",

**TABLE 520** Cluster upload KSP file started event (continued)

Event	Cluster upload KSP file started
Displayed on the web interface	Cluster {{ clusterName}} upload KSP file completed.
Description	This event occurs when the cluster starts the upload process of the <i>ksp</i> file.

## Cluster upload KSP file completed

**TABLE 521** Cluster upload KSP file completed event

Event	Cluster upload KSP file completed
Event Type	clusterUploadKspFileSuccess
Event Code	857
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting upload KSP file in cluster {{clusterName}}
Description	This event occurs when the cluster uploads the <i>ksp</i> file successfully.

## Cluster upload KSP file failed

**TABLE 522** Cluster upload KSP file failed event

Event	Cluster upload KSP file failed
Event Type	clusterUploadKspFileFailed
Event Code	858
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{ clusterName}} upload KSP file failed.
Description	This event occurs when the cluster fails to upload the <i>ksp</i> file.
Auto Clearance	This event triggers the alarm 858, which is auto cleared by the event code 857.

## NTP unreachable server

**TABLE 523** NTP unreachable server

Event	NTP unreachable server
Event Type	NTP server reach failed
Event Code	859
Severity	Critical
Attribute	NTP server
Displayed on the web interface	System cannot reach NTP sever [NTP Server]
Description	This event occurs when system fails to reach the NTP server.

## Configuration backup started

**TABLE 524** Configuration backup started event

Event	Configuration backup started
Event Type	clusterCfgBackupStart
Event Code	860
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration backup is started.
Description	This event occurs when cluster configuration backup starts.

## Configuration backup succeeded

**TABLE 525** Configuration backup succeeded

Event	Configuration backup succeeded
Event Type	clusterCfgBackupSuccess
Event Code	861
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration backup succeeded.
Description	This event occurs when cluster backup configuration is successful.

## Configuration backup failed

**TABLE 526** Configuration backup failed event

Event	Configuration backup failed
Event Type	clusterCfgBackupFailed
Event Code	862
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration backup failed.
Description	This event occurs when backup configuration fails.
Auto Clearance	This event triggers the alarm 862, which is auto cleared by the event code 861.

## Configuration restore succeeded

**TABLE 527** Configuration restore succeeded event

Event	Configuration restore succeeded
Event Type	clusterCfgRestoreSuccess
Event Code	863

**TABLE 527** Configuration restore succeeded event (continued)

Event	Configuration restore succeeded
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration restore succeeded.
Description	This event occurs when the cluster restore configuration is successful.

## Configuration restore failed

**TABLE 528** Configuration restore failed event

Event	Configuration restore failed
Event Type	clusterCfgRestoreFailed
Event Code	864
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration restore failed.
Description	This event occurs when the restore configuration fails.
Auto Clearance	This event triggers the alarm 864, which is auto cleared by the event code 863.

## AP Certificate Expired

**TABLE 529** AP Certificate Expired event

Event	AP Certificate Expired
Event Type	apCertificateExpire
Event Code	865
Severity	Critical
Attribute	"count"="XXX"
Displayed on the web interface	{{count}} APs need to update their certificates.
Description	This event occurs when the AP certificate expires.
Auto Clearance	This event triggers the alarm 865, which is auto cleared by the event code 866.

## AP Certificate Updated

**TABLE 530** AP Certificate Updated event

Event	AP Certificate Updated
Event Type	apCertificateExpireClear
Event Code	866
Severity	Informational
Attribute	"count"="XXX"
Displayed on the web interface	{{count}} APs need to update their certificates.

**TABLE 530** AP Certificate Updated event (continued)

Event	AP Certificate Updated
Description	This event occurs when the AP certificates are updated.

## Configuration restore started

**TABLE 531** Configuration restore started event

Event	Configuration restore started
Event Type	clusterCfgRestoreStarted
Event Code	867
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration restore started.
Description	This event occurs when the cluster configuration is restored.

## Upgrade SStable failed

**TABLE 532** Upgrade SStable failed event

Event	Upgrade SStable failed
Event Type	upgradeSStableFailed
Event Code	868
Severity	Major
Attribute	"nodeName"="xxx"
Displayed on the web interface	Node [{nodeName}] upgrade SStable failed.
Description	This event occurs when the upgrade to the SS table fails.

## Reindex elastic search finished

**TABLE 533** Reindex elastic search finished event

Event	Reindex elastic search finished
Event Type	Reindex ElasticSearch finished
Event Code	869
Severity	Major
Attribute	
Displayed on the web interface	Reindex ElasticSearch finished.
Description	This event occurs when the re-index elastic search is completed.

## Initiated APs contact APR

**TABLE 534** Initiated APs contact APR event

Event	Initiated APs contact APR
Event Type	clusterInitContactApr
Event Code	870
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{ clusterName}] initiated APs contact APR
Description	This event occurs on receiving APs contact APR configuration command.

## All nodes back in service

**TABLE 535** All nodes back in service event

Event	All nodes back in service
Event Type	allNodeBackToInService
Event Code	871
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	All nodes in cluster [{clusterName}] are back in service.
Description	This event occurs when all nodes are back in service.

## Not management service ready

**TABLE 536** Not management service ready event

Event	Not management service ready
Event Type	allServiceOutOfService
Event Code	872
Severity	Informational
Attribute	"clusterName"="xx", "nodeName"="xx", "reason"="xxx"
Displayed on the web interface	Not all management services on Node [{nodeName}] in cluster [{clusterName}] are ready. Reason\:{reason}].
Description	This event occurs when any applications of the node is down and the management service state is marked as out of service

## Management service ready

**TABLE 537** Management service ready event

Event	Management service ready
Event Type	allServiceInService
Event Code	873
Severity	Informational

**TABLE 537** Management service ready event (continued)

Event	Management service ready
Attribute	"clusterName"="xx", "nodeName"="xx"
Displayed on the web interface	All management services on Node [{nodeName}] in cluster [{clusterName}] are ready
Description	This event occurs when all applications of the node is in service and the management service state is marked as in service.

## Configuration sync failed

**TABLE 538** Configuration sync failed event

Event	Configuration sync failed
Event Type	clusterRedundancySyncCfgFailed
Event Code	874
Severity	Major
Attribute	"clusterName"="xx", "reason"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration sync failed. Reason: [{reason}]
Description	This event occurs when synchronization configuration fails in a cluster redundancy.

## Node IPv6 address added

**TABLE 539** Node IPv6 address added event

Event	Node IPv6 address added
Event Type	nodeIPv6Added
Event Code	2501
Severity	Informational
Attribute	"nodeMac"="xxx", "ifName"="xx:xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Network interface [{networkInterface}   {ifName}] on node [{nodeName}] added IPv6 address [{ip}].
Description	This event occurs when the node adds the IPv6 address.

## AP is connected to standby cluster over the expiration date

**TABLE 540** AP is connected to standby cluster over the expiration date event

Event	AP is connected to standby cluster over the expiration date
Event Type	ApConnectedToStandbyClusterOverTheExpirationDate
Event Code	188
Severity	Critical
Attribute	apMac="xx:xx:xx:xx:xx:xx", days="xx"
Displayed on the web interface	The AP[{apMac}] is connected to standby cluster over [{days}] days, please move it to active cluster to avoid service interruption
Description	This event occurs when a AP is connected to standby cluster over the expiration date.

## Node IPv6 address deleted

**TABLE 541** Node IPv6 address deleted event

Event	Node IPv6 address deleted
Event Type	nodeIPv6Deleted
Event Code	2502
Severity	Informational
Attribute	"nodeMac"="xxx", "ifName"="xx:xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Network interface [{networkInterface}  ifName}] on node [{nodeName}] deleted IPv6 address [{ip}].
Description	This event occurs when the node deletes the IPv6 address.

## Sync Configuration started for Cluster Redundancy

**TABLE 542** Sync Configuration started for Cluster Redundancy Event

Event	Sync Configuration started for Cluster Redundancy
Event Type	SyncCfgStartClusterRedundancy
Event Code	875
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] sync configuration start for cluster redundancy.
Description	This event occurs when sync configuration start for cluster redundancy.

## Sync Configuration Success for Cluster Redundancy

**TABLE 543** Sync Configuration Success for Cluster Redundancy Event

Event	Sync Configuration Success for Cluster Redundancy
Event Type	SyncCfgSuccessClusterRedundancy
Event Code	876
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] sync configuration success for cluster redundancy.
Description	This event occurs when sync configuration success for cluster redundancy.

## Standby Cluster Failed to Restore a Configuration for Cluster Redundancy

**TABLE 544** Standby Cluster Failed to Restore a Configuration for Cluster Redundancy event

Event	Cluster restore failed
Event Type	RestoreClusterFailedforClusterRedundancy
Event Code	877
Severity	Major
Attribute	"clusterName"="xxx"



**TABLE 544** Standby Cluster Failed to Restore a Configuration for Cluster Redundancy event (continued)

Event	Cluster restore failed
Displayed on the web interface	Standby Cluster [{clusterName}] restore failed for cluster redundancy. Reason[{reason]}.
Description	This event occurs when standby cluster failed to restore a configuration for cluster redundancy.

## Standby Cluster Restores a Configuration for Cluster Redundancy

**TABLE 545** Standby Cluster Restores a Configuration for Cluster Redundancy event

Event	Standby Cluster Restores a Configuration for Cluster Redundancy
Event Type	StandbyClusterRestoresConfigurationForClusterRedundancy
Event Code	878
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] restores for cluster redundancy.
Description	This event occurs when standby cluster restored a configuration success for cluster redundancy.

## Standby Cluster Restored a Configuration Success for Cluster Redundancy

**TABLE 546** Standby Cluster Restored a Configuration Success for Cluster Redundancy event

Event	Standby Cluster Restored a Configuration Success for Cluster Redundancy
Event Type	StandbyClusterRestoredaConfigurationSuccessforClusterRedundancy
Event Code	879
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] restored a configuration success for cluster redundancy.
Description	This event occurs when standby cluster restored a configuration success for cluster redundancy.

## Standby Cluster Back to Monitoring Mode for Cluster Redundancy

**TABLE 547** Standby Cluster Back to Monitoring Mode for Cluster Redundancy event

Event	Standby Cluster Back to Monitoring Mode for Cluster Redundancy
Event Type	StandbyClusterBacktoMonitoringModeforClusterRedundancy
Event Code	880
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] back to monitoring mode for cluster redundancy.
Description	This event occurs when standby cluster back to monitoring mode for cluster redundancy.

## AP Connected to Standby Cluster after Rehome Timeout

**TABLE 548** AP Connected to Standby Cluster after Rehome Timeout event

Event	AP Connected to Standby Cluster after Rehome Timeout
Event Type	APConnectedtoStandbyClusterAfterRehomeTimeout
Event Code	881
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster {{clusterName}} AP connected after rehome timeout
Description	This event occurs when there is still AP connected to standby cluster after rehome timeout.

## Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy

**TABLE 549** Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy event

Event	Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Event Type	ActiveClusterUnabletoConnectOtherActiveCustersforClusterRedundancy
Event Code	882
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}} Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Description	This event occurs when active cluster unable to connect to other active clusters for cluster redundancy.

## External DP Connected to Standby Cluster after Rehome Timeout

**TABLE 550** External DP Connected to Standby Cluster after Rehome Timeout event

Event	External DP Connected to Standby Cluster after Rehome Timeout
Event Type	ExternalDPConnectedtoStandbyClusterafterRehomeTimeout
Event Code	887
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}}This event occurs when there is still external DP connected to standby cluster after rehome timeout
Description	This event occurs when there is still external DP connected to standby cluster after rehome timeout.

## Certificate is about to Expire

**TABLE 551** Certificate is about to Expire event

Event	Certificate is about to Expire
Event Type	certificateAboutToExpire
Event Code	890
Severity	Major

**TABLE 551** Certificate is about to Expire event (continued)

Event	Certificate is about to Expire
Attribute	"certName"="xxx", days="x", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate [{certName}] is about to expire in [{days}] days ({expireDateTime})
Description	This event occurs when certificate is about to expire.

## Certificate is already Expired

**TABLE 552** Certificate is already Expired event

Event	Certificate is already Expired
Event Type	certificateExpire
Event Code	891
Severity	Major
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate is already expired
Description	This event occurs when certificate is already expired

## Result of Renew Certificate

**TABLE 553** Result of Renew Certificate event

Event	Result of Renew Certificate
Event Type	certificateGenerateResult
Event Code	892
Severity	Major
Attribute	"certName"="xxx", "result"="xxx"
Displayed on the web interface	Result of renew certificate [{certName}] : {result}
Description	This event occurs to show the result of renew certificate

## Configuration Events

Following are the events related to configuration:

- [Configuration updated](#) on page 252
- [Configuration update failed](#) on page 252
- [Configuration receive failed](#) on page 252
- [Incorrect flat file configuration](#) on page 253
- [Zone configuration preparation failed](#) on page 253
- [AP configuration generation failed](#) on page 253
- [End-of-life AP model detected](#) on page 254
- [VLAN configuration mismatch on non-DHCP/NAT WLAN](#) on page 254

## Events Types

### Configuration Events

- [VLAN configuration mismatch on DHCP/NAT WLAN on page 254](#)
- [Generation failed during CCM GPB generation on page 255](#)
- [Preparation failed during AP knowledge generation on page 255](#)
- [Generation failed during AP knowledge generation on page 255](#)
- [End-of-life AP model detected during AP knowledge generation on page 256](#)
- [Notification failed during AP knowledge generation on page 256](#)

## Configuration updated

**TABLE 554** Configuration updated event

Event	Configuration updated
Event Type	cfgUpdSuccess
Event Code	1007
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" , "srcProcess"="cnr" , "realm"="NA" "processName"="aut" "SCGMgmtIp"="x.x.x.x" "cause"="xx"
Displayed on the web interface	Configuration [{{cause}}] applied successfully in [{{processName}}] process at {produce.short.name} [{{SCGMgmtIp}}]
Description	This event occurs when the configuration notification receiver (CNR) process successfully applies the configuration to the modules.

## Configuration update failed

**TABLE 555** Configuration update failed event

Event	Configuration update failed
Event Type	cfgUpdFailed
Event Code	1008
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" , "srcProcess"="cnr" "realm"="NA" "processName"="aut" "SCGMgmtIp"="x.x.x.x" "cause"="xx"
Displayed on the web interface	Failed to apply configuration [{{cause}}] in [{{processName}}] process at {produce.short.name} [{{SCGMgmtIp}}].
Description	This event occurs when the CNR receives a negative acknowledgment when applying the configuration settings to the module. Possible cause is that a particular process/module is down.

## Configuration receive failed

**TABLE 556** Configuration receive failed event

Event	Configuration receive failed
Event Type	cfgRcvFailed
Event Code	1009
Severity	Debug

**TABLE 556** Configuration receive failed event (continued)

Event	Configuration receive failed
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="cnr" "realm"="NA" "SCGMgmtIp"="x.x.x.x", "cause"="xx"
Displayed on the web interface	Failed to fetch configuration [{cause}] by CNR in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the CNR receives an error or negative acknowledgment/improper/incomplete information from the configuration change notifier (CCN).

## Incorrect flat file configuration

**TABLE 557** Incorrect flat file configuration event

Event	Incorrect flat file configuration
Event Type	incorrectFlatFileCfg
Event Code	1012
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut", "realm"="NA", "SCGMgmtIp"="xxx", "cause"="xxx", "file"="xx"
Displayed on the web interface	[[srcProcess]] detected an configuration parameter is incorrectly configured in file [[file]] at {produce.short.name} [{SCGMgmtIp}].
Description	This event occurs when any flat file configuration parameter is not semantically or syntactically correct.

## Zone configuration preparation failed

**TABLE 558** Zone configuration preparation failed event

Event	Zone configuration preparation failed
Event Type	zoneCfgPrepareFailed
Event Code	1021
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone"
Displayed on the web interface	Failed to prepare zone [{zoneName}] configuration required by ap configuration generation
Description	This event occurs when the controller is unable to prepare a zone configuration required by the AP.

## AP configuration generation failed

**TABLE 559** AP configuration generation failed event

Event	AP configuration generation failed
Event Type	apCfgGenFailed
Event Code	1022
Severity	Major

**TABLE 559** AP configuration generation failed event (continued)

Event	AP configuration generation failed
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "apCfgGenFailedCount"="25"
Displayed on the web interface	Failed to generate configuration for [{{apCfgGenFailedCount}}] AP(s) under zone[{{zoneName}}].
Description	This event occurs when the controller fails to generate the AP configuration under a particular zone.

## End-of-life AP model detected

**TABLE 560** End-of-life AP model detected event

Event	End-of-life AP model detected
Event Type	cfgGenSkippedDueToEolAp
Event Code	1023
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "model"="R300,T300"
Displayed on the web interface	Detected usage of end-of-life ap model(s)[{{model}}] while generating configuration for AP(s) under zone[{{zoneName}}].
Description	This event occurs when the controller detects the AP model's end-of-life under a certain zone.

**NOTE**

Refer to [Configuration Alarms](#) on page 74.

## VLAN configuration mismatch on non-DHCP/NAT WLAN

**TABLE 561** VLAN configuration mismatch on non-DHCP/NAT WLAN event

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN.
Event Type	apCfgNonDhcpNatWlanVlanConfigMismatch
Event Code	1024
Severity	Critical
Attribute	"ssid"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [{{apMac}}] detected VLAN configuration mismatch on non-DHCP/NAT WLAN [{{ssid}}]. Configured VLAN is [{{configuredVlan}}] and resolved VLAN is [{{vlanId}}]. Clients may not be able to get IP or access Internet.
Description	This event occurs when the AP detects a non DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

## VLAN configuration mismatch on DHCP/NAT WLAN

**TABLE 562** VLAN configuration mismatch on DHCP/NAT WLAN event

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on DHCP/NAT WLAN
Event Type	apCfgDhcpNatWlanVlanConfigMismatch

**TABLE 562** VLAN configuration mismatch on DHCP/NAT WLAN event (continued)

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on DHCP/NAT WLAN
Event Code	1025
Severity	Critical
Attribute	"ssid"="xxxx", "vlanID"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [apMac] detected VLAN configuration mismatch on DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This event occurs when the AP detects a DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

## Generation failed during CCM GPB generation

**TABLE 563** Generation failed during CCM GPB generation event

Event	Generation failed during CCM (Common Configuration Module) GPB (Google Protocol Buffer) generation
Event Type	ccmGpbGenerateFailed
Event Code	9001
Severity	Major
Attribute	topicName = "SimpleTopci"
Displayed on the web interface	Failed to generate [{topicName}] GPB
Description	This event occurs when controller fails to generate GPB (Google Protocol Buffer) for a certain topic.

## Preparation failed during AP knowledge generation

**TABLE 564** Preparation failed during AP knowledge generation event

Event	Preparation failed during AP knowledge generation
Event Type	ccmApTraversalPrepareFailed
Event Code	9021
Severity	Major
Attribute	topicName = "SimpleTopci"
Displayed on the web interface	Failed to generate [{topicName}] GPB
Description	This event occurs when controller fails to generate GPB for a certain topic.

## Generation failed during AP knowledge generation

**TABLE 565** Generation failed during AP knowledge generation event

Event	Generation failed during AP knowledge generation
Event Type	ccmApTraversalGenerateFailed
Event Code	9022

**TABLE 565** Generation failed during AP knowledge generation event (continued)

Event	Generation failed during AP knowledge generation
Severity	Major
Attribute	apCfgGenFailedCount = "3", zoneName = "myZone"
Displayed on the web interface	Failed to execute generation during AP knowledge generation for [apCfgGenFailedCount] AP(s) under zone[zoneName].
Description	This event occurs when controller fails to complete generation phase during AP knowledge generation for any AP under a certain zone.

## End-of-life AP model detected during AP knowledge generation

**TABLE 566** End-of-life AP model detected during AP knowledge generation event

Event	End-of-life AP model detected during AP knowledge generation
Event Type	ccmApTraversalGenerateSkippedDueToEolAp
Event Code	9023
Severity	Major
Attribute	model = "CcmModel", zoneName = "myZone"
Displayed on the web interface	Detected usage of end-of-life AP model(s)[model] while executing AP knowledge generation for AP(s) under zone[zoneName]
Description	This event occurs when controller detects an APs end of life under a certain zone.

## Notification failed during AP knowledge generation

**TABLE 567** Notification failed during AP knowledge generation event

Event	Notification failed during AP knowledge generation
Event Type	ccmApTraversalNotifyFailed
Event Code	9024
Severity	Major
Attribute	apCfgNotifyFailedCount = "3", zoneName = "myZone"
Displayed on the web interface	Failed to execute notification during AP knowledge generation for [apCfgNotifyFailedCount] AP(s) under zone[zoneName].
Description	This event occurs when controller fails to complete notification phase during AP knowledge generation for any AP under a certain zone.

## Datablade Events

The following are the events related to Datablade Based Service.

- [DP integrity test failed](#) on page 257
- [DP CLI enable failed](#) on page 257
- [DP re-authentication](#) on page 258
- [DP password min length updated](#) on page 258
- [DP password changed](#) on page 258
- [DP enable password changed](#) on page 258



- [DP https authentication failed](#) on page 259
- [DP certificate uploaded](#) on page 259
- [DP Scg FQDN updated](#) on page 259
- [DP initial upgrade](#) on page 260
- [DP discontinuous time change NTP server DP Ntp time sync](#) on page 260
- [DP user login](#) on page 260
- [DP user login failed](#) on page 260
- [DP user logout](#) on page 261
- [DP account locked](#) on page 261
- [DP session idle updated](#) on page 261
- [DP session idle terminated](#) on page 262
- [DP SSH tunnel failed](#) on page 262
- [DP https connection failed](#) on page 262
- [DP IPsec tunnel create failed](#) on page 262

## DP integrity test failed

**TABLE 568** DP integrity test failed event

Event	DP integrity test failed
Event Type	dpIntegrityTestFailed
Event Code	99200
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	Data plane [{dpKey}] self integrity test failed
Description	This event occurs when the data plane self integrity test failed.

## DP CLI enable failed

**TABLE 569** DP CLI enable failed event

Event	DP CLI enable failed
Event Type	dpCliEnableFailed
Event Code	99201
Severity	Informational
Attribute	"dpKey"="XXXX", "source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] CLI enabled failed, [{source}].
Description	This event occurs when the data plane CLI enabled failed.

## DP re-authentication

**TABLE 570** DP re-authentication event

Event	DP re-authentication
Event Type	dpReAuth
Event Code	99202
Severity	Informational
Attribute	"dpKey"="XXX", "Source"="x.x.x.x/console/WebGUI"
Displayed on the web interface	Data plane [{dpKey}] attempt to re-authenticate, [{source}].
Description	This event occurs when the data plane attempt to re-authenticate.

## DP password min length updated

**TABLE 571** DP password min length updated event

Event	DP password min length updated
Event Type	dpPasswordMinLengthUpdated
Event Code	99203
Severity	Informational
Attribute	"dpKey"="XXX", "Source"="x.x.x.x/console/webGUI"
Displayed on the web interface	Data plane [{dpKey}] min password length changed, [{source}].
Description	This event occurs when the data plane min password length changed.

## DP password changed

**TABLE 572** DP password changed event

Event	DP password changed
Event Type	dpPasswordChanged
Event Code	99204
Severity	Informational
Attribute	"dpKey"="XXX", "Source"="x.x.x.x/console/webGUI"
Displayed on the web interface	Data plane [{dpKey}] password changed, [{source}].
Description	This event occurs when the data plane password changed.

## DP enable password changed

**TABLE 573** DP enable password changed event

Event	DP enable password changed
Event Type	dpEnablePasswordChanged
Event Code	99205
Severity	Informational

**TABLE 573** DP enable password changed event (continued)

Event	DP enable password changed
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] enable password changed, [{source}].
Description	This event occurs when the data plane enable password changed.

## DP https authentication failed

**TABLE 574** DP https authentication failed event

Event	DP https authentication failed
Event Type	dpHttpsAuthFailed
Event Code	99206
Severity	Informational
Attribute	"dpKey"="XXXX", "reason"="xxx"
Displayed on the web interface	Data plane [{dpKey}] certificate verification failed, [{source}].
Description	This event occurs when the data plane certificate verification failed.

## DP certificate uploaded

**TABLE 575** DP certificate uploaded event

Event	DP certificate uploaded
Event Type	dpCertUploaded
Event Code	99207
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	Data plane [{dpKey}] certificate trusted CA chain uploaded.
Description	This event occurs when the data plane certificate trusted CA chain uploaded.

## DP Scg FQDN updated

**TABLE 576** DP Scg FQDN updated event

Event	DP Scg FQDN updated
Event Type	dpScgFqdnUpdated
Event Code	99208
Severity	Informational
Attribute	"dpKey"="XXXX", "fqdn"="xxx.xxx.xxx"
Displayed on the web interface	SZ [{scgIP}] FQDN [{fqdn}] setting on DP [{dpKey}].
Description	This event occurs when the SZ FQDN setting on data plane.

## DP initial upgrade

**TABLE 577** DP initial upgrade event

Event	DP initial upgrade
Event Type	dpInitUpgrade
Event Code	99210
Severity	Informational
Attribute	"dpKey"="XXXX", "source"="xxx"
Displayed on the web interface	Data plane [{dpKey}] initiate to upgrade, [{source}].
Description	This event occurs when the data plane initiate to upgrade.

## DP discontinuous time change NTP server DP Ntp time sync

**TABLE 578** DP discontinuous time change NTP server DP Ntp time sync event

Event	DP discontinuous time change NTP server DP Ntp time sync
Event Type	dpDiscontinuousTimeChangeNTPServerdpNtpTimeSync
Event Code	99211
Severity	Informational
Attribute	"dpKey"="XXXX", "before"="XXXX", "after"="XXXX", "source"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] time change due to ntp sync, from [{before}] to [{after}], Source: [{source}].
Description	This event occurs when the data plane time change due to ntp sync.

## DP user login

**TABLE 579** DP user login event

Event	DP user login
Event Type	dpUserLogin
Event Code	99212
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User login into data plane [{dpKey}], Source: [{source}].
Description	This event occurs when the user login into data plane.

## DP user login failed

**TABLE 580** DP user login failed event

Event	DP user login failed
Event Type	dpUserLoginFailed
Event Code	99213
Severity	Informational

**TABLE 580** DP user login failed event (continued)

Event	DP user login failed
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User login into data plane [{dpKey}] and failed, Source: [{source}].
Description	This event occurs when the user login into data plane and failed.

## DP user logout

**TABLE 581** DP user logout event

Event	DP user logout
Event Type	dpUserLogout
Event Code	99214
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User logout to data plane [{dpKey}], Source: [{source}].
Description	This event occurs when the user logout to data plane.

## DP account locked

**TABLE 582** DP account locked event

Event	DP account locked
Event Type	dpAccountLocked
Event Code	99215
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	User account was locked, data plane: [{dpKey}].
Description	This event occurs when the user account was locked.

## DP session idle updated

**TABLE 583** DP session idle updated event

Event	DP session idle updated
Event Type	dpSessionIdleUpdated
Event Code	99220
Severity	Informational
Attribute	"dpKey"="XXXX", "sessionIdle"="xx", "Source"="console/webGui"
Displayed on the web interface	Data plane [{dpKey}] session timeout [{sessionIdle}] change, [{source}].
Description	This event occurs when the data plane session timeout change.

## DP session idle terminated

**TABLE 584** DP session idle terminated event

Event	DP session idle terminated
Event Type	dpSessionIdleTerminated
Event Code	99221
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] session terminated due to timeout, [{source}].
Description	This event occurs when the data plane session terminated due to timeout.

## DP SSH tunnel failed

**TABLE 585** DP SSH tunnel failed event

Event	DP SSH tunnel failed
Event Type	dpSshTunnFailed
Event Code	99230
Severity	Informational
Attribute	"dpKey"="XXXX", "scgIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] establish ssh tunnel failed, SZ [{scgIP}].
Description	This event occurs when the data plane establish ssh tunnel failed.

## DP https connection failed

**TABLE 586** DP https connection failed event

Event	DP https connection failed
Event Type	dpHttpsConnFailed
Event Code	99231
Severity	Informational
Attribute	"dpKey"="XXXX", "scgIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] https connection failed, SZ [{scgIP}].
Description	This event occurs when the data plane https connection failed.

## DP IPsec tunnel create failed

**TABLE 587** DP IPsec tunnel create failed event

Event	DP IPsec tunnel create failed
Event Type	dpIPsecTunnCreateFailed
Event Code	99240
Severity	Informational

**TABLE 587** DP IPsec tunnel create failed event (continued)

Event	DP IPsec tunnel create failed
Attribute	"dpKey"="XXXX", "dpIP"="x.x.x.x", apIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey&&dpIP}] IPsec tunnel establishment failed, AP [{apIP}].
Description	This event occurs when the data plane IPsec tunnel establishment failed.

## Data Plane Events

**NOTE**

Events 530, 532, 537, 538, 550, 551, 552 and 553 are not applicable for SZ300/SZ100.

Following are the events related to the data plane:

Event	Event	Event
Data plane discovered on page 263	Data plane discovery failed on page 264	Data plane configuration updated on page 264
Data plane configuration update failed on page 264	Data plane rebooted on page 265	Data plane heartbeat lost on page 265
Data plane IP address updated on page 265	Data plane updated to a new control plane on page 265	Data plane status update failed on page 266
Data plane statistics update failed on page 266	Data plane connected on page 266	Data plane disconnected on page 267
Data plane physical interface down on page 267	Data plane physical interface up on page 267	Data plane packet pool is under low water mark on page 267
Data plane packet pool is under critical low water mark on page 268	Data plane packet pool is above high water mark on page 268	Data plane core dead on page 268
Data plane process restarted on page 269	Data plane discovery succeeded on page 269	Data plane managed on page 269
Data plane deleted on page 270	Data plane license is not enough on page 270	Data plane upgrade started on page 270
Data plane upgrading on page 271	Data plane upgrade succeeded on page 271	Data plane upgrade failed on page 271
Data plane of data center side successfully connects to the CALEA server on page 272	Data plane of data center side fails to connect to the CALEA server on page 272	Data Plane of data center side disconnects to CALEA server on page 272
Data plane successfully connects to the other data plane on page 273	Data plane fails to connect to the other data plane on page 273	Data plane disconnects to the other data plane on page 273
Start CALEA mirroring client in data plane on page 274	Stop CALEA mirroring client in data plane on page 274	Data plane DHCP IP pool usage rate is 100 percent on page 274
Data plane DHCP IP pool usage rate is 80 percent on page 275	Data plane NAT session capacity usage rate is 80 percent on page 275	Data plane NAT session capacity usage rate is 100 percent on page 276
Data plane DHCP IP capacity usage rate is 80 percent on page 276	Data plane DHCP IP capacity usage rate is 100 percent on page 276	Data plane backup success on page 277
Data plane backup failed on page 277	Data plane restore success on page 277	Data plane restore failed on page 278
Remote Administration Start on page 280	Remote Administration Stop on page 281	

## Data plane discovered

**TABLE 588** Data plane discovered event

Event	Data plane discovered
Event Type	dpDiscoverySuccess (server side detect)
Event Code	501

**TABLE 588** Data plane discovered event (continued)

Event	Data plane discovered
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane {{dpName   dpKey}} sent a connection request to {produce.short.name} {{cpName   wsgIP}}.
Description	This event occurs when the data plane successfully connects to the controller.

## Data plane discovery failed

**TABLE 589** Data plane discovery failed event

Event	Data plane discovery failed
Event Type	dpDiscoveryFail (detected on the server side)
Event Code	502
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane {{dpName   dpKey}} failed to send a discovery request to {produce.short.name} {{cpName   wsgIP}}.
Description	This event occurs when the data plane fails to connect to the controller.

## Data plane configuration updated

**TABLE 590** Data plane configuration updated event

Event	Data plane configuration updated
Event Type	dpConfUpdated
Event Code	504
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"= "123456781234567"
Displayed on the web interface	Data plane {{dpName   dpKey}} updated to configuration {{configID}}.
Description	This event occurs when the data plane configuration is updated.

## Data plane configuration update failed

**TABLE 591** Data plane configuration update failed event

Event	Data plane configuration update failed
Event Type	dpConfUpdateFailed
Event Code	505
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"=" 123456781234567"
Displayed on the web interface	Data plane {{dpName   dpKey}} failed to update to configuration {{configID}}
Description	This event occurs when the data plane configuration update fails.
Auto Clearance	This event triggers the alarm 501, which is auto cleared by the event code 504.



## Data plane rebooted

**TABLE 592** Data plane rebooted event

Event	Data plane rebooted
Event Type	dpReboot (server side detect)
Event Code	506
Severity	Minor
Attribute	"dpKey"="xx:xx:xx:xx:xx",
Displayed on the web interface	Data plane [{dpName}   dpKey]} rebooted
Description	This event occurs when the data plane is rebooted.

## Data plane heartbeat lost

**TABLE 593** Data plane heartbeat lost event

Event	Data plane heartbeat lost
Event Type	dpLostConnection (detected on the server side)
Event Code	507
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx",
Displayed on the web interface	Data plane [{dpName}   dpKey]} heartbeat lost.
Description	This event occurs when the data plane heartbeat lost.

## Data plane IP address updated

**TABLE 594** Data plane IP address updated event

Event	Data plane IP address updated
Event Type	dpIPChanged
Event Code	508
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx",
Displayed on the web interface	Data plane [{dpName}   dpKey]} IP address changed
Description	This event occurs when the IP address of the data plane is modified.

## Data plane updated to a new control plane

**TABLE 595** Data plane updated to a new control plane event

Event	Data plane updated to a new control plane
Event Type	dpChangeControlBlade
Event Code	509
Severity	Informational

## Events Types

### Data Plane Events

**TABLE 595** Data plane updated to a new control plane event (continued)

Event	Data plane updated to a new control plane
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "oldwsgIP"="xxx.xxx.xxx.xxx", "newwsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] switched from {produce.short.name} [{oldCpName   oldWsgIP}] to [{cpName   newWsgIP}].
Description	This event occurs when the data plane connects to a new controller instance.

## Data plane status update failed

**TABLE 596** Data plane status update failed event

Event	Data plane status update failed
Event Type	dpUpdateStatusFailed
Event Code	510
Severity	Minor
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] failed to update its status to {produce.short.name} [{cpName   wsgIP}].
Description	This event occurs when the data plane fails to update its status on the controller.

## Data plane statistics update failed

**TABLE 597** Data plane statistics update failed event

Event	Data plane statistics update failed
Event Type	dpUpdateStatisticFailed
Event Code	511
Severity	Minor
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] failed to update its statistics to {produce.short.name} [{cpName   wsgIP}].
Description	This event occurs when the data plane fails to update statistics to the controller.

## Data plane connected

**TABLE 598** Data plane connected event

Event	Data plane connected
Event Type	dpConnected
Event Code	512
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] connected to {produce.short.name} [{cpName   wsgIP}].
Description	This event occurs when the data plane connects to the controller.

## Data plane disconnected

**TABLE 599** Data plane disconnected event

Event	Data plane disconnected
Event Type	dpDisconnected
Event Code	513
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName}   {dpKey}] disconnected from {produce.short.name} {cpName}   {wsgIP}.
Description	This event occurs when the data plane disconnects from the controller.
Auto Clearance	This event triggers the alarm 503, which is auto cleared by the event code 512.

## Data plane physical interface down

**TABLE 600** Data plane physical interface down event

Event	Data plane physical interface down
Event Type	dpPhyInterfaceDown
Event Code	514
Severity	Critical
Attribute	"portID"="xx", "dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName}   {dpKey}] is down.
Description	This event occurs when the network link of the data plane is down.
Auto Clearance	This event triggers the alarm 504, which is auto cleared by the event code 515.

## Data plane physical interface up

**TABLE 601** Data plane physical interface up event

Event	Data plane physical interface up
Event Type	dpPhyInterfaceUp
Event Code	515
Severity	Informational
Attribute	"portID"="xx", "dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName}   {dpKey}] is up.
Description	This event occurs when the network link of the data plane is up.

## Data plane packet pool is under low water mark

**TABLE 602** Data plane packet pool is under low water mark event

Event	Data plane packet pool is under low water mark
Event Type	dpPktPoolLow

## Events Types

### Data Plane Events

**TABLE 602** Data plane packet pool is under low water mark event (continued)

Event	Data plane packet pool is under low water mark
Event Code	516
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName   dpKey}] is under low-water mark.
Description	This event occurs when the data core packet pool is below the water mark level.
Auto Clearance	This event triggers the alarm 516, which is auto cleared by the event code 518.

## Data plane packet pool is under critical low water mark

**TABLE 603** Data plane's packet pool is under critical low water mark event

Event	Data plane packet pool is under critical low water mark
Event Type	dpPktPoolCriticalLow
Event Code	517
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName   dpKey}] is under critical low-water mark.
Description	This event occurs when the data core packet pool reaches the critical water mark level.

## Data plane packet pool is above high water mark

**TABLE 604** Data plane packet pool is above high water mark event

Event	Data plane packet pool is above high water mark
Event Type	dpPktPoolRecover
Event Code	518
Severity	Informational
Attribute	dpKey="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName   dpKey}] is above high-water mark
Description	This event occurs when the data plane's packet pool is recovered when it is above high-water mark.

## Data plane core dead

**TABLE 605** Data plane core dead event

Event	Data plane core dead
Event Type	dpCoreDead
Event Code	519
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx"

**TABLE 605** Data plane core dead event (continued)

Event	Data plane core dead
Displayed on the web interface	Data plane {{dpName&&dpKey}} has dead data core.
Description	This event occurs when one or multiple data core packet pool is lost /dead.

## Data plane process restarted

**TABLE 606** Data plane process restarted event

Event	Data plane process restarted
Event Type	dpProcessRestart
Event Code	520
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	{{processName}} on data plane {{dpName&&dpKey}} is restarted.
Description	This event occurs when any process on the data plane crashes and restarts.

**NOTE**

Event 530 is not applicable for SCG.

## Data plane discovery succeeded

**NOTE**

This event is not applicable to SZ300/SZ100.

**TABLE 607** Data plane discovery succeeded event

Event	Data plane discovery succeeded
Event Type	dpDiscoverySuccess
Event Code	530
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane {{dpName&&dpKey}} sent a discovery request to {produce.short.name} {{wsgIP}}.
Description	This event occurs when data plane sends a discovery request to the {produce.short.name} successfully.

## Data plane managed

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 608** Data plane managed event

Event	Data plane managed
Event Type	dpStatusManaged

## Events Types

### Data Plane Events

**TABLE 608** Data plane managed event (continued)

Event	Data plane managed
Event Code	532
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] approved by {produce.short.name} [{wsgIP}].
Description	This event occurs when data plane is approved by the {produce.short.name}.

#### NOTE

Events 537, 538, 550, 551, 552 and 553 are not applicable for SZ300/SZ100.

## Data plane deleted

**TABLE 609** Data plane deleted event

Event	Data plane deleted
Event Type	dpDeleted
Event Code	537
Severity	Informational
Attribute	"dpKey"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] deleted.
Description	This event occurs when data plane is deleted.

## Data plane license is not enough

**TABLE 610** Data plane license is not enough event

Event	Data plane license is not enough
Event Type	dpLicenseInsufficient
Event Code	538
Severity	Major
Attribute	"count"=<delete-vdp-count>
Displayed on the web interface	Data plane license is not enough, [{count}] instance of data plane will be deleted.
Description	This event occurs when data plane licenses are insufficient.

## Data plane upgrade started

**TABLE 611** Data plane upgrade started event

Event	Data plane upgrade started
Event Type	dpUpgradeStart
Event Code	550
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"

**TABLE 611** Data plane upgrade started event (continued)

Event	Data plane upgrade started
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] started the upgrade process.
Description	This event occurs when data plane starts the upgrade process.

## Data plane upgrading

**TABLE 612** Data plane upgrading event

Event	Data plane upgrading
Event Type	dpUpgrading
Event Code	551
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] is upgrading.
Description	This event occurs when data plane starts to upgrade programs and configuration.

## Data plane upgrade succeeded

**TABLE 613** Data plane upgrade succeeded event

Event	Data plane upgrade succeeded
Event Type	dpUpgradeSuccess
Event Code	552
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] has been upgraded successfully.
Description	This event occurs when data plane upgrade is successful.

## Data plane upgrade failed

**TABLE 614** Data plane upgrade failed event

Event	Data plane upgrade failed
Event Type	dpUpgradeFailed
Event Code	553
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] failed to upgrade.
Description	This event occurs when data plane upgrade fails.
Auto Clearance	This event triggers the alarm 553, which is auto cleared by the event code 552.

## Data plane of data center side successfully connects to the CALEA server

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 615** Data plane of data center side successfully connects to the CALEA server event

Event	Data plane of data center side successfully connects to the CALEA server
Event Type	dpDcToCaleaConnected
Event Code	1257
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [{dpName&&dpKey}] successfully connects to the CALEA server[{caleaServerIP}].
Description	This event occurs when the data plane successfully connects to the CALEA server.

## Data plane of data center side fails to connect to the CALEA server

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 616** Data plane of data center side fails to connect to the CALEA server event

Event	Data plane of data center side fails to connect to the CALEA server.
Event Type	dpDcToCaleaConnectFail
Event Code	1258
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [{dpName&&dpKey}] fails to connects to the CALEA server[{caleaServerIP}].
Description	This event occurs when the data plane fails to connect to the CALEA server.
Auto Clearance	This event triggers the alarm 1258, which is auto cleared by the event code 1257.

## Data Plane of data center side disconnects to CALEA server

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 617** Data Plane of data center side disconnects to CALEA server event

Event	Data Plane of data center side disconnects to CALEA server.
Event Type	dpDcToCaleaDisconnected
Event Code	1259
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [{dpName&&dpKey}] fails to connects to the CALEA server [{caleaServerIP}].



**TABLE 617** Data Plane of data center side disconnects to CALEA server event (continued)

Event	Data Plane of data center side disconnects to CALEA server.
Description	This event occurs when the data plane disconnects from the CALEA server.

## Data plane successfully connects to the other data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 618** Data plane successfully connects to the other data plane event

Event	Data plane successfully connects to the other data plane
Event Type	dpP2PTunnelConnected
Event Code	1260
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dplP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDplp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] successfully connects to the other Data Plane[{targetDpKey&&targetDplp}]
Description	This event occurs when the data plane connects to another data plane.

## Data plane fails to connect to the other data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 619** Data plane fails to connect to the other data plane event

Event	Data plane fails to connect to the other data plane
Event Type	dpP2PTunnelConnectFail
Event Code	1261
Severity	Warning
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dplP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDplp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] fails connects to the other Data Plane[{targetDpKey&&targetDplp}]
Description	This event occurs when the data plane fails to connect to another data plane.
Auto Clearance	This event triggers the alarm 1261, which is auto cleared by the event code 1260.

## Data plane disconnects to the other data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 620** Data plane disconnects to the other data plane event

Event	Data plane disconnects to the other data plane
Event Type	dpP2PTunnelDisconnected
Event Code	1262

## Events Types

### Data Plane Events

**TABLE 620** Data plane disconnects to the other data plane event (continued)

Event	Data plane disconnects to the other data plane
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dplP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx","targetDplp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] disconnects to the other Data Plane[{targetDpKey&&targetDplp}]
Description	This event occurs when the data plane disconnects from another data plane.

## Start CALEA mirroring client in data plane

### NOTE

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 621** Start CALEA mirroring client in data plane event

Event	Start CALEA mirroring client in data plane
Event Type	dpStartMirroringClient
Event Code	1263
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dplP"="xx.xx.xx.xx"
Displayed on the web interface	Start CALEA mirroring client [{userName}   IP   {clientMac}] on WLAN [{ssid}] from AP [{apName&&apMac}]
Description	This event occurs when the CALEA server starts mirroring the client image.

## Stop CALEA mirroring client in data plane

### NOTE

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 622** Stop CALEA mirroring client in data plane event

Event	Stop CALEA mirroring client in data plane
Event Type	dpStopMirroringClient
Event Code	1264
Severity	Warning
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dplP"="xx.xx.xx.xx"
Displayed on the web interface	Stop CALEA mirroring client [{userName}   IP   {clientMac}] on WLAN [{ssid}   authType] from AP [{apName&&apMac}]. TxBytes[{txBytes}]
Description	This event occurs when the CALEA server stops mirroring the client image.

## Data plane DHCP IP pool usage rate is 100 percent

### NOTE

This event is not applicable for SZ300/SZ100.

**TABLE 623** Data plane DHCP IP pool usage rate is 100 percent event

Event	Data plane DHCP IP pool usage rate is 100 percent
Event Type	dpDhcpIpPoolUsageRate100
Event Code	1265
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane[{{dpName&&dpKey}} DHCP IP Pool usage rate is 100 percent
Description	This event occurs when the data plane DHCP pool usage rate is 100%.

## Data plane DHCP IP pool usage rate is 80 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 624** Data plane DHCP IP pool usage rate is 80 percent event

Event	Data plane DHCP IP pool usage rate is 80 percent
Event Type	dpDhcpIpPoolUsageRate80
Event Code	1266
Severity	Warning
Attribute	"dpName"="xxxxxxx", "dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane[{{dpName&&dpKey}} DHCP IP Pool usage rate is 80 percent
Description	This event occurs when the data plane DHCP pool usage rate is 80%.

## Data plane NAT session capacity usage rate is 80 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 625** Data plane NAT session capacity usage rate is 80 percent event

Event	Data plane NAT session capacity usage rate is 80 percent
Event Type	dpNatSessionCapacityUsageRate80
Event Code	1283
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{{dpKey}} NAT Session Capacity usage rate is 80 percent. ( total {{totalLicenseCnt}}, consumed {{consumedLicenseCnt}}, available {{availableLicenseCnt}} )
Description	This event occurs when the data plane NAT session capacity usage rate is 80%.

## Data plane NAT session capacity usage rate is 100 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 626** Data plane NAT session capacity usage rate is 100 percent event

Event	Data plane NAT session capacity usage rate is 100 percent
Event Type	dpNatSessionCapacityUsageRate100
Event Code	1284
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] NAT Session Capacity usage rate is 100 percent. (total [totalLicenseCnt], consumed [consumedLicenseCnt], available [availableLicenseCnt])
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

## Data plane DHCP IP capacity usage rate is 80 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 627** Data plane DHCP IP capacity usage rate is 80 percent event

Event	Data plane DHCP IP capacity usage rate is 80 percent
Event Type	dpDhcpIpCapacityUsageRate80
Event Code	1285
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] DHCP IP Capacity usage rate is 80 percent. (total [totalLicenseCnt], consumed [consumedLicenseCnt], available [availableLicenseCnt])
Description	This event occurs when the data plane DHCP IP capacity usage rate is 80%.

## Data plane DHCP IP capacity usage rate is 100 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 628** Data plane DHCP IP capacity usage rate is 100 percent event

Event	Data plane DHCP IP capacity usage rate is 100 percent
Event Type	dpDhcpIpCapacityUsageRate100
Event Code	1286
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"

**TABLE 628** Data plane DHCP IP capacity usage rate is 100 percent event (continued)

Event	Data plane DHCP IP capacity usage rate is 100 percent
Displayed on the web interface	Data Plane{{dpKey}} DHCP IP Capacity usage rate is 100 percent. (total {{totalLicenseCnt}}, consumed {{consumedLicenseCnt}}, available {{availableLicenseCnt}})
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

## Data plane backup success

**TABLE 629** Data plane backup success event

Event	Data plane backup success
Event Type	dpBackupSuccess
Event Code	1290
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane {{dpName&&dpKey}} backup successful.
Description	This event occurs when Data plane backup is successful.

## Data plane backup failed

**TABLE 630** Data plane backup failed event

Event	Data plane backup failed
Event Type	dpBackupFailed
Event Code	1291
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane {{dpName&&dpKey}} backup failed.
Description	This event occurs when Data plane backup fails.

## Data plane restore success

**TABLE 631** Data plane restore success event

Event	Data plane restore success
Event Type	dpRestoreSuccess
Event Code	1292
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane {{dpName&&dpKey}} restore successful.
Description	This event occurs when Data plane restore is successful.

## Data plane restore failed

**TABLE 632** Data plane restore failed event

Event	Data plane restore failed
Event Type	dpRestoreFailed
Event Code	1293
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] restore failed.
Description	This event occurs when Data plane restore fails.

## dplpmiPsStatus

**TABLE 633** dplpmiPsStatus event

Event	dplpmiPsStatus
Event Type	dplpmiPsStatus
Event Code	2901
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The voltage [{status}] on the data plane [{dpName&&dpKey}]..
Description	This event occurs when the voltage status on the data plane is sent.

## dplpmiThempIOH

**TABLE 634** dplpmiThempIOH event

Event	dplpmiThempIOH
Event Type	dplpmiThempIOH
Event Code	2904
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	IOH temperature [{status}] on data plane [{dpName&&dpKey}]..
Description	This event occurs when the IOH temperature status on the data plane is sent..

## dplpmiThempMemP

**TABLE 635** dplpmiThempMemP event

Event	dplpmiThempMemP
Event Type	dplpmiThempMemP
Event Code	2905
Severity	Major

**TABLE 635** dplpmiThempMemP event (continued)

Event	dplpmiThempMemP
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	The processor memory temperature [{status}] on the data plane[{dpName&&dpKey}].
Description	This event occurs when the processor memory temperature status on the data plane is sent.

## dplpmiPsStatus

**TABLE 636** dplpmiPsStatus event

Event	dplpmiPsStatus
Event Type	dplpmiPsStatus
Event Code	2913
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the power supply status on the data plane is sent.

## dplpmiREVoltage

**TABLE 637** dplpmiREVoltage event

Event	dplpmiREVoltage
Event Type	dplpmiREVoltage
Event Code	2926
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	The voltage [{status}] on the data plane [{dpName&&dpKey}]]
Description	This event occurs when the baseboard temperature status recover from the abnormal condition.

## dplpmiREThempIOH

**TABLE 638** dplpmiREThempIOH event

Event	dplpmiREThempIOH
Event Type	dplpmiREThempIOH
Event Code	2929
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	IOH temperature [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the IOH temperature status recover from abnormal condition.

## dplpmiREThempMemP

**TABLE 639** dplpmiREThempMemP event

Event	dplpmiREThempMemP
Event Type	dplpmiREThempMemP
Event Code	2930
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	The processor memory temperature [{status}] on the data plane[{dpName&&dpKey}].
Description	This event occurs when the processor memory temperature status recover from abnormal condition.

## dplpmiRePsStatus

**TABLE 640** dplpmiRePsStatus event

Event	dplpmiRePsStatus
Event Type	dplpmiRePsStatus
Event Code	2938
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the power supply status recover from abnormal condition.

## dpSSDHealthDegrade

**TABLE 641** dpSSDHealthDegrade event

Event	dpSSDHealthDegrade
Event Type	dpSSDHealthDegrade
Event Code	2961
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	The SSD health is degrading on data plane [{dpName&&dpKey}]. [{status}]
Description	This event occurs when SSD health is degrading.

## Remote Administration Start

**TABLE 642** Remote administration event

Event	Remote administration
Event Type	dpremoteadministration
Event Code	99250
Severity	Major



**TABLE 642** Remote administration event (continued)

Event	Remote administration
Attribute	No attributes for this event.
Displayed on the web interface	No web interface for this event.
Description	This event occurs when data plane SSHD starts.

## Remote Administration Stop

**TABLE 643** Remote administration event

Event	Remote administration event
Event Type	remoteadministration
Event Code	99251
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	No web interface for this event.
Description	This event occurs when data plane SSHD stops.

## Data Streaming Event

[Connected to Data a Streaming Endpoint](#) on page 281

[Disconnected to Data a Streaming Endpoint](#) on page 281

[Connected to Data a Streaming Endpoint Failure](#) on page 282

## Connected to Data a Streaming Endpoint

**TABLE 644** Connected to Data a Streaming Endpoint event

Event	Connected to Data a Streaming Endpoint
Event Type	connectedtoDataStreamingEndpoint
Event Code	4701
Severity	Informational
Displayed on the web interface	Connect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ connected to data a streaming endpoint.

## Disconnected to Data a Streaming Endpoint

**TABLE 645** Disconnected to Data a Streaming Endpoint event

Event	Disconnected to Data a Streaming Endpoint
Event Type	disconnectedtoDataStreamingEndpoint
Event Code	4702

**TABLE 645** Disconnected to Data a Streaming Endpoint event (continued)

Event	Disconnected to Data a Streaming Endpoint
Severity	Warning
Displayed on the web interface	Disconnect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ disconnected to data a streaming endpoint.

## Connected to Data a Streaming Endpoint Failure

**TABLE 646** Connected to Data a Streaming Endpoint Failure event

Event	Connected to Data a Streaming Endpoint Failure
Event Type	connectingFailure
Event Code	4703
Severity	Critical
Displayed on the web interface	name="xxxxx", connectorType="SCI", "ip"="2.2.2.2", "port"="8883"
Description	This event occurs when SZ try to connect to a data streaming profile but failure.

## DHCP Events

**NOTE**

This event is not applicable for vSZ-H.

Following are the events related to DHCP (Dynamic Host Configuration Protocol).

- [DHCP inform received](#) on page 282
- [DHCP dcln received](#) on page 283

## DHCP inform received

**TABLE 647** DHCP inform received event

Event	DHCP inform received
Event Type	dhcpInfmRcvd
Event Code	1238
Severity	Informational
Attribute	"mvnoid"=NA "wlanId"=NA,"zoneId"="NA" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="dhcp", "realm"="NA" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	DHCP Inform was received by {produce.short.name} [{SCGMgmtIp}] from UE [{ueMacAddr}]
Description	This event occurs when the controller receives the DHCP information.

## DHCP dcln received

**TABLE 648** DHCP dcln received event

Event	DHCP dcln received
Event Type	dhcpDclnRcvd
Event Code	1239
Severity	Major
Attribute	"mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut","realm"="NA" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	DHCP Decline was received by {produce.short.name} [{SCGMgmtIp}] from UE [{ueMacAddr}]
Description	This event occurs when the controller receives the DHCP declined message. The GTP (GPRS Tunneling Protocol) tunnel is deleted and recreated.

## GA Interface Events

### NOTE

This section is not applicable for vSZ-H.

Following are the events related to the GA interface (CDRs and GTP').

- [CGF keepalive not responded](#) on page 283
- [CDR transfer succeeded](#) on page 284

## Connection to CGF failed

**TABLE 649** Connection to CGF failed event

Event	Connection to CGF failed
Event Type	cnxnToCgfFailed
Event Code	1610
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA", "radSvrIp"="7.7.7.7" "cgfSvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Connection with CGF [{cgfSvrIp}] from RADServerIP [{radSvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when channel interface processor (CIP) or GPRS tunneling protocol prime (GTPP) stack detects a connection loss to the charging gateway function (CGF server).
Auto Clearance	This event triggers the alarm 1610, which is auto cleared by the event code 1613.

## CGF keepalive not responded

**TABLE 650** CGF keepalive not responded event

Event	CGF keepalive not responded
Event Type	cgfKeepAliveNotResponded

## Events Types

### GA Interface Events

**TABLE 650** CGF keepalive not responded event (continued)

Event	CGF keepalive not responded
Event Code	1612
Severity	Informational
Attribute	"mynoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA", "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Heartbeat missed between RAD Server [{radSrvrIp}] and CGF Server [{cgfSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when channel interface processor does not receive an acknowledgment for a keep alive request.

## CDR transfer succeeded

**TABLE 651** CDR transfer succeeded event

Event	CDR transfer succeeded
Event Type	cdrTxfrSuccessful
Event Code	1613
Severity	Debug
Attribute	"mynoid"="12" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="wlan. 3gppnetwork.org" "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	CDR Transfer successful from RAD Server [{radSrvrIp}] to CGF [{cgfSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the call details record is successfully transferred.

## CDR generation failed

**TABLE 652** CDR generation failed event

Event	CDR generation failed
Event Type	cdrGenerationFailed
Event Code	1615
Severity	Major
Attribute	"mynoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="wlan. 3gppnetwork.org" "radSrvrIp"="7.7.7.7" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Failed to generate CDR by RAD Server [{radSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the controller cannot format/generate the call detail records.

## CDR transfer failed

**TABLE 653** CDR transfer failed event

Event	CDR transfer failed
Event Type	cdrTxfrFailed
Event Code	1614

**TABLE 653** CDR transfer failed event (continued)

Event	CDR transfer failed
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radSrvrlp"="7.7.7" "cgfSrvrlp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2" "cause"="<reason for failure>"
Displayed on the web interface	CDR Transfer failed from RAD Server [{radSrvrlp}] to CGF [{cgfSrvrlp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the call detail record transfers fails.

## Gn/S2a Interface Events

### NOTE

This event is not applicable for vSZ-H.

Following are the events related to Gn/S2a interface.

Event	Event	Event
<a href="#">GGSN restarted</a> on page 285	<a href="#">GGSN not reachable</a> on page 286	<a href="#">Echo response not received</a> on page 286
<a href="#">GGSN not resolved</a> on page 286	<a href="#">PDP context established</a> on page 287	<a href="#">PDP create failed</a> on page 287
<a href="#">PDP update by HLR succeeded</a> on page 287	<a href="#">PDP update by HLR failed</a> on page 288	<a href="#">PDP update by roaming succeeded</a> on page 288
<a href="#">PDP update by roaming failed</a> on page 288	<a href="#">PDP update by GGSN succeeded</a> on page 289	<a href="#">PDP update by GGSN failed</a> on page 289
<a href="#">PDP delete by TTG succeeded</a> on page 289	<a href="#">PDP delete by TTG failed</a> on page 290	<a href="#">PDP delete by GGSN succeeded</a> on page 290
<a href="#">PDP delete by GGSN failed</a> on page 290	<a href="#">IP assigned</a> on page 291	<a href="#">IP not assigned</a> on page 291
<a href="#">Unknown UE</a> on page 292	<a href="#">PDP update success COA</a> on page 292	<a href="#">PDP update fail COA</a> on page 292
<a href="#">PDNGW could not be resolved</a> on page 293	<a href="#">PDNGW version not supported</a> on page 293	<a href="#">Associated PDNGW down</a> on page 293
<a href="#">Create session response failed</a> on page 294	<a href="#">Decode failed</a> on page 294	<a href="#">Modify bearer response failed</a> on page 295
<a href="#">Delete session response failed</a> on page 295	<a href="#">Delete bearer request failed</a> on page 295	<a href="#">Update bearer request failed</a> on page 296
<a href="#">CGF server not configured</a> on page 296		

## GGSN restarted

**TABLE 654** GGSN restarted event

Event	GGSN restarted
Event Type	ggsnRestarted
Event Code	1210
Severity	Major
Attribute	"mvnold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm" "realm"="NA" "gtpclp"="5.5.5.5", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{ggsnIp}] connected to {produce.short.name} [{SCGMgmtIp}] (GTPC-IP [{gtpclp}]) is restarted
Description	This event occurs when GPRS protocol control plane receives a new recovery value.

## GGSN not reachable

**TABLE 655** GGSN not reachable event

Event	GGSN not reachable
Event Type	ggsnNotReachable
Event Code	1211
Severity	Major
Attribute	"mvnold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm", "realm"="NA", "gtpclp"="5.5.5.5", "ggsnlp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{{ggsnlp}}] connected to {produce.short.name} (GTPC-IP [{{gtpclp}}]) is not reachable
Description	This event occurs when echo request is timed out.

## Echo response not received

**TABLE 656** Echo response not received event

Event	Echo response not received
Event Type	echoRspNotRcvd
Event Code	1212
Severity	Informational
Attribute	"mvnold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm", "realm"="NA", "gtpclp"="5.5.5.5", "ggsnlp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{{ggsnlp}}] did not respond to Echo Request from {produce.short.name} (GTPC-IP [{{gtpclp}}]) is not reachable
Description	This event occurs when GPRS protocol control plane does not receive an acknowledgment for the single echo request.

## GGSN not resolved

**TABLE 657** GGSN not resolved event

Event	GGSN not resolved
Event Type	ggsnNotResolved
Event Code	1215
Severity	Major
Attribute	"mvnold"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="wlan.3gppnetwork.org", "gtpclp"="5.5.5.5", "apn"="ruckuswireless.com", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	Failed to resolve GGSN from APN [{{apn}}] for UE with IMSI [{{ueImsi}}] and MSISDN [{{ueMsisdn}}]
Description	This event occurs when access point name is unable to resolve to gateway GPRS support node.

## PDP context established

**TABLE 658** PDP context established event

Event	PDP context established
Event Type	pdpCtxtEstablished
Event Code	1216
Severity	Debug
Attribute	"mvnoid"=12,"wlanId"=1,"zoneId"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplcp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	PDP context created for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol is established.

## PDP create failed

**TABLE 659** PDP create failed event

Event	PDP create failed
Event Type	crtPdpFailed
Event Code	1217
Severity	Debug
Attribute	"mvnoid"=12,"wlanId"=1,"zoneId"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplcp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	PDP context create failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Cause [{cause}]
Description	This event occurs when create packet data protocol fails.

## PDP update by HLR succeeded

**TABLE 660** PDP update by HLR succeeded event

Event	PDP update by HLR succeeded
Event Type	initPdpUpdSuccHlr
Event Code	1218
Severity	Debug
Attribute	"mvnoid"=12,"wlanId"=1,"zoneId"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplcp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "hlrEvent"="<event received from HLR>"
Displayed on the web interface	PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because of [hrlEvent] from HLR
Description	This event occurs when packet data protocol context is updated successfully. Update is initiated by tunneling termination gateway (TTG) control plane as a result of the home location register (HLR) initiation.

## PDP update by HLR failed

**TABLE 661** PDP update by HLR failed event

Event	PDP update by HLR failed
Event Type	initPdpUpdFailureHlr
Event Code	1219
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpclp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error" "hlrEvent"="<event received from HLR>"
Displayed on the web interface	PDP context update initiated because of HLR Event {{hlrEvent}} failed for UE with IMSI {{ueImsi}} and MSISDN {{ueMsisdn}} at {produce.short.name} {{SCGMgmtIp}}. Failure Cause {{cause}}
Description	This event occurs when update packet data protocol fails. Update is initiated by TTG control plane as a result of HLR initiation.

## PDP update by roaming succeeded

**TABLE 662** PDP update by roaming succeeded event

Event	PDP update by roaming succeeded
Event Type	initPdpUpdSuccRoam
Event Code	1220
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpclp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787"
Displayed on the web interface	PDP context updated for UE with IMSI {{ueImsi}} and MSISDN {{ueMsisdn}} at {produce.short.name} {{SCGMgmtIp}} because of UE Roaming
Description	This event occurs when packet data protocol context is updated successfully. Update is initiated by TTG control plane as a result of user equipment.

## PDP update by roaming failed

**TABLE 663** PDP update by roaming failed event

Event	PDP update by roaming failed
Event Type	initPdpUpdFailureRoam
Event Code	1221
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpclp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error"



**TABLE 663** PDP update by roaming failed event (continued)

Event	PDP update by roaming failed
Displayed on the web interface	PDP context update initiated because of UE Roaming failed for UE with IMSI [{{ueImsi}}] and MSISDN [{{ueMsisdn}}] at {produce.short.name} [{{SCGMgmtIp}}] Failure Cause [{{cause}}]
Description	This event occurs when the packet data protocol update fails. This is initiated by TTG control plane as a result of user equipment.

## PDP update by GGSN succeeded

**TABLE 664** PDP update by GGSN succeeded event

Event	PDP update by GGSN succeeded
Event Type	recvPdpUpdSuccGgsn
Event Code	1222
Severity	Debug
Attribute	"mvsidn"=12 "wlanid"=1,"zoneid"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	GGSN initiated; PDP context updated for UE with IMSI [{{ueImsi}}] and MSISDN [{{ueMsisdn}}] at {produce.short.name} [{{SCGMgmtIp}}]
Description	This event occurs when packet data protocol is updated successfully, which is initiated by the GGSN.

## PDP update by GGSN failed

**TABLE 665** PDP update by GGSN failed event

Event	PDP update by GGSN failed
Event Type	recvPdpUpdFailureGgsn
Event Code	1223
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_process" "realm"="NA" "gtplp"="5.5.5.5" "ggsnIp"="10.10.10.10" "ueMacAddr"="NA" "ueImsi"="NA" "apn"="NA" "SCGMgmtIp"="2.2.2.2" "cause"="cause of error"
Displayed on the web interface	GGSN initiated; PDP context update received from IP [{{ggsnIp}}] at {produce.short.name} [{{SCGMgmtIp}}] is failed. Cause [{{cause}}]
Description	This event occurs when the packet data protocol update fails.

## PDP delete by TTG succeeded

**TABLE 666** PDP delete by TTG succeeded event

Event	PDP delete by TTG succeeded
Event Type	initPdpDelSucc
Event Code	1224
Severity	Debug

**TABLE 666** PDP delete by TTG succeeded event (continued)

Event	PDP delete by TTG succeeded
Attribute	"mvsidn"=12 "wlanid"=1,"zoneid"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787"
Displayed on the web interface	{produce.short.name} initiated; PDP context deleted for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol delete is successful.

## PDP delete by TTG failed

**TABLE 667** PDP delete by TTG failed event

Event	PDP delete by TTG failed
Event Type	initPdpDelFailure
Event Code	1225
Severity	Debug
Attribute	"mvsidn"=12 "wlanid"=1,"zoneid"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	{produce.short.name} initiated; PDP context delete failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Cause [{cause}]
Description	This event occurs when packet data protocol delete fails.

## PDP delete by GGSN succeeded

**TABLE 668** PDP delete by GGSN succeeded event

Event	PDP delete by GGSN succeeded
Event Type	recvPdpDelSucc
Event Code	1226
Severity	Debug
Attribute	"mvsidn"=12 "wlanid"=1,"zoneid"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	GGSN initiated; PDP context deleted for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol delete is successful, as initiated by the GGSN.

## PDP delete by GGSN failed

**TABLE 669** PDP delete by GGSN failed event

Event	PDP delete by GGSN failed
Event Type	recvPdpDelFailure

**TABLE 669** PDP delete by GGSN failed event (continued)

Event	PDP delete by GGSN failed
Event Code	1227
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_process" "realm"="NA" "gtpclp"="5.5.5.5" "ggsnIp"="10.10.10.10" "ueMacAddr"="NA" "ueImsi"="NA" "apn"="NA" "SCGMgmtIp"="2.2.2.2" "cause"="cause of error"
Displayed on the web interface	GGSN initiated; PDP context delete received from IP [{ggsnIp}] at {produce.short.name} [{SCGMgmtIp}] is failed. Cause [{cause]}.
Description	This event occurs when delete packet data protocol fails. Delete is initiated by GGSN.

## IP assigned

**TABLE 670** IP assigned event

Event	IP assigned
Event Type	ipAssigned
Event Code	1229
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] was assigned IP [{ueIpAddr}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when IP address is assigned to the user equipment. This event is applicable for TTG/PDG sessions only.

## IP not assigned

**TABLE 671** IP not assigned event

Event	IP not assigned
Event Type	ipNotAssigned
Event Code	1230
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="<why IP could not be assigned>"
Displayed on the web interface	IP could not be assigned to UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because [{cause]}
Description	This event occurs when the IP address is not assigned to user equipment. This event is applicable for TTG/PDG sessions only.

## Unknown UE

**TABLE 672** Unknown UE event

Event	Unknown UE
Event Type	unknownUE
Event Code	1231
Severity	Minor
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "cause"="Subscriber Info Not Found" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Received request from un-known UE [{ueMacAddr}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when TTG control plane receives either a DHCP message or a trigger from data plane. It is unable to find the user equipment in the session context.

## PDP update success COA

**TABLE 673** PDP update success COA event

Event	PDP update success COA
Event Type	pdpUpdSuccCOA
Event Code	1244
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdN"="98787" "aaaSrvrIp"="5.5.5.5"
Displayed on the web interface	PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdN}] at {produce.short.name} [{SCGMgmtIp}] because of COA from AAA server [{aaaSrvrIp}]
Description	This event occurs when the packet data protocol update is successful when initiating the update process based on the change of authorization received from the external AAA server.

## PDP update fail COA

**TABLE 674** PDP update fail COA event

Event	PDP update fail COA
Event Type	pdpUpdFailCOA
Event Code	1245
Severity	Debug
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtplp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdN"="98787" "aaaSrvrIp"="5.5.5.5" "cause"="cause of error"
Displayed on the web interface	PDP context update initiated because of COA from AAA server [{gtplp}] failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdN}] at {produce.short.name} [{SCGMgmtIp}]. Failure Cause [{cause}].

**TABLE 674** PDP update fail COA event (continued)

Event	PDP update fail COA
Description	This event occurs when the packet data protocol update fails when initiating the update process based on the change of authorization received from the external AAA server.

## PDNGW could not be resolved

**TABLE 675** PDNGW could not be resolved event

Event	PDNGW could not be resolved
Event Type	pdnGwNotResolved
Event Code	1950
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345",  "ueMsisdn"="98787" "apn"="ruckus.com"
Displayed on the web interface	{{srcProcess}} APN {{apn}} could not be resolved on {produce.short.name} {{SCGMgmtIp}}, with username {{ueImsi}}@{realm}}
Description	This event occurs when the access point name is unable to resolve to PDN GW.

## PDNGW version not supported

**TABLE 676** PDNGW version not supported event

Event	PDNGW version not supported
Event Type	pdnGwVersionNotSupportedMsgReceived
Event Code	1952
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "APN"="ruckus.com", "pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Version not supported message received from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when the version is not supported for messages received from PDN GW.

## Associated PDNGW down

**TABLE 677** Associated PDNGW down event

Event	Associated PDNGW down
Event Type	pdnGwAssociationDown
Event Code	1953
Severity	Critical

## Events Types

### Gn/S2a Interface Events

**TABLE 677** Associated PDNGW down event (continued)

Event	Associated PDNGW down
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345",  "ueMsisdn"="98787" "APN"="ruckus.com","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Association with PDN GW with IP {{pgwIp}} from {produce.short.name} {{SCGMgmtIp}} down
Description	This event occurs when the association with PDN GW is down due to echo request time out or it fails to send messages to PDN GW.

## Create session response failed

**TABLE 678** Create session response failed event

Event	Create session response failed
Event Type	createSessionResponseFailed
Event Code	1954
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345",  "ueMsisdn"="98787" "APN"="ruckus.com" "cause"="xx","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Create Session response from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	This event occurs when create session response from PDN GW fails with a cause.

## Decode failed

**TABLE 679** Decode failed event

Event	Decode failed
Event Type	decodeFailed
Event Code	1955
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345",  "ueMsisdn"="98787" "APN"="ruckus.com","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Decode of message received from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed
Description	This event occurs when decoding of messages received from PDN GW fails.

## Modify bearer response failed

**TABLE 680** Modify bearer response failed event

Event	Modify bearer response failed
Event Type	modifyBearerResponseFailed
Event Code	1956
Severity	Major
Attribute	mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787", "APN"="ruckus.com" "cause"="xx","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Modify Bearer Response from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	This event occurs when modify bearer response from PDN GW fails with a cause.

## Delete session response failed

**TABLE 681** Delete session response failed event

Event	Delete session response failed
Event Type	deleteSessionResponseFailed
Event Code	1957
Severity	Major
Attribute	mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com" "cause"="xx","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Delete Session response from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	This event occurs when the delete session response from PDN GW fails.

## Delete bearer request failed

**TABLE 682** Delete bearer request failed event

Event	Delete bearer request failed
Event Type	deleteBearerRequestFailed
Event Code	1958
Severity	Major
Attribute	mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com","cause"="<reason for failure>","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Delete Bearer Request from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm} because {{cause}}
Description	This event occurs when the delete bearer request from PDN GW fails with decode error.

## Update bearer request failed

**TABLE 683** Update bearer request failed event

Event	Update bearer request failed
Event Type	updateBearerRequestFailed
Event Code	1959
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "uelmsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com", "cause"="reason for failure>","pgwIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Update bearer request from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{uelmsi}}@{realm} because {{cause}}
Description	This event occurs when the update bearer request fails with a decode error.

## CGF server not configured

**TABLE 684** CGF server not configured event

Event	CGF server not configured
Event Type	cgfServerNotConfigured
Event Code	1960
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="CIP" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "uelmsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com" "cgfSrvrIp" = "1.1.1.1", "ggsnIp"="10.10.10.10"
Displayed on the web interface	CGF server IP {{cgfSrvrIp}} received from PDN GW/GGSN with IP {{ggsnIp}} on {produce.short.name} {{SCGMgmtIp}} is not configured
Description	This event occurs when the IP address of the charging gateway function server received from GGSN/PDNGW is not configured in the controller web interface.

## Gr Interface Event

### NOTE

This section is not applicable for vSZ-H.

Following are the events related to GR interface.

- [Destination not reachable](#) on page 297
- [Destination available](#) on page 297
- [App server down](#) on page 298
- [App server inactive](#) on page 298
- [App server active](#) on page 298
- [Association establishment failed](#) on page 299
- [Association down](#) on page 299



- [Association up](#) on page 299
- [Send auth info success](#) on page 300
- [Auth info sending failed](#) on page 300
- [GPRS location update succeeded](#) on page 300
- [GPRS location update failed](#) on page 300
- [Insert sub data success](#) on page 301
- [Insert sub data failed](#) on page 301
- [Outbound routing failure](#) on page 301
- [Did allocation failure](#) on page 302
- [Restore data success](#) on page 302
- [Restore data failed](#) on page 302

## Destination not reachable

**TABLE 685** Destination not reachable event

Event	Destination not reachable
Event Type	destNotRecheable
Event Code	1618
Severity	Critical
Attribute	"mvsold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "pointCode"="1.1.1"
Displayed on the web interface	Remote Point Code {{pointCode}} is unavailable
Description	This event occurs when the point code is unreachable due to a pause indicator
Auto Clearance	This event triggers the alarm 1618, which is auto cleared by the event code 1620.

## Destination available

**TABLE 686** Destination available event

Event	Destination available
Event Type	destAvailable
Event Code	1620
Severity	Critical
Attribute	"mvsold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "pointCode"="1.1.1"
Displayed on the web interface	Remote Point Code {{pointCode}} is available
Description	This event occurs when the point code is available due to the resume indicator.

## App server down

**TABLE 687** App server down event

Event	App server down
Event Type	appServerDown
Event Code	1623
Severity	Critical
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "routingContext"="1" "pointCode"="1.1.1" "SSN" = "7"
Displayed on the web interface	Application Server Down, Routing Context {{routingContext}}, local Point Code {{pointCode}}, local SSN {{SSN}}
Description	This event occurs when the local application server is down from the remote IP security protocol (IPSP) or controller.
Auto Clearance	This event triggers the alarm 1623, which is auto cleared by the event code 1625.

## App server inactive

**TABLE 688** App server inactive event

Event	App server inactive
Event Type	appServerInactive
Event Code	1624
Severity	Critical
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "routingContext"="1" "pointCode"="1.1.1" "SSN" = "7"
Displayed on the web interface	Application Server Inactive, Routing Context {{routingContext}}, lpcal Point Code {{pointCode}}, local SSN {{SSN}}
Description	This event occurs when the local application server is inactive from the remote IPSP/ controller.
Auto Clearance	This event triggers the alarm 1624, which is auto cleared by the event code 1625.

## App server active

**TABLE 689** App server active event

Event	App server active
Event Type	appServerActive
Event Code	1625
Severity	Critical
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "routingContext"="1" "pointCode"="1.1.1" "SSN" = "7"
Displayed on the web interface	Application Server Active, Routing Context {{routingContext}}, lpcal Point Code {{pointCode}}, local SSN {{SSN}}
Description	This event occurs when the local application server is active from the remote IPSP or signalling gateway (SG).

## Association establishment failed

**TABLE 690** Association establishment failed event

Event	Association establishment failed
Event Type	assocEstbFailed
Event Code	1626
Severity	Critical
Attribute	"mvnold"="3" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "srcIP"="10.1.4.10" "srcPort"="2960" "destIP"="10.1.4.20" "destPort"="2960"
Displayed on the web interface	Failed to establish SCTP association. SCTP Abort received from srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This event occurs when it is unable to establish an association to the controller/IPSP.
Auto Clearance	This event triggers the alarm 1626, which is auto cleared by the event code 1628.

## Association down

**TABLE 691** Association down event

Event	Association down
Event Type	assocDown
Event Code	1627
Severity	Critical
Attribute	"mvnold"="3" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "srcIP"="10.1.4.10" "srcPort"="2960" "destIP"="10.1.4.20" "destPort"="2960"
Displayed on the web interface	SCTP association DOWN srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This event occurs when the stream control transmission protocol (SCTP) association is down.
Auto Clearance	This event triggers the alarm 1627, which is auto cleared by the event code 1628.

## Association up

**TABLE 692** Association up event

Event	Association up
Event Type	assocUp
Event Code	1628
Severity	Critical
Attribute	"mvnold"="3" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "srcIP"="10.1.4.10" "srcPort"="2960" "destIP"="10.1.4.20" "destPort"="2960"
Displayed on the web interface	SCTP association UP. srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This event occurs when the SCTP association is UP.

## Send auth info success

**TABLE 693** Send auth info success event

Event	Send auth info success
Event Type	sendAuthInfoSuccess
Event Code	1630
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918"
Displayed on the web interface	MAP-SendAuthInfo Operation successful from IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when authentication parameters are successfully retrieved.

## Auth info sending failed

**TABLE 694** Auth info sending failed event

Event	Auth info sending failed
Event Type	sendAuthInfoFailed
Event Code	1631
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-SendAuthInfo Operation Failed for IMSI [{ueImsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to retrieve the authentication parameters.

## GPRS location update succeeded

**TABLE 695** GPRS location update succeeded event

Event	GPRS location update succeeded
Event Type	updateGprsLocSuccess
Event Code	1632
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918"
Displayed on the web interface	MAP-UpdateGprsLocation Operation Successful for IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when it successfully updates the GPRS location operation.

## GPRS location update failed

**TABLE 696** GPRS location update failed event

Event	GPRS location update failed
Event Type	updateGprsLocFailed

**TABLE 696** GPRS location update failed event (continued)

Event	GPRS location update failed
Event Code	1633
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "uelmsi"="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-UpdateGprsLocation Operation Failed for IMSI [{uelmsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when the GPRS location update process fails.

## Insert sub data success

**TABLE 697** Insert sub data success event

Event	Insert sub data success
Event Type	insertSubDataSuccess
Event Code	1634
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "uelmsi"="04844624203918"
Displayed on the web interface	MAP-InsertSubscriberData Operation Successful for IMSI [{uelmsi}] with [{hlrInstance}]
Description	This event occurs when it successfully inserts the subscriber data operation.

## Insert sub data failed

**TABLE 698** Insert sub data failed event

Event	Insert sub data failed
Event Type	insertSubDataFailed
Event Code	1635
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "uelmsi"="04844624203918" "cause"="ASN decode error"
Displayed on the web interface	MAP-InsertSubscriberData Operation Failed for IMSI [{uelmsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to insert the subscriber data operation

## Outbound routing failure

**TABLE 699** Outbound routing failure event

Event	Outbound routing failure
Event Type	outboundRoutingFailure
Event Code	1636
Severity	Major

## Events Types

### Gr Interface Event

**TABLE 699** Outbound routing failure event (continued)

Event	Outbound routing failure
Attribute	"mvsold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "operation"="updateGprsLocationReq" "hlrInstance"="Vodafone_HLR" "uelmsi"="04844624203918"
Displayed on the web interface	Unable to route [{operation}] for IMSI [{uelmsi}] to HLR [{hlrInstance}]
Description	This event occurs when it is unable to route transaction capabilities application (TCAP) message to the destination.

## Did allocation failure

**TABLE 700** Did allocation failure event

Event	Did allocation failure
Event Type	didAllocationFailure
Event Code	1637
Severity	Critical
Attribute	"mvsold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip"
Displayed on the web interface	HIP unable to allocate new dialogue
Description	This event occurs when it is unable to allocate the dialogue identifier for a new transaction. This indicates an overload condition.

## Restore data success

**TABLE 701** Restore data success event

Event	Restore data success
Event Type	restoreDataSuccess
Event Code	1639
Severity	Debug
Attribute	"mvsold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "uelmsi"="04844624203918"
Displayed on the web interface	MAP-RestoreData Operation Successful for IMSI [{uelmsi}] with [{hlrInstance}]
Description	This event occurs when it successfully restores the data operation.

## Restore data failed

**TABLE 702** Restore data failed event

Event	Restore data failed
Event Type	restoreDataFailed
Event Code	1640
Severity	Major
Attribute	"mvsold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "uelmsi"="04844624203918" "cause"="Timeout"

**TABLE 702** Restore data failed event (continued)

Event	Restore data failed
Displayed on the web interface	MAP-RestoreData Operation Failed for IMSI [{uemsI}] with [{hIrlnstance}], cause [{cause}]
Description	This event occurs when it fails to restore the data operation.

## IPMI Events

### NOTE

This section is not applicable for vSZ-H.

Following are the events related to IPMIs:

Event	Event	Event
<a href="#">ipmiVoltage</a> on page 303	<a href="#">ipmiThempBB</a> on page 304	<a href="#">ipmiThempFP</a> on page 304
<a href="#">ipmiThempIOH</a> on page 304	<a href="#">ipmiThempMemP</a> on page 305	<a href="#">ipmiThempPS</a> on page 305
<a href="#">ipmiThempP</a> on page 305	<a href="#">ipmiThempHSBP</a> on page 306	<a href="#">ipmiFan</a> on page 306
<a href="#">ipmiPower</a> on page 306	<a href="#">ipmiCurrent</a> on page 307	<a href="#">ipmiFanStatus</a> on page 307
<a href="#">ipmiPsStatus</a> on page 307	<a href="#">ipmiDrvStatus</a> on page 308	<a href="#">ipmiREVote</a> on page 308
<a href="#">ipmiREThempBB</a> on page 308	<a href="#">ipmiREThempFP</a> on page 308	<a href="#">ipmiREThempIOH</a> on page 309
<a href="#">ipmiREThempMemP</a> on page 309	<a href="#">ipmiREThempPS</a> on page 309	<a href="#">ipmiREThempP</a> on page 310
<a href="#">ipmiREThempHSBP</a> on page 310	<a href="#">ipmiREFan</a> on page 310	<a href="#">ipmiREPower</a> on page 311
<a href="#">ipmiRECurrent</a> on page 311	<a href="#">ipmiREFanStatus</a> on page 311	<a href="#">ipmiREPsStatus</a> on page 311
<a href="#">ipmiREDrvStatus</a> on page 312		

## ipmiVoltage

**TABLE 703** ipmiVoltage event

Event	ipmiVoltage
Event Type	ipmiVoltage
Event Code	901
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard voltage [{status}] on control plane [{nodeMac}]
Description	This event occurs due to under /over voltage on the control plane. Baseboard threshold temperatures are:  Critical high - 66 <sup>0</sup> C  Non critical high - 61 <sup>0</sup> C  Non critical low - 10 <sup>0</sup> C  Critical low - 5 <sup>0</sup> C
Auto Clearance	This event triggers the alarm 901, which is auto cleared by the event code 926.

## ipmiThempBB

**TABLE 704** ipmiThempBB event

Event	ipmiThempBB
Event Type	ipmiThempBB
Event Code	902
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on controlplane [{nodeMac}]
Description	This event occurs when the baseboard temperature status is sent. Baseboard threshold temperatures are in the range of 10 <sup>0</sup> Celsius to 61 <sup>0</sup> Celsius. The default threshold is 61 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 902, which is auto cleared by the event code 927.

## ipmiThempFP

**TABLE 705** ipmiThempFP event

Event	ipmiThempFP
Event Type	ipmiThempFP
Event Code	903
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the front panel temperature status is sent. Front panel threshold temperatures are in the range of 5 <sup>0</sup> Celsius to 44 <sup>0</sup> Celsius. The default threshold is 44 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 903, which is auto cleared by the event code 928.

## ipmiThempIOH

**TABLE 706** ipmiThempIOH event

Event	ipmiThempIOH
Event Type	ipmiThempIOH
Event Code	904
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Chipset temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the chip set temperature status is sent. IOH thermal margin threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 904, which is auto cleared by the event code 929.



## ipmiThempMemP

**TABLE 707** ipmiThempMemP event

Event	ipmiThempMemP
Event Type	ipmiThempMemP
Event Code	905
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] memory temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the processor memory temperature status is sent. Process 1 memory thermal margin threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 905, which is auto cleared by the event code 930.

## ipmiThempPS

**TABLE 708** ipmiThempPS event

Event	ipmiThempPS
Event Type	ipmiThempPS
Event Code	906
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the power supply temperature status is sent. Power supply 1 and power supply 2 threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 906, which is auto cleared by the event code 931.

## ipmiThempP

**TABLE 709** ipmiThempP event

Event	ipmiThempP
Event Type	ipmiThempP
Event Code	907
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This event is triggered when the threshold value is in the range of 1 <sup>0</sup> to 11 <sup>0</sup> Celsius. The default threshold is 11 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 907, which is auto cleared by the event code 932.

## ipmiThempHSBP

**TABLE 710** ipmiThempHSBP event

Event	ipmiThempHSBP
Event Type	ipmiThempHSBP
Event Code	908
Severity	Majorf
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Hot swap backplane temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the hot swap back plane temperature status in the range of 9 <sup>0</sup> Celsius to 55 <sup>0</sup> Celsius. The default threshold is 55 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 908, which is auto cleared by the event code 933.

## ipmiFan

**TABLE 711** ipmiFan event

Event	ipmiFan
Event Type	ipmiFan
Event Code	909
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}]
Description	This event occurs when the system fan module status is sent.
Auto Clearance	This event triggers the alarm 909, which is auto cleared by the event code 934.

## ipmiPower

**TABLE 712** ipmiPower event

Event	ipmiPower
Event Type	ipmiPower
Event Code	910
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}]
Description	This event occurs when the AC power input status is sent.
Auto Clearance	This event triggers the alarm 910, which is auto cleared by the event code 935.

## ipmiCurrent

**TABLE 713** ipmiCurrent event

Event	ipmiCurrent
Event Type	ipmiCurrent
Event Code	911
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] +12V% of maximum current output [{status}] on control plane [{nodeMac}]
Description	This event occurs when the power supply and the maximum voltage output status is sent.
Auto Clearance	This event triggers the alarm 911, which is auto cleared by the event code 936.

## ipmiFanStatus

**TABLE 714** ipmiFanStatus event

Event	ipmiFanStatus
Event Type	ipmiFanStatus
Event Code	912
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the fan module status is sent.
Auto Clearance	This event triggers the alarm 912, which is auto cleared by the event code 937.

## ipmiPsStatus

**TABLE 715** ipmiPsStatus event

Event	ipmiPsStatus
Event Type	ipmiPsStatus
Event Code	913
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the power supply status is sent.
Auto Clearance	This event triggers the alarm 913, which is auto cleared by the event code 938.

## ipmiDrvStatus

**TABLE 716** ipmiDrvStatus event

Event	ipmiDrvStatus
Event Type	ipmiDrvStatus
Event Code	914
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Disk drive [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the disk drive status is sent.
Auto Clearance	This event triggers the alarm 914, which is auto cleared by the event code 939.

## ipmiREVotage

**TABLE 717** ipmiREVotage event

Event	ipmiREVotage
Event Type	ipmiREVotage
Event Code	926
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard voltage [{status}] on control plane [{nodeMac}].
Description	This event occurs when the baseboard voltage comes back to the normal status.

## ipmiREThempBB

**TABLE 718** ipmiREThempBB event

Event	ipmiREThempBB
Event Type	ipmiREThempBB
Event Code	927
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the baseboard temperature comes back to the normal status.

## ipmiREThempFP

**TABLE 719** ipmiREThempFP event

Event	ipmiREThempFP
Event Type	ipmiREThempFP
Event Code	928

**TABLE 719** ipmiREThempFP event (continued)

Event	ipmiREThempFP
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the front panel temperature comes back to the normal status.

## ipmiREThempIOH

**TABLE 720** ipmiREThempIOH event

Event	ipmiREThempIOH
Event Type	ipmiREThempIOH
Event Code	929
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Chipset temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the chipset temperature comes back to the normal status.

## ipmiREThempMemP

**TABLE 721** ipmiREThempMemP event

Event	ipmiREThempMemP
Event Type	ipmiREThempMemP
Event Code	930
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] memory temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the processor memory temperature comes back to the normal status.

## ipmiREThempPS

**TABLE 722** ipmiREThempPS event

Event	ipmiREThempPS
Event Type	ipmiREThempPS
Event Code	931
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] temperature [{status}] on control plane [{nodeMac}]

**TABLE 722** ipmiREThempPS event (continued)

Event	ipmiREThempPS
Description	This event occurs when the power supply temperature comes back to the normal status.

## ipmiREThempP

**TABLE 723** ipmiREThempP event

Event	ipmiREThempP
Event Type	ipmiREThempP
Event Code	932
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the processor temperature comes back to the normal status.

## ipmiREThempHSBP

**TABLE 724** ipmiREThempHSBP event

Event	ipmiREThempHSBP
Event Type	ipmiREThempHSBP
Event Code	933
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Hot swap backplane temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the hot swap backplane temperature comes back to the normal status.

## ipmiREFan

**TABLE 725** ipmiREFan event

Event	ipmiREFan
Event Type	ipmiREFan
Event Code	934
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}].
Description	This event occurs when the system fan module comes back to the normal status.

## ipmiREPower

**TABLE 726** ipmiREPower event

Event	ipmiREPower
Event Type	ipmiREPower
Event Code	935
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}].
Description	This event occurs when the AC power supply comes back to the normal status.

## ipmiRECurrent

**TABLE 727** ipmiRECurrent event

Event	ipmiRECurrent
Event Type	ipmiRECurrent
Event Code	936
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}].
Description	This event occurs when the AC power supply comes back to the normal status.

## ipmiREFanStatus

**TABLE 728** ipmiREFanStatus event

Event	ipmiREFanStatus
Event Type	ipmiREFanStatus
Event Code	937
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}].
Description	This event occurs when the fan module comes back to the normal status.

## ipmiREPsStatus

**TABLE 729** ipmiREPsStatus event

Event	ipmiREPsStatus
Event Type	ipmiREPsStatus
Event Code	938
Severity	Informational

## Events Types

### Licensing Interface Events

**TABLE 729** ipmiREPsStatus event (continued)

Event	ipmiREPsStatus
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on control plane [{nodeMac}].
Description	This event occurs when the power supply comes back to the normal status.

## ipmiREDrvStatus

**TABLE 730** ipmiREDrvStatus event

Event	ipmiREDrvStatus
Event Type	ipmiREDrvStatus
Event Code	939
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Disk drive [{id}] [{status}] on control plane [{nodeMac}].
Description	This event occurs when the disk drive status comes back to the normal status.

## Licensing Interface Events

Following are the events related to licensing:

- [TTG session warning threshold](#) on page 313
- [TTG session major threshold](#) on page 313
- [TTG session critical threshold](#) on page 313
- [TTG session license exhausted](#) on page 314
- [License sync succeeded](#) on page 314
- [License sync failed](#) on page 314
- [License import succeeded](#) on page 315
- [License import failed](#) on page 315
- [License data changed](#) on page 315
- [License going to expire](#) on page 315
- [Insufficient license capacity](#) on page 316
- [Data plane DHCP IP license insufficient](#) on page 316
- [Data plane NAT session license insufficient](#) on page 316
- [AP number limit exceeded](#) on page 317
- [Insufficient license capacity](#) on page 317
- [Insufficient license capacity](#) on page 317



## TTG session warning threshold

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 731** TTG session warning threshold event

Event	TTG session warning threshold
Event Type	ttgSessionWarningThreshold
Event Code	1240
Severity	Warning
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached warning level.
Description	This event occurs when the number of user equipment attached to the system has reached the critical threshold limit.

## TTG session major threshold

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 732** TTG session major threshold event

Event	TTG session major threshold
Event Type	ttgSessionMajorThreshold
Event Code	1241
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached major level.
Description	This event occurs when the number of user equipment attached to the system has reached the major threshold limit.

## TTG session critical threshold

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 733** TTG session critical threshold event

Event	TTG session critical threshold
Event Type	ttgSessionCriticalThreshold
Event Code	1242
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached critical level.
Description	This event occurs when the number of user equipment attached to the system has reached the critical threshold limit.

## TTG session license exhausted

### NOTE

This event is not applicable for vSZ-H.

**TABLE 734** TTG session license exhausted event

Event	TTG session license exhausted
Event Type	ttgSessionLicenseExhausted
Event Code	1243
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed of {produce.short.name} [{SCGMgmtIp}] have been exhausted for all sessions.
Description	This event occurs when the number of user equipment attached to the system has exceeded the license limit.

## License sync succeeded

**TABLE 735** License sync succeeded event

Event	License sync succeeded
Event Type	licenseSyncSuccess
Event Code	1250
Severity	Informational
Attribute	"nodeName"="xxxxxxx", "licenseServerName"="ruckuswireless.flexeraoperation.com"
Displayed on the web interface	Node [{nodeName}] sync-up license with license server [{licenseServerName}] succeeded.
Description	This event occurs when the controller successfully synchronizes the license data with the license server.

## License sync failed

**TABLE 736** License sync failed event

Event	License sync failed
Event Type	licenseSyncFail
Event Code	1251
Severity	Warning
Attribute	"nodeName"="xxxxxxx", "licenseServerName"="ruckuswireless.flexeraoperation.com"
Displayed on the web interface	Node [{nodeName}] sync-up license with license server [{licenseServerName}] failed.
Description	This event occurs when the controller fails to synchronize the license data with the license server.

## License import succeeded

**TABLE 737** License import succeeded event

Event	License import succeeded
Event Type	licenseImportSuccess
Event Code	1252
Severity	Informational
Attribute	"nodeName"="xxxxxxx",
Displayed on the web interface	Node [{nodeName}] import license data succeeded.
Description	This event occurs when the controller successfully imports the license data

## License import failed

**TABLE 738** License import failed event

Event	License import failed
Event Type	licenseImportFail
Event Code	1253
Severity	Warning
Attribute	"nodeName"="xxxxxxx",
Displayed on the web interface	Node [{nodeName}] import license data failed.
Description	This event occurs when the controller fails to imports the license data

## License data changed

**TABLE 739** License data changed event

Event	License data changed
Event Type	licenseChanged
Event Code	1254
Severity	Informational
Attribute	"nodeName"="xxxxxxx",
Displayed on the web interface	Node [{nodeName}] license data has been changed.
Description	This event occurs when the controller license data is modified.

## License going to expire

**TABLE 740** License going to expire event

Event	License going to expire
Event Type	licenseGoingToExpire
Event Code	1255
Severity	Major

## Events Types

### Licensing Interface Events

**TABLE 740** License going to expire event (continued)

Event	License going to expire
Attribute	"nodeName"="xxx", "licenseType"=" xxx"
Displayed on the web interface	The [{licenseType}] on node [{nodeName}] will expire on [{associationTime}].
Description	This event occurs when the validity of the license is going to expire.

## Insufficient license capacity

**TABLE 741** Insufficient license capacity event

Event	Insufficient license capacity
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1256
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing AP connections to terminate.
Description	This event occurs when connected APs are rejected due to insufficient licenses.

## Data plane DHCP IP license insufficient

### NOTE

This event is not applicable for SZ300/SZ100.

**TABLE 742** Data plane DHCP IP license insufficient event

Event	Data plane DHCP IP license insufficient
Event Type	dpDhcpIpLicenseNotEnough
Event Code	1277
Severity	Major
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This event occurs when Data Plane DHCP IP license insufficient. ( total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}] )
Description	This event occurs when the data plane DHCP IP address license is insufficient.

## Data plane NAT session license insufficient

### NOTE

This event is not applicable for SZ300/SZ100.

**TABLE 743** Data plane NAT session license insufficient event

Event	Data plane NAT session license insufficient
Event Type	dpNatSessionLicenseNotEnough

**TABLE 743** Data plane NAT session license insufficient event (continued)

Event	Data plane NAT session license insufficient
Event Code	1278
Severity	Major
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This event occurs when Data Plane NAT session license insufficient. ( total {{totalLicenseCnt}}, consumed {{consumedLicenseCnt}}, available {{availableLicenseCnt}} )
Description	This event occurs when the data plane NAT session license is insufficient.

## AP number limit exceeded

**TABLE 744** AP number limit exceeded event

Event	AP number limit exceeded
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1280
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient {{licenseType}} license is detected and it will cause existing AP connections to terminate.
Description	This event occurs when an approved AP is rejected due to number of APs having exceeded the limit.

## Insufficient license capacity

**TABLE 745** Insufficient license capacity event

Event	Insufficient license capacity
Event Type	urlFilteringLicenseInsufficient
Event Code	1281
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient {{licenseType}} licenses have been detected, which will cause the URL Filtering feature to be disabled.
Description	This event occurs when the number of the APs exceeds the number of URL filtering licenses purchased.

## Insufficient license capacity

**TABLE 746** Insufficient license capacity event

Event	Insufficient license capacity
Event Type	switchConnectionTerminatedDueToInsufficientLicense
Event Code	1289

**TABLE 746** Insufficient license capacity event (continued)

Event	Insufficient license capacity
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{{licenseType}}] license is detected and it will cause existing switch connections to terminate.
Description	This event occurs when some connected switches were rejected due to insufficient license capacity.

## Location Delivery Events

### NOTE

This section is not applicable for vSZ-H.

Following are the events related to location delivery.

- [Unavailable location info requested](#) on page 318
- [Incapable location info requested](#) on page 318
- [Unsupported location delivery request](#) on page 319

## Unavailable location info requested

**TABLE 747** Unavailable location info requested event

Event	Unavailable location info requested
Event Type	unavailableLocInfoRequested
Event Code	1655
Severity	Debug
Attribute	"mvnold"=12, "wlanId"=1, "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd", "realm"="operator realm", "radSrvrIp"="1.1.1.1", "requestedInfo"="target location   geo location, etc", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	AAA [{{radSrvrIp}}] requests [{{requestedInfo}}] that is not available with {produce.short.name}{{SCGMgmtIp}}
Description	This event occurs when the AAA server requests for the location information, which is not available at the controller. For example, the AAA server requests for the target location even after the controller communicating that it can only support NAS locations.

## Incapable location info requested

**TABLE 748** Incapable location info requested event

Event	Incapable location info requested
Event Type	incapableLocInfoRequested
Event Code	1656
Severity	Debug

**TABLE 748** Incapable location info requested event (continued)

Event	Incapable location info requested
Attribute	<pre>"mvsold"=12, "wlanId"=1, "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius"  "realm"="operator realm", "radSrvrIp"="1.1.1.1", "requestedInfo"="target location   geo location, etc", "SCGMgmtIp"="2.2.2.2"</pre>
Displayed on the web interface	AAA [{radSrvrIp}] requests [{requestedInfo}] that is not advertised by {produce.short.name}{{SCGMgmtIp}}
Description	This event occurs when the AAA server requests for location information though the controller does not advertise that it is capable of delivering the location information.

## Unsupported location delivery request

**TABLE 749** Unsupported location delivery request event

Event	Unsupported location delivery request
Event Type	unSupportedLocDeliveryRequest
Event Code	1657
Severity	Debug
Attribute	<pre>"mvsold"=12, "wlanId"=1, "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radius"  "realm"="operator realm", "radSrvrIp"="1.1.1.1"  "requestedMethod"="out of band   initial request, etc" "SCGMgmtIp"="2.2.2.2"</pre>
Displayed on the web interface	AAA [{radSrvrIp}] requests [{requestedInfo}] that is not supported by {produce.short.name}{{SCGMgmtIp}}.
Description	This event occurs when the AAA server requests for a delivery method that is not supported by the controller.

## PMIPv6 Events

### NOTE

This section is not applicable for vSZ-H.

Following are the events related to PMIPv6.

- [Config update failed](#) on page 319
- [LMA ICMP reachable](#) on page 320
- [LMA server unreachable](#) on page 320
- [DHCP connected](#) on page 320
- [DHCP connection lost](#) on page 321

## Config update failed

**TABLE 750** Config update failed event

Event	Config update failed
Event Type	updateCfgFailed

**TABLE 750** Config update failed event (continued)

Event	Config update failed
Event Code	5004
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2","cause"="reason"
Displayed on the web interface	Failed to apply configuration [{cause}] in PMIPv6 process at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 receives an error or negative acknowledgment or improper/incomplete information from D-bus client.

## LMA ICMP reachable

**TABLE 751** LMA ICMP reachable event

Event	LMA ICMP reachable
Event Type	lmaIcmpReachable
Event Code	5005
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2","lmaIp"="1.1.1.1"
Displayed on the web interface	[[lmaIp]] ICMP reachable on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 daemon connects to the local mobility anchor (LMA) server through the internet control message protocol (ICMP) packet.

## LMA server unreachable

**TABLE 752** LMA server unreachable event

Event	LMA server unreachable
Event Type	lmaHbUnreachable
Event Code	5007
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2","lmaIp"="1.1.1.1"
Displayed on the web interface	[[lmaIp]] fail have been detected on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 daemon detects either restart or failure of the LMA server.

## DHCP connected

**TABLE 753** DHCP connected event

Event	DHCP connected
Event Type	connectedToDHCP
Event Code	5101
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2"



**TABLE 753** DHCP connected event (continued)

Event	DHCP connected
Displayed on the web interface	PMIPv6 process connect to DHCP server successfully on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 completes the configuration procedure successfully.

## DHCP connection lost

**TABLE 754** DHCP connection lost event

Event	DHCP connection lost
Event Type	lostCnxnToDHCP
Event Code	5102
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process cannot connect to DHCP server on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the connection between PMIPv6 process and DHCP server is lost.
Auto Clearance	This event triggers the alarm 5102, which is auto cleared by the event code 5101.

## Session Events

Following are the events related to session interface (UE TTG sessions)

- [Session timeout](#) on page 321
- [Delete all sessions](#) on page 322
- [Binding succeeded](#) on page 322
- [Binding failed](#) on page 323
- [Binding time expired](#) on page 323
- [Binding revoked](#) on page 323
- [Binding released](#) on page 324

## Session timeout

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 755** Session timeout event

Event	Session timeout
Event Type	sessTimeout
Event Code	1235
Severity	Debug

**TABLE 755** Session timeout event (continued)

Event	Session timeout
Attribute	"mvnoid"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "cause"="Session Timeout" "SCGMgmtIp"="2.2.2.2" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	Session for UE with IMSI [{{ueImsi}}] and MSISDN [{{ueMsisdn}}] got deleted due to Session Timeout on {produce.short.name} [{{SCGMgmtIp}}]
Description	This event occurs when a session is deleted due to a timeout specified by the AAA server.

## Delete all sessions

**TABLE 756** Delete all sessions event

Event	Delete all sessions
Event Type	delAllSess
Event Code	1237
Severity	Minor
Attribute	"mvnoid"="NA" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "cause"="Admin Delete" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	All sessions got terminated on {produce.short.name} [{{SCGMgmtIp}}] due to [{{cause}}]
Description	This event occurs when all sessions are deleted based on the indicators received from the controller web interface or CLI.

## Binding succeeded

### NOTE

This event is not applicable for vSZ-H.

**TABLE 757** Binding succeeded event

Event	Binding succeeded
Event Type	bindingSuccess
Event Code	5009
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmaIp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueIpAddr"="5.5.5.5" "dataBladeIp"="3.3.3.3"
Displayed on the web interface	[{{ueMacAddr}}] UE binding update successful on {produce.short.name}-D [{{dataBladeIp}}], and get IP address: [{{ueIpAddr}}] from LMA: [{{lmaIp}}]
Description	This event occurs when the mobile node binding update is successful.

## Binding failed

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 758** Binding failed event

Event	Binding failed
Event Type	bindingFailure
Event Code	5010
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmalp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5" "cause"="failure cause"
Displayed on the web interface	Binding for [{ueMacAddr}] UE binding update failure on {produce.short.name}-D [{dataBladeIp}]. Failure Cause [{cause}]
Description	This event occurs when mobile node binding update fails.
Auto Clearance	This event triggers the alarm 5010, which is auto cleared by the event code 5009.

## Binding time expired

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 759** Binding time expired event

Event	Binding time expired
Event Type	bindingExpired
Event Code	5011
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2" "lmalp"="1.1.1.1", "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	[{ueMacAddr}] UE Binding expired on {produce.short.name}-D [{dataBladeIp}]
Description	This event occurs when the binding expires.

## Binding revoked

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 760** Binding revoked event

Event	Binding revoked
Event Type	bindingRevoked
Event Code	5012
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmalp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5"

**TABLE 760** Binding revoked event (continued)

Event	Binding revoked
Displayed on the web interface	{{ueMacAddr}} UE Binding have been revoked on {produce.short.name}-D {{dataBladelp}}
Description	This event occurs when the binding is revoked on the controller.

## Binding released

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 761** Binding released event

Event	Binding released
Event Type	bindingReleased
Event Code	5013
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmaIp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladelp"="3.3.3.3" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	{{ueMacAddr}} UE Binding have been released on {produce.short.name}-D {{dataBladelp}}
Description	This event occurs when some mobile node binding are released.

## STA Interface Events

**NOTE**

This section is not applicable for vSZ-H.

Following are the events related to STA interface.

- [STA successful authentication](#) on page 324
- [STA session termination {produce.short.name} initiated success](#) on page 325
- [STA session termination AAA initiated success](#) on page 325
- [STA session termination AAA initiated failed](#) on page 325
- [STA re-authorization successful](#) on page 326

## STA successful authentication

**TABLE 762** STA successful authentication event

Event	STA successful authentication
Event Type	staSuccessfulAuthentication
Event Code	1550
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12, "srcProcess"="STA", "ueImsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaServIp"="1.1.1.1"

**TABLE 762** STA successful authentication event (continued)

Event	STA successful authentication
Displayed on the web interface	{{srcProcess}} Auth of {{uelmsi}}/{{ueUsername}} on {produce.short.name} [SCGMgmtIp] with AAA server [aaaSrvrIp] Successful
Description	This event occurs when the authentication procedure with external 3GPP AAA server is successful. The diameter EAP request (DER) is received from the 3GPP AAA server with result code as successful.

## STA session termination {produce.short.name} initiated success

**TABLE 763** STA session termination {produce.short.name} initiated success event

Event	STA session termination {produce.short.name} initiated success
Event Type	staSessionTermSCGInitSuccess
Event Code	1554
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12,"srcProcess"="STA", "realm"= "wlan.mnc080.mcc405.3gppnetwork.org", "uelmsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvrIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} session termination of {{uelmsi}}/{{ueUsername}} on {produce.short.name} [SCGMgmtIp] with 3GPP AAA [aaaSrvrIp] successful
Description	This event occurs when the controller initiated session termination-r (STR) is received and successfully terminated by the STA interface.

## STA session termination AAA initiated success

**TABLE 764** STA session termination AAA initiated success event

Event	STA session termination AAA initiated success
Event Type	staSessionTermAAAINitSuccess
Event Code	1555
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12, "srcProcess"="STA", "realm"= "wlan.mnc080.mcc405.3gppnetwork.org", "uelmsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvrIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Session Termination of {{uelmsi}}/{{ueUsername}} on {produce.short.name} [SCGMgmtIp] from 3GPP AAA [aaaSrvrIp] successful. AS-R request from AAA
Description	This event occurs when the controller receives and successfully terminates the abort session request (ASR) initiated by the 3GPP AAA server.

## STA session termination AAA initiated failed

**TABLE 765** STA session termination AAA initiated failed event

Event	STA session termination AAA initiated failed
Event Type	staSessionTermAAAINitFailed
Event Code	1556
Severity	Informational

**TABLE 765** STA session termination AAA initiated failed event (continued)

Event	STA session termination AAA initiated failed
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12, "srcProcess"="STA", "realm"= "wlan.mnc080.mcc405.3gppnetwork.org", "ueImsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvrIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Session Termination of {{ueImsi}}/{{ueUsername}} on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] failed. AS-R request from AAA
Description	This event occurs when the controller does not receive the abort session request initiated by the 3GPP AAA server.

## STA re-authorization successful

**TABLE 766** STA re-authorization successful event

Event	STA re-authorization successful
Event Type	staReAuthSuccess
Event Code	1557
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12, "srcProcess"="STA", "realm"="wlan.mnc080.mcc405.3gppnetwork.org", "ueImsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvrIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Re-Auth of {{ueImsi}}/{{ueUsername}} on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] successful
Description	This event occurs when the 3GPP AAA initiated reauthorization re-auth request (RAR) is successful.

## System Events

Following are the events with the system log severity:

**NOTE**

{produce.short.name} refers to controller.

Event	Event	Event
No LS responses on page 327	LS authentication failure on page 327	{produce.short.name} connected to LS on page 328
{produce.short.name} failed to connect to LS on page 328	{produce.short.name} received passive request on page 328	{produce.short.name} sent controller information report on page 329
{produce.short.name} received management request on page 329	{produce.short.name} sent AP info by venue report on page 329	{produce.short.name} sent associated client report on page 330
{produce.short.name} forwarded calibration request to AP on page 330	{produce.short.name} forwarded calibration request to AP on page 330	{produce.short.name} forwarded footfall request to AP on page 330
{produce.short.name} received unrecognized request on page 331	Syslog server reachable on page 331	Syslog server unreachable on page 331
Syslog server switched on page 332	System service failure on page 332	Generate AP config for plane load rebalance succeeded on page 332
Generate AP config for plane load rebalance failed on page 333	FTP transfer on page 333	FTP transfer error on page 333
CSV export FTP transfer on page 333	CSV export FTP transfer error on page 334	CSV export FTP transfer maximum retry on page 334

Event	Event	Event
CSV export disk threshold exceeded on page 334	CSV export disk max capacity reached on page 335	CSV export disk threshold back to normal on page 335
File upload on page 335	Email sent successfully on page 336	Email sent failed on page 336
SMS sent successfully on page 336	SMS sent failed on page 337	Process restart on page 337
Service unavailable on page 337	Keepalive failure on page 338	Resource unavailable on page 338
HIP started on page 338	HIP stopped on page 339	Standby HIP restarted on page 339
HIP cache cleaned on page 339	All data planes in the zone affinity profile are disconnected on page 340	CALEA UE Matched on page 340
Diameter peer transport failure on page 340	Diameter CER error on page 341	Diameter CER success on page 341
Diameter invalid version on page 342	Diameter peer add successful on page 342	ZD AP migrating on page 343
ZD AP migrated on page 343	ZD AP rejected on page 343	ZD AP migration failed on page 344
Database error on page 344	Recover cassandra error on page 344	Process initiated on page 345
PMIPv6 unavailable on page 345	Memory allocation failed on page 345	Process stopped on page 346
SZ Login Fail on page 346	SZ Login on page 346	SZ Logout on page 346
Password expiration on page 347	Admin account lockout on page 347	Admin session expired on page 347
Disable inactive admins on page 348	Two factor auth failed on page 348	Unconfirmed program detection on page 348
Admin account lockout after failed attempts on page 349	Discontinuous time change on page 349	Mesh network connectivity lost on page 349

## No LS responses

**TABLE 767** No LS responses event

Event	No LS responses
Event Type	scgLBSNoResponse
Event Code	721
Severity	Major
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] no response from LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller does not get a response while connecting to the location based service.

## LS authentication failure

**TABLE 768** LS authentication failure event

Event	LS authentication failure
Event Type	scgLBSAuthFailed
Event Code	722
Severity	Major
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] authentication failed: url=[{url}], port=[{port}]

**TABLE 768** LS authentication failure event (continued)

Event	LS authentication failure
Description	This event occurs due to the authentication failure on connecting to the location based service.

## {produce.short.name} connected to LS

**TABLE 769** {produce.short.name} connected to LS event

Event	{produce.short.name} connected to LS
Event Type	scgLBSConnectSuccess
Event Code	723
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] connected to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller successfully connects to the location based service.

## {produce.short.name} failed to connect to LS

**TABLE 770** {produce.short.name} failed to connect to LS event

Event	{produce.short.name} failed to connect to LS
Event Type	scgLBSConnectFailed
Event Code	724
Severity	Major
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] connection failed to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller failed to connect to the location based service.
Auto Clearance	This event triggers the alarm 724, which is auto cleared by the event code 723.

## {produce.short.name} received passive request

**TABLE 771** {produce.short.name} received passive request event

Event	{produce.short.name} received passive request
Event Type	scgLBSStartLocationService
Event Code	725
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "type"="", "venue"="", "SCGMgmtIp"="", "band"=""
Displayed on the web interface	SmartZone [{SCGMgmtIp}] received Passive Request, band=[{band}], type=[{type}]
Description	This event occurs when the controller receives a passive request.



## {produce.short.name} sent controller information report

**TABLE 772** {produce.short.name} sent controller information report event

Event	{produce.short.name} sent controller information report
Event Type	scgLBSSentControllerInfo
Event Code	727
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "api"="", "sw"="", "clusterName"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent Controller Info Report: mac={{mac}}, api={{api}}, sw={{sw}}, clusterName ={{clusterName}}
Description	This event occurs when the controller sends the controller information report.

## {produce.short.name} received management request

**TABLE 773** {produce.short.name} received management request event

Event	{produce.short.name} received management request
Event Type	scgLBRCvdMgmtRequest
Event Code	728
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "venue"="", "type"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] received Management Request: venue={{venue}}, type={{type}}
Description	This event occurs when the controller receives the management request.

## {produce.short.name} sent AP info by venue report

**TABLE 774** {produce.short.name} sent AP info by venue report event

Event	{produce.short.name} sent AP info by venue report
Event Type	scgLBSSendAPInfoByVenueReport
Event Code	729
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "venue"="", "count"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent AP Info by Venue Report: venue={{venue}}, count ={{count}}
Description	This event occurs when the controller sends the venue report regarding AP information.

## {produce.short.name} sent query venues report

**TABLE 775** {produce.short.name} sent query venues report event

Event	{produce.short.name} sent query venues report
Event Type	scgLBSSendVenuesReport
Event Code	730
Severity	Informational

**TABLE 775** {produce.short.name} sent query venues report event (continued)

Event	{produce.short.name} sent query venues report
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "count"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent Query Venues Report: count={count}
Description	This event occurs when the controller sends the query venue report.

## {produce.short.name} sent associated client report

**TABLE 776** {produce.short.name} sent associated client report event

Event	{produce.short.name} sent associated client report
Event Type	scgLBSSendClientInfo
Event Code	731
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "count"="", "SCGMgmtIp"="", "type"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent Associated Client Report: count= {count}, type= {type}
Description	This event occurs when the controller sends the associated client report.

## {produce.short.name} forwarded calibration request to AP

**TABLE 777** {produce.short.name} forwarded calibration request to AP event

Event	{produce.short.name} forwarded calibration request to AP
Event Type	scgLBSFwdPassiveCalReq
Event Code	732
Severity	Informational
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "SCGMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"="", "count"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] forward Passive Calibration Request to [{apName&&apMac}]: venue= {venue}, interval= {interval}, duration= {duration}, band= {band}, count= {count}
Description	This event occurs when the controller sends a forward calibration request to the AP on its reconnection to the controller.

## {produce.short.name} forwarded footfall request to AP

**TABLE 778** {produce.short.name} forwarded footfall request to AP event

Event	{produce.short.name} forwarded footfall request to AP
Event Type	scgLBSFwdPassiveFFReq
Event Code	733
Severity	Informational
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "SCGMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"=""

**TABLE 778** {produce.short.name} forwarded footfall request to AP event (continued)

Event	{produce.short.name} forwarded footfall request to AP
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] forward Passive Footfall Request to [{apName&&apMac}]: venue= [{venue}], interval= [{interval}], duration= [{duration}], band= [{band}]
Description	This event occurs when the controller sends a forward footfall request to the AP on its reconnection to the controller.

## {produce.short.name} received unrecognized request

**TABLE 779** {produce.short.name} received unrecognized request event

Event	{produce.short.name} received unrecognized request
Event Type	scgLBSRcvdUnrecognizedRequest
Event Code	734
Severity	Warning
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "type"="", "length"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] received Unrecognized: length =[{length}]
Description	This event occurs when the controller receives an unrecognized request.

## Syslog server reachable

**TABLE 780** Syslog server reachable event

Event	Syslog server reachable
Event Type	syslogServerReachable
Event Code	750
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is reachable on {produce.short.name}.
Description	This event occurs when the syslog server can be reached.

## Syslog server unreachable

**TABLE 781** Syslog server unreachable event

Event	Syslog server unreachable
Event Type	syslogServerUnreachable
Event Code	751
Severity	Major
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is unreachable on {produce.short.name}.
Description	This event occurs when the syslog server is unreachable.

**TABLE 781** Syslog server unreachable event (continued)

Event	Syslog server unreachable
Auto Clearance	This event triggers the alarm 751, which is auto cleared by the event code 750.

## Syslog server switched

**TABLE 782** Syslog server switched event

Event	Syslog server switched
Event Type	syslogServerSwitched
Event Code	752
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "srcAddress"="xxx.xxx.xxx.xxx", "destAddress"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Syslog server is switched from {{srcAddress}} to {{destAddress}} on {produce.short.name}.
Description	This event occurs when the syslog server is switched.

## System service failure

**TABLE 783** System service failure event

Event	System service failure
Event Type	systemservicefailure
Event Code	753
Severity	Critical
Attribute	"sysService"="", "hostName"=""
Displayed on the web interface	Service [sysService] on node [hostName] failed and respawning
Description	This event occurs when the service is not available.

## Generate AP config for plane load rebalance succeeded

**TABLE 784** Generate AP config for plane load rebalance succeeded event

Event	Generate AP config for plane load rebalance succeeded
Event Type	planeLoadingRebalancingSucceeded
Event Code	770
Severity	Informational
Attribute	No attributes for this event.
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing succeeded.
Description	This event occurs when the user executes the load of data plane for re-balancing and generates a new AP configuration successfully.

## Generate AP config for plane load rebalance failed

**TABLE 785** Generate AP config for plane load rebalance failed event

Event	Generate AP config for plane load rebalance failed
Event Type	planeLoadingRebalancingFailed
Event Code	771
Severity	Informational
Attribute	
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing failed.
Description	This event occurs when the user executes the load of data plane for re-balancing and generation of a new AP configuration fails.

## FTP transfer

**TABLE 786** FTP transfer event

Event	FTP transfer
Event Type	ftpTransfer
Event Code	970
Severity	Informational
Attribute	"ip"="xxx.xxx.xxx.xxx", "portID"="xxxx", "reason"="xxxxx"
Displayed on the web interface	File [{reason}] transferred to FTP server [{ip}:{portID}] successfully
Description	This event occurs when a file transfer to the FTP server is successful.

## FTP transfer error

**TABLE 787** FTP transfer error event

Event	FTP transfer error
Event Type	ftpTransferError
Event Code	971
Severity	Warning
Attribute	"ip"="xxx.xxx.xxx.xxx", "portID"="xxxx", "reason"="xxxxx"
Displayed on the web interface	File [{reason}] transferred to FTP server [{ip}:{portID}] unsuccessfully
Description	This event occurs when the file transfer to the FTP server fails.

## CSV export FTP transfer

**TABLE 788** CSV export FTP transfer event

Event	CSV export FTP transfer
Event Type	csvFtpTransfer
Event Code	972
Severity	Informational

**TABLE 788** CSV export FTP transfer event (continued)

Event	CSV export FTP transfer
Attribute	"nodeName"="xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx", "portID"="xx:xx:xx:xx:xx", "filename"="xxx.xxx.xxx.xxx"
Displayed on the web interface	CSV export file {{filename}} transferred on control plane {{nodeName}}-C to FTP server {{ip}}:{{portID}}successfully.
Description	This event occurs when the CSV file is successfully sent to a remote server.

## CSV export FTP transfer error

**TABLE 789** CSV export FTP transfer error event

Event	CSV export FTP transfer error
Event Type	csvFtpTransferError
Event Code	973
Severity	Warning
Attribute	"nodeName"="xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx", "portID"="xx:xx:xx:xx:xx", "filename"="xxx.xxx.xxx.xxx"
Displayed on the web interface	CSV export file {{filename}} transferred on control plane {{nodeName}}-C to FTP server {{ip}}:{{portID}}unsuccessfully.
Description	This event occurs when the CSV file transfer to the remote sever fails.
Auto Clearance	This event triggers the alarm 973, which is auto cleared by the event code 972.

## CSV export FTP transfer maximum retry

**TABLE 790** CSV export FTP transfer maximum retry event

Event	CSV export FTP maximum retry
Event Type	csvFtpTransferMaxRetryReached
Event Code	974
Severity	Major
Attribute	"nodeName"="xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx", "portID"="xx:xx:xx:xx:xx", "filename"="xxx.xxx.xxx.xxx"
Displayed on the web interface	CSV export file {{filename}} transferred on control plane {{nodeName}}-C to FTP server {{ip}}:{{portID}} max retries reached.
Description	This event occurs when the CSV file fails to transfer after a maximum of five (5) retries.

## CSV export disk threshold exceeded

**TABLE 791** CSV export disk threshold exceeded event

Event	CSV export disk threshold exceeded
Event Type	csvDiskThresholdExceeded
Event Code	975
Severity	Warning
Attribute	"nodeName"="xx:xx:xx:xx:xx", "threshold"="xx:xx:xx:xx:xx", "availableDiskSize"="xx:xx:xx:xx:xx",

**TABLE 791** CSV export disk threshold exceeded event (continued)

Event	CSV export disk threshold exceeded
Displayed on the web interface	CSV export disk threshold $\{\{threshold\}\}$ exceeded on control plane $\{\{nodeName\}\}$ -C. Available disk size left $\{\{availableDiskSize\}\}$ .
Description	This event occurs when the CSV report size exceeds 80% of its capacity.

## CSV export disk max capacity reached

**TABLE 792** CSV export disk max capacity reached event

Event	CSV export disk max capacity reached
Event Type	csvDiskMaxCapacityReached
Event Code	976
Severity	Critical
Attribute	CSV export disk maximum capacity reached on control plane $\{\{nodeName\}\}$ -C. Allocated disk size $\{\{allocatedDiskSize\}\}$ .
Displayed on the web interface	CSV export disk threshold $\{\{threshold\}\}$ exceeded on control plane $\{\{nodeName\}\}$ -C. Available disk size left $\{\{availableDiskSize\}\}$ .
Description	This event occurs when the CSV report size reaches its maximum capacity.

## CSV export disk threshold back to normal

**TABLE 793** CSV export disk threshold back to normal event

Event	CSV export disk threshold back to normal
Event Type	csvDiskThresholdBackToNormal
Event Code	977
Severity	Informational
Attribute	"nodeName"="xx.xx.xx.xx.xx ", "availableDiskSize"="xx.xx.xx.xx.xx", "currentUsedPercent"="xx.xx.xx.xx.xx"
Displayed on the web interface	CSV export disk usage $\{\{currentUsedPercent\}\}$ got back to normal on control plane $\{\{nodeName\}\}$ -C. Available disk size left $\{\{availableDiskSize\}\}$ .
Description	This event occurs when the CSV export file is under the threshold limit.

## File upload

**TABLE 794** File upload event

Event	File upload
Event Type	fileUpload
Event Code	980
Severity	Informational
Attribute	"ip"="xxx.xxx.xxx.xxx", "cause"="xxxxx"
Displayed on the web interface	Backup file $\{\{cause\}\}$ uploading from $\{\{ip\}\}$ failed
Description	This event occurs when the backup file upload fails.

## Email sent successfully

**TABLE 795** Email sent successfully event

Event	Email sent successfully
Event Type	mailSendSuccess
Event Code	981
Severity	Informational
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	{{srcProcess}} sent email to {{receiver}} successfully.
Description	This event occurs when system sends mail successfully.

## Email sent failed

**TABLE 796** Email sent failed event

Event	Email sent failed
Event Type	mailSendFailed
Event Code	982
Severity	Warning
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	{{srcProcess}} sent email to {{receiver}} failed.
Description	This event occurs when the system fails to send the mail.

## SMS sent successfully

**TABLE 797** SMS sent successfully event

Event	SMS sent successfully
Event Type	smsSendSuccess
Event Code	983
Severity	Informational
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	{{srcProcess}} sent short message to {{receiver}} successfully.
Description	This event occurs when system sends the short message successfully.



## SMS sent failed

**TABLE 798** SMS sent failed event

Event	SMS sent failed
Event Type	smsSendFailed
Event Code	984
Severity	Warning
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "reason"="xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	{{srcProcess}} sent short message to {{receiver}} failed, reason: {{reason}}.
Description	This event occurs when system fails to send the short message.

## Process restart

**TABLE 799** Process restart event

Event	Process restart
Event Type	processRestart
Event Code	1001
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA", "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{processName}} process got re-started on {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when any process crashes and restarts.

## Service unavailable

**TABLE 800** Service unavailable event

Event	Service unavailable
Event Type	serviceUnavailable
Event Code	1002
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA", "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{processName}} process is not stable on {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when the process repeatedly restarts and is unstable.

## Keepalive failure

**TABLE 801** Keepalive failure event

Event	Keepalive failure
Event Type	keepAliveFailure
Event Code	1003
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA", "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} on {produce.short.name} {{SCGMgmtIp}} restarted [{processName}] process.
Description	This event occurs when the <b>mon/nc</b> restarts the process due to a keep alive failure.

## Resource unavailable

**TABLE 802** Resource unavailable event

Event	Resource unavailable
Event Type	resourceUnavailable
Event Code	1006
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd", "realm"="NA", "SCGMgmtIp"="3.3.3.3", "cause"="xx"
Displayed on the web interface	System resource [{cause}] not available in [{srcProcess}] process at {produce.short.name} {{SCGMgmtIp}}
Description	This event is generated due to unavailability of any other system resource, such as memcached.

## HIP started

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 803** HIP started event

Event	HIP started
Event Type	hipStarted
Event Code	1014
Severity	Informational
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	{{srcProcess}} process gets Started on {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when the HIP instance starts.

## HIP stopped

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 804** HIP stopped event

Event	HIP stopped
Event Type	hipStopped
Event Code	1015
Severity	Informational
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	{{srcProcess}} process stopped HIP on {produce.short.name} {{SCGMgmtIp}}
Description	This event occurs when HIP is stopped.

## Standby HIP restarted

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 805** Standby HIP restarted event

Event	Standby HIP restarted
Event Type	hipStandbyRestart
Event Code	1017
Severity	Informational
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	{{srcProcess}} Standby HIP node failed detected from Active {produce.short.name} {{SCGMgmtIp}}
Description	This event is logged when the active node detects failure of the standby node.

## HIP cache cleaned

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 806** HIP cache cleaned event

Event	HIP cache cleaned
Event Type	hipCacheCleanup
Event Code	1018
Severity	Informational
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102", mvnold="12", hlrProfileName="HLR1",
Displayed on the web interface	{{srcProcess}} Cache cleanup started on {produce.short.name} {{SCGMgmtIp}}

**TABLE 806** HIP cache cleaned event (continued)

Event	HIP cache cleaned
Description	This event is generated when the cache cleanup process is completed.

## All data planes in the zone affinity profile are disconnected

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 807** All data planes in the zone affinity profile are disconnected event

Event	All data planes in the zone affinity profile are disconnected
Event Type	zoneAffinityLastDpDisconnected
Event Code	1267
Severity	Major
Attribute	"dpName="xxxxxxx", "dpKey"="xx:xx:xx:xx:xx:xx", "zoneAffinityProfileId"="xxxxxxx"
Displayed on the web interface	The Last one Data Plane [{dpName&&dpKey}] is disconnected Zone Affinity profile [{zoneAffinityProfileId}].
Description	This event occurs when all the data planes disconnect from the zone affinity profile.

## CALEA UE Matched

**TABLE 808** CALEA UE Matched event

Event	CALEA UE Matched
Event Type	dpCaleaUeInterimMatched
Event Code	1268
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	CALEA matches client [{clientMac}] on WLAN [{ssid   authType}]from AP [{apName&&apMac}]. TxBytes[{txBytes}], RxBytes[{rxBytes}].
Description	This event occurs when the data plane CALEA user equipment and client matches.

## Diameter peer transport failure

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 809** Diameter peer transport failure event

Event	Diameter peer transport failure
Event Type	diaPeerTransportFailure
Event Code	1403
Severity	Major

**TABLE 809** Diameter peer transport failure event (continued)

Event	Diameter peer transport failure
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"="839f87c6-d116-497e-afce-aa8157abd30c", "srcProcess"="<Application Name>", "realm"="ruckus.com", "originHost" = "Node1", "SCGMgmtIp"="2.2.2.2", "peerIp" = "3.3.3.3", "peerName" = "OCS1", "peerRealmName" = "operator.com", "desc" = "Failed to read from peer socket"
Displayed on the web interface	[[srcProcess]] Failed to read from peer [[peerName]] Transport Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This event occurs when the transport with the peer is down and the stack fails to read the data.

## Diameter CER error

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 810** Diameter CER error event

Event	Diameter CER error
Event Type	diaCERError
Event Code	1404
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"="839f87c6-d116-497e-afce-aa8157abd30c", "srcProcess"="<Application Name>", "realm"="ruckus.com", "originHost" = "Node1", "SCGMgmtIp"="2.2.2.2", "peerIp" = "3.3.3.3", "peerName" = "OCS1", "peerRealmName" = "operator.com", "desc" = "Failed to decode CER from Peer"
Displayed on the web interface	[[srcProcess]] Failed to decode CER from Peer [[peerName]] Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This event occurs when the diameter stack fails to decode the capabilities exchange request (CER) received from peer.

## Diameter CER success

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 811** Diameter CER success event

Event	Diameter CER success
Event Type	diaCERSuccess
Event Code	1405
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"="839f87c6-d116-497e-afce-aa8157abd30c", "srcProcess"="<Application Name>", "realm"="ruckus.com", "originHost" = "Node1", "SCGMgmtIp"="2.2.2.2", "peerIp" = "3.3.3.3", "peerName" = "OCS1", "peerRealmName" = "organization.com", "desc" = "Successfully decoded CER received from Peer"

**TABLE 811** Diameter CER success event (continued)

Event	Diameter CER success
Displayed on the web interface	{{srcProcess}} CER Success From Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the CER received from peer is successfully decoded.

## Diameter invalid version

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 812** Diameter invalid version event

Event	Diameter invalid version
Event Type	diaInvalidVer
Event Code	1406
Severity	Warning
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"="839f87c6-d116-497e-afce-aa8157abd30c", "src Process"="<Application Name>", "realm"="ruckus.com", "originHost" = "Node1", "SCGMgmtIp"="2.2.2.2", "peerIp" = "3.3.3.3", "peerName" = "OCS1", "peerRealmName" = "organization.com", "desc" = "Invalid version in Diameter header of received CER from peer"
Displayed on the web interface	{{srcProcess}} Invalid version in Diameter header in CER from Peer [{peerName}], Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the version in the diameter header of received CER is invalid.

## Diameter peer add successful

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 813** Diameter peer add successful event

Event	Diameter peer add successful
Event Type	diaPeerAddSuccess
Event Code	1408
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"="839f87c6-d116-497e-afce-aa8157abd30c", "srcProcess"="<Application Name>", "realm"="ruckus.com", "originHost" = "Node1", "SCGMgmtIp"="2.2.2.2", "peerIp" = "3.3.3.3", "peerName" = "OCS1", "peerRealmName" = "organization.com", "desc" = "Peer addition successful"
Displayed on the web interface	{{srcProcess}} Peer [{peerName}] Realm [{peerRealmName}] addition is successful on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the peer addition is successful.

## ZD AP migrating

**TABLE 814** ZD AP migrating event

Event	ZD AP migrating
Event Type	zdAPMigrating
Event Code	2001
Severity	Informational
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="ZF7962", "firmware"="3.0.0.0"
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is upgrading with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP is upgrading with the controller AP firmware image.

## ZD AP migrated

**TABLE 815** ZD AP migrated event

Event	ZD AP migrated
Event Type	zdAPMigrated
Event Code	2002
Severity	Informational
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="R700", "firmware"="3.2.0.0.x"
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] has been upgraded with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP has upgraded its firmware with the controller AP firmware image.

## ZD AP rejected

**TABLE 816** ZD AP rejected event

Event	ZD AP rejected
Event Type	zdAPRejected
Event Code	2003
Severity	Warning
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="ZF7962"
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is not being upgraded with {produce.short.name} AP firmware because of ACL setting.
Description	This event occurs when the ZoneDirector AP is not upgraded with the controller AP firmware because of ACL setting.

## ZD AP migration failed

**TABLE 817** ZD AP migration failed event

Event	ZD AP migration failed
Event Type	zdAPMigrationFailed
Event Code	2004
Severity	Major
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="ZF7962", "firmware"="3.0.0.0.0"
Displayed on the web interface	ZD-AP {{apMac}} / {{serialNumber}} model {{model}} is failed to upgrade with {produce.short.name} AP firmware version - {{firmware}}
Description	This event occurs when the Zone Director AP fails to upgrade with the controller AP firmware image.

## Database error

**TABLE 818** Database error event

Event	Database error
Event Type	cassandraError
Event Code	3001
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2", reason="reason",
Displayed on the web interface	Database internal error on node {{nodeName}}, reason: {{reason}}.
Description	This event occurs due to internal errors on the database.

## Recover cassandra error

**TABLE 819** Recover cassandra error event

Event	Recover cassandra error
Event Type	recoverCassandraError
Event Code	3011
Severity	Informational
Attribute	"nodeName"="xxx", "reason"="recovery reason"
Displayed on the web interface	Recover database error on node {{nodeName}}, reason: []
Description	This event occurs when the internal errors on the database are fixed.



## Process initiated

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 820** Process initiated event

Event	Process initiated
Event Type	processInit
Event Code	5001
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process got re-started on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when PMIPv6 process crashes and restarts.

## PMIPv6 unavailable

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 821** PMIPv6 unavailable event

Event	PMIPv6 unavailable
Event Type	pmipUnavailable
Event Code	5002
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process is not stable on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the PMIPv6 process repeatedly restarts and is not stable.

## Memory allocation failed

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 822** Memory allocation failed event

Event	Memory allocation failed
Event Type	unallocatedMemory
Event Code	5003
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Insufficient Heap Memory in PMIPv6 process at {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the memory allocation fails in the PMIPv6 process.

## Process stopped

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 823** Process stopped event

Event	Process stopped
Event Type	processStop
Event Code	5100
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2",
Displayed on the web interface	PMIPv6 process stop on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the PMIPv6 process stops

## SZ Login Fail

**TABLE 824** SZ login fail event

Event	SZ login fail
Event Type	szLoginFail
Event Code	8007
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on failed from [{ip}].
Description	Administrator logged on failed SZ.

## SZ Login

**TABLE 825** SZ login event

Event	SZ login
Event Type	szLogin
Event Code	8008
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on from [{ip}].
Description	Administrator logged on SZ.

## SZ Logout

**TABLE 826** SZ logout event

Event	SZ logout
Event Type	szLogout

**TABLE 826** SZ logout event (continued)

Event	SZ logout
Event Code	8009
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged off from [{ip}].
Description	Administrator logged off SZ.

## Password expiration

**TABLE 827** Password expiration event

Event	Password expiration
Event Type	passwordExpiration
Event Code	8010
Severity	Informational
Attribute	userId = "x", time = "mm:dd:yyyy hh:mm:ss"
Displayed on the web interface	Administrative account [{userId}] password has expired as of [{time}].
Description	This event occurs when the password expires.

## Admin account lockout

**TABLE 828** Admin account lockout event

Event	Admin account lockout
Event Type	Admin account lockout
Event Code	8011
Severity	Warning
Attribute	User Account Name User IP Address Lock Duration Time
Displayed on the web interface	Administrative account [User Account Name] has been locked out because of repeated login failures from [User IP Address], wait for [Lock Duration Time] minutes to re-login.
Description	This event occurs when the account is locked.

## Admin session expired

**TABLE 829** Admin session expired event

Event	Admin session expired
Event Type	AdminSessionExpired
Event Code	8012
Severity	Informational
Attribute	userName = "x"

**TABLE 829** Admin session expired event (continued)

Event	Admin session expired
Displayed on the web interface	Administrative account [{userName}] login session has timed out.
Description	This event occurs when the session is timed out due to inactivity or because of absolute session timeout.

## Disable inactive admins

**TABLE 830** Disable inactive admins event

Event	Disable inactive admins
Event Type	DisableInactiveAdmins
Event Code	8013
Severity	Informational
Attribute	userName = "x", inactiveDays="x"
Displayed on the web interface	Administrative account [{userName}] has been disabled due to not logging for [{inactiveDays}] days.
Description	This event occurs when the account is disabled for a period of time.

## Two factor auth failed

**TABLE 831** Two factor auth failed event

Event	Two factor auth failed
Event Type	TwoFactorAuthFailed
Event Code	8014
Severity	Warning
Attribute	userName = "x"
Displayed on the web interface	Administrative account [{userName}] failed to response the SMS one time password code.
Description	This event occurs when the account fails to send a one time password code as a SMS text.

**NOTE**

Refer to [System Events](#) on page 326.

## Unconfirmed program detection

**TABLE 832** Unconfirmed program detection event

Event	Unconfirmed program detection
Event Type	Unconfirmed Program Detection
Event Code	1019
Severity	Warning
Attribute	"nodeName"="xxx", "status"="xxxxx"
Displayed on the web interface	Detect unconfirmed program on control plane [{nodeName}]. [{status}]

**TABLE 832** Unconfirmed program detection event (continued)

Event	Unconfirmed program detection
Description	This event occurs when an unconfirmed program is detected.

## Admin account lockout after failed attempts

**TABLE 833** Admin account lockout after failed attempts

Event	Admin account lockout after failed attempts
Event Type	Admin account lockout after failed attempts
Event Code	8016
Severity	Warning
Attribute	User account name, User IP address
Displayed on the web interface	Administrative account [User account name] is locked out because of repeated login failure from [User IP Address]
Description	This event occurs when the user account is locked on failed attempts

## Discontinuous time change

**TABLE 834** Discontinuous time change

Event	Discontinuous time change
Event Type	Discontinuous time change
Event Code	99301
Severity	Warning
Attribute	FromTime, ToTime, NTP Server, SZ IP
Displayed on the web interface	The discontinuous time of the controller is changed from [ Fromtime] to [Totime], server: [NTP Server], IP: [SZ IP]
Description	This event occurs when the discontinuous time of the controller changes to more than a minute

## Mesh network connectivity lost

**TABLE 835** Mesh network connectivity lost event

Event	Mesh network connectivity lost
Event Type	meshConnectivityFailed
Event Code	9116
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currIface = "xxxxx", "apName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] Mesh network connectivity lost on [{currIface}]
Description	This event occurs when mesh network connectivity is lost.

## Failure of Key Generation

**TABLE 836** Failure of Key Generation

Event	Failure of Key Generation
Event Type	keyGenFail
Event Code	99100
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Failure of Key generation. Reason : {{reason}} failed
Description	This event occurs when Smart Zone key generation is failed.

## Failure of IPsec

**TABLE 837** Failure of IPsec Event

Event	Failure of IPsec
Event Type	IPSecFailure
Event Code	99101
Severity	Major
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63", "reason"="Root CA is expired"
Displayed on the web interface	Failure of IP Sec. Reason : {{reason}} failed
Description	This event occurs when Smart Zone IPsec is failed.

## Failure Certificate

**TABLE 838** Failure Certificate Event

Event	Failure Certificate
Event Type	FailureCertificate
Event Code	99102
Severity	Major
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63", "reason"="Root CA is expired"
Displayed on the web interface	Failure of Certificate Reason : {{reason}} failed
Description	This event occurs when Smart Zone server certificate validation is failed.

## IPsec KE is Up

**TABLE 839** IPsec IKE is Up Event

Event	IPsec IKE is Up
Event Type	IPSecIKEup
Event Code	99103
Severity	Informational

**TABLE 839** IPsec IKE is Up Event (continued)

Event	IPsec IKE is Up
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63", "srcProcess"="strongswan", "SCGMgmtIp"="10.206.66.223", "reason"="System IPsec IKE is up"
Displayed on the web interface	IPsec IKE is Up. Reason : [{reason}] failed
Description	This event occurs when Smart Zone IPsec IKE is up.

## IPsec IKE is Down

**TABLE 840** IPsec IKE is Down Event

Event	IPsec IKE is Down
Event Type	IPSecIKEDown
Event Code	99104
Severity	Critical
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63", "srcProcess"="strongswan", "SCGMgmtIp"="10.206.66.223", "reason"="System IPsec IKE is terminated"
Displayed on the web interface	IPsec IKE is down. Reason : [{reason}] failed
Description	This event occurs when Smart Zone IPsec IKE is down.

## Discontinuous Time Change

**TABLE 841** Discontinuous Time Change Event

Event	Discontinuous Time Change
Event Type	DiscontinuousTimeChange
Event Code	99301
Severity	Warning
Attribute	Discontinuous Time Change, "before"= , "after"=
Displayed on the web interface	
Description	This event occurs when the time of Smart Zone is changed discontinuously.

## Switch Events

Following are the events related to switch severity:

- [Switch critical message](#) on page 352
- [Switch alert message](#) on page 352
- [Switch warning message](#) on page 353
- [Switch CPU warning threshold exceed](#) on page 353
- [Switch CPU major threshold exceed](#) on page 353
- [Switch CPU critical threshold exceed](#) on page 353

- [Switch memory warning threshold exceed](#) on page 354
- [Switch memory major threshold exceed](#) on page 354
- [Switch memory critical threshold exceed](#) on page 354
- [Switch custom warning threshold exceed](#) on page 355
- [Switch custom major threshold exceed](#) on page 355
- [Switch custom critical threshold exceed](#) on page 355
- [GetCACert Request](#) on page 355
- [Certificate signing request](#) on page 356
- [Accept certificate signing request](#) on page 356
- [Reject certificate signing request](#) on page 356
- [Pending certificate signing request](#) on page 357
- [Over Switch Max Capacity](#) on page 357
- [Switch Duplicated](#) on page 357
- [Switch Firmware Upgrade](#) on page 358
- [Switch is Offline for 15 Minutes](#) on page 357
- [Switch Firmware Upgrade Failed](#) on page 358
- [Switch Configuration Update](#) on page 358
- [Switch Configuration Update Failed](#) on page 359
- [Switch Reboot](#) on page 359

## Switch critical message

**TABLE 842** Switch critical message event

Event	Switch critical message
Event Type	SwitchCriticalMessage
Event Code	20000
Severity	Critical
Description	This event occurs when the there is a switch critical message.

## Switch alert message

**TABLE 843** Switch alert message event

Event	Switch alert message
Event Type	SwitchAlertMessage
Event Code	20001
Severity	Major
Description	This event occurs when there is a switch alert message.



## Switch warning message

**TABLE 844** Switch warning message event

Event	Switch warning message
Event Type	SwitchWarningMessage
Event Code	20003
Severity	Warning
Description	This event occurs when there is a switch warning message.

## Switch CPU warning threshold exceed

**TABLE 845** Switch CPU warning threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	warningCpuThresholdExceed
Event Code	22010
Severity	Warning
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (1% - Major Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU warning threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the warning threshold.

## Switch CPU major threshold exceed

**TABLE 846** Switch CPU major threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	majorCpuThresholdExceed
Event Code	22011
Severity	Major
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Warning Threshold – Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU major threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the major threshold.

## Switch CPU critical threshold exceed

**TABLE 847** Switch CPU critical threshold exceed event

Event	Switch CPU critical threshold exceed
Event Type	criticalCpuThresholdExceed
Event Code	22012
Severity	Critical
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Major Threshold - 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"

**TABLE 847** Switch CPU critical threshold exceed event (continued)

Event	Switch CPU critical threshold exceed
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU critical threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the critical threshold.

## Switch memory warning threshold exceed

**TABLE 848** Switch memory warning threshold exceed event

Event	Switch memory warning threshold exceed
Event Type	warningMemoryThresholdExceed
Event Code	22020
Severity	Warning
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (1% - Major Threshold), switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory warning threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the warning threshold.

## Switch memory major threshold exceed

**TABLE 849** Switch memory major threshold exceed event

Event	Switch memory major threshold exceed
Event Type	majorMemoryThresholdExceed
Event Code	22021
Severity	Major
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Warning Threshold – Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the major threshold.

## Switch memory critical threshold exceed

**TABLE 850** Switch memory critical threshold exceed event

Event	Switch memory critical threshold exceed
Event Type	criticalMemoryThresholdExceed
Event Code	22022
Severity	Critical
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Major Threshold – 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory critical threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the critical threshold of 100%.

## Switch custom warning threshold exceed

**TABLE 851** Switch custom warning threshold exceed event

Event	Switch custom warning threshold exceed
Event Type	hitWarningSwitchCombinedEvent
Event Code	22030
Severity	Warning
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Warning Event] {userDefinedDescription}
Description	This event occurs when the Switch custom warning event crosses the threshold.

## Switch custom major threshold exceed

**TABLE 852** Switch custom major threshold exceed event

Event	Switch custom major threshold exceed
Event Type	hitMajorSwitchCombinedEvent
Event Code	22031
Severity	Major
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Major Event] {userDefinedDescription}
Description	This event occurs when the Switch custom major event crosses the threshold.

## Switch custom critical threshold exceed

**TABLE 853** Switch custom critical threshold exceed event

Event	Switch custom critical threshold exceed
Event Type	hitCriticalSwitchCombinedEvent
Event Code	22032
Severity	Critical
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Critical Event] {userDefinedDescription}
Description	This event occurs when the Switch custom critical event crosses the threshold.

## GetCACert Request

**TABLE 854** GetCACert Request event

Event	GetCACert Request
Event Type	getCACertRequest
Event Code	22000
Severity	Informational

**TABLE 854** GetCACert Request event (continued)

Event	GetCACert Request
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] GetCACert Request.
Description	This event occurs when there is a SCEP GetCACert Request.

## Certificate signing request

**TABLE 855** Certificate signing request event

Event	Certificate signing request
Event Type	certificateSigningRequest
Event Code	22001
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Certificate Signing Request.
Description	This event occurs when there is a SCEP Certificate Signing Request.

## Accept certificate signing request

**TABLE 856** Accept certificate signing request event

Event	Accept certificate signing request
Event Type	acceptCertificateSigningRequest
Event Code	22002
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Accept Certificate Signing Request.
Description	This event occurs when there is a SCEP Accept Certificate Signing Request.

## Reject certificate signing request

**TABLE 857** Reject certificate signing request event

Event	Reject certificate signing request
Event Type	rejectCertificateSigningRequest
Event Code	22003
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Reject Certificate Signing Request.
Description	This event occurs when there is a SCEP Reject Certificate Signing Request.

## Pending certificate signing request

**TABLE 858** Pending certificate signing request event

Event	Pending certificate signing request
Event Type	pendingCertificateSigningRequest
Event Code	22004
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Pending Certificate Signing Request.
Description	This event occurs when there is a SCEP Pending Certificate Signing Request.

## Switch is Offline for 15 Minutes

**TABLE 859** Switch is Offline for 15 Minutes event

Event	Switch is Offline for 15 Minutes
Event Type	SwitchOffline+B688
Event Code	21000
Severity	Warning
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[[switchSerialNumber] / {switchName}] offline for more than 15 minutes
Description	This event occurs when the switch is offline over 15 minutes

## Over Switch Max Capacity

**TABLE 860** Over Switch Max Capacity event

Event	Over Switch Max Capacity
Event Type	OverSwitchMaxCapacity
Event Code	21001
Severity	Critical
Displayed on the web interface	The volume of switches is over system capacity.
Description	This event occurs when the volumn of switches is over system capacity

## Switch Duplicated

**TABLE 861** Switch Duplicated event

Event	Switch Duplicated
Event Type	SwitchDuplicated
Event Code	21002
Severity	Warning
Attributes	"switchSerialNumber"="x",switchName = "x", "switchMac"="aa:bb:cc:dd:ee:ff", "duplicatedSwitchSerialNumber"="x", "duplicatedSwitchName"="x"

**TABLE 861** Switch Duplicated event (continued)

Event	Switch Duplicated
Displayed on the web interface	{{switchSerialNumber} / {switchName}} A duplicated switch mac address from {{duplicatedSwitchSerialNumber}}/{{duplicatedSwitchName}} is coming while existing one {{switchMac}} is online.
Description	This event occurs when duplicated switches are detected.

## Switch Firmware Upgrade

**TABLE 862** Switch Firmware Upgrade event

Event	Switch Firmware Upgrade
Event Type	SwitchFirmwareUpgrade
Event Code	22041
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} Switch firmware upgraded
Description	This event occurs when the switch firmware is upgraded.

## Switch Firmware Upgrade Failed

**TABLE 863** Switch Firmware Upgrade Failed event

Event	Switch Firmware Upgrade Failed
Event Type	SwitchFirmwareUpgradeFailed
Event Code	22042
Severity	Critical
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} switch firmware upgrade failed
Description	This event occurs when the switch firmware upgrade is failed.

## Switch Configuration Update

**TABLE 864** Switch Configuration Update event

Event	Switch Configuration Update
Event Type	SwitchConfigurationUpdate
Event Code	22051
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} switch configuration update
Description	This event occurs when the switch configuration is updated.

## Switch Configuration Update Failed

**TABLE 865** Switch Configuration Update Failed event

Event	Switch Configuration Update Failed
Event Type	SwitchConfigurationUpdateFailed
Event Code	22052
Severity	Critical
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} switch configuration update failed
Description	This event occurs when the switch configuration update is failed.

## Switch Reboot

**TABLE 866** Switch Reboot event

Event	Switch Reboot
Event Type	SwitchReboot
Event Code	22061
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} offline for more than 15 minutes
Description	This event occurs when the Switch re-booted by the controller.

## Switch Delete

**TABLE 867** Switch Delete Event

Event	Switch Delete
Event Type	switchDeleteByController
Event Code	22071
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch was deleted by the controller.
Description	This event occurs when the switch was deleted by the controller.

## Switch Disconnected from the Controller

**TABLE 868** Switch Disconnected from the Controller Event

Event	Switch Disconnected from the Controller
Event Type	switchDisconnectFromController
Event Code	22081
Severity	Informational

**TABLE 868** Switch Disconnected from the Controller Event (continued)

Event	Switch Disconnected from the Controller
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch disconnected from the controller.
Description	This event occurs when the switch is disconnected from the controller.

## Switch is Connected to the Controller

**TABLE 869** Switch is Connected to the Controller Event

Event	Switch is Connected to the Controller
Event Type	switchConnectToController
Event Code	22082
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch is connected to the controller.
Description	This event occurs when the switch is connected to the controller.

## Switch Discovered by the Controller

**TABLE 870** Switch Discovered by the Controller Event

Event	Switch Discovered by the Controller
Event Type	switchDiscoverByController
Event Code	22091
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch discovered by the controller.
Description	This event occurs when the switch is discovered by the controller.

## Threshold Events

Following are the events related to threshold system set:

- [CPU threshold exceeded](#) on page 361
- [Memory threshold exceeded](#) on page 361
- [Disk usage threshold exceeded](#) on page 361
- [CPU threshold back to normal](#) on page 362
- [Memory threshold back to normal](#) on page 362
- [Disk threshold back to normal](#) on page 362
- [License threshold exceeded](#) on page 363
- [The drop of client count threshold exceeded](#) on page 363



- [Rate limit threshold surpassed](#) on page 363
- [Rate limit threshold restored](#) on page 364
- [Rate limit for TOR surpassed](#) on page 364
- [The number of users exceed its limit](#) on page 364
- [The number of devices exceeded its limit](#) on page 365
- [Over AP maximum capacity](#) on page 365
- [Over Device Maximum Capacity](#) on page 365
- [Device Capacity Threshold Back to Normal](#) on page 366

## CPU threshold exceeded

**TABLE 871** CPU threshold exceeded event

Event	CPU threshold exceeded
Event Type	cpuThresholdExceeded
Event Code	950
Severity	Critical
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	CPU threshold [{perc}%] exceeded on control plane [{nodeName}-C]
Description	This event occurs when the CPU usage exceeds the threshold limit of 80%.
Auto Clearance	This event triggers the alarm 950, which is auto cleared by the event code 954.

## Memory threshold exceeded

**TABLE 872** Memory threshold exceeded event

Event	Memory threshold exceeded
Event Type	memoryThresholdExceeded
Event Code	951
Severity	Critical
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This event occurs when the memory usage exceeds the threshold limit of 85% and for vSZ-H the limit is 90%.
Auto Clearance	This event triggers the alarm 951, which is auto cleared by the event code 954.

## Disk usage threshold exceeded

**TABLE 873** Disk usage threshold exceeded event

Event	Disk usage threshold exceeded
Event Type	diskUsageThresholdExceeded
Event Code	952
Severity	Critical

**TABLE 873** Disk usage threshold exceeded event (continued)

Event	Disk usage threshold exceeded
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk usage threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This event occurs when the disk usage exceeds the threshold limit of 80%.
Auto Clearance	This event triggers the alarm 952, which is auto cleared by the event code 955.

## CPU threshold back to normal

**TABLE 874** CPU threshold back to normal event

Event	CPU threshold back to normal
Event Type	cpuThresholdBackToNormal
Event Code	953
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	CPU threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the CPU usage comes back to normal.

## Memory threshold back to normal

**TABLE 875** Memory threshold back to normal event

Event	Memory threshold back to normal
Event Type	memoryThresholdBackToNormal
Event Code	954
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Memory threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the memory usage comes back to normal.

## Disk threshold back to normal

**TABLE 876** Disk threshold back to normal event

Event	Disk threshold back to normal
Event Type	diskUsageThresholdBackToNormal
Event Code	955
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the disk usage comes back to normal.

## License threshold exceeded

**TABLE 877** License threshold exceeded event

Event	License threshold exceeded
Event Type	licenseThresholdExceeded
Event Code	960
Severity	Critical 90%; Major 80%; Informational 70%;
Attribute	"perc"="xxx", "nodeName"="", "nodeMac"="xx:xx:xx:xx:xx", licenseType="SG00"
Displayed on the web interface	{{licenseType}} limit reached at {{perc}}%
Description	This event occurs when the number of user equipment is attached to the system has exceeded the license limit.

## The drop of client count threshold exceeded

**TABLE 878** The drop of client count threshold exceeded event

Event	The drop of client count threshold exceeded
Event Type	clientCountDropThresholdExceeded
Event Code	956
Severity	Warning
Attribute	"perc"="XX"
Displayed on the web interface	The drop of client count exceeded threshold {{perc}}% in cluster.
Description	This event occurs when client count exceeds the criterion value of 1500 and the drop percentage exceeds the threshold limit of 60%.

## Rate limit threshold surpassed

**TABLE 879** Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major
Attribute	"mvsold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "UserName"=abc@xyz.com "realm"="wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold surpassed for AAA Server [{{aaaSrvrIp}}] and ServerType [{{AAAServerType}}]
Description	This event occurs when the rate limit threshold is surpassed. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds the limit of 701.

## Rate limit threshold restored

**TABLE 880** Rate limit threshold restored event

Event	Rate limit threshold restored
Event Type	rateLimitThresholdRestored
Event Code	1301
Severity	Informational
Attribute	"mvsold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "UserName"=abc@xyz.com "realm"="wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold restored for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is restored. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server is lesser or equal to 700.

## Rate limit for TOR surpassed

**TABLE 881** Rate limit for TOR surpassed event

Event	Rate limit for TOR surpassed
Event Type	rateLimitMORSurpassed
Event Code	1302
Severity	Critical
Attribute	"mvsold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "UserName"=abc@xyz.com "realm"="wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This event occurs when the rate limit for maximum outstanding requests (MOR) is surpassed. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds 1000.
Auto Clearance	This event triggers the alarm1302, which is auto cleared by the event code 1301.

## The number of users exceed its limit

**TABLE 882** The number of users exceed its limit event

Event	The number of users exceed its limit
Event Type	tooManyUsers
Event Code	7001
Severity	Major
Attribute	No attributes for this event.

**TABLE 882** The number of users exceed its limit event (continued)

Event	The number of users exceed its limit
Displayed on the web interface	The number of users exceeded its limit.
Description	This event occurs when the number of users exceeds the specified limit. The threshold limit for the controller is 950000.

## The number of devices exceeded its limit

**TABLE 883** The number of devices exceeded its limit event

Event	The number of devices exceeded its limit
Event Type	tooManyDevices
Event Code	7002
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	The number of devices exceeded its limit
Description	This event occurs when the number of devices exceeds the specified limit. The threshold limit for the controller is 2850000.

## Over AP maximum capacity

**TABLE 884** Over AP maximum capacity event

Event	Over AP maximum capacity
Event Type	apCapacityReached
Event Code	962
Severity	Warning
Attribute	
Displayed on the web interface	The volume of AP is over system capacity.
Description	This event occurs when the volume of AP is over system capacity.

## Over Device Maximum Capacity

**TABLE 885** Over Device Maximum Capacity event

Event	Over Device Maximum Capacity
Event Type	connectedDeviceMaxCapacityReached
Event Code	963
Severity	Warning
Attributes	"deviceType"="xx"
Displayed on the web interface	The volume of {{deviceType}} is over maximum device capacity.
Description	This event is triggered when the volume is over maximum device capacity.

## Device Capacity Threshold Back to Normal

**TABLE 886** Device Capacity Threshold Back to Normal event

Event	Device Capacity Threshold Back to Normal
Event Type	connectedDeviceThresholdBackToNormal
Event Code	964
Severity	Informational
Displayed on the web interface	The device capacity threshold back to normal
Description	This event occurs when the device capacity threshold back to normal.

## Tunnel Events - Access Point (AP)

Following are the events related to tunnel events on access point.

- [Data plane accepted a tunnel request](#) on page 366
- [Data plane rejected a tunnel request](#) on page 367
- [Data plane terminated a tunnel](#) on page 367
- [AP created a tunnel](#) on page 367
- [AP tunnel disconnected](#) on page 367
- [AP softGRE tunnel fails over primary to secondary](#) on page 368
- [AP softGRE tunnel fails over secondary to primary](#) on page 368
- [AP softGRE gateway reachable](#) on page 368
- [AP softGRE gateway not reachable](#) on page 369
- [Data plane set up a tunnel](#) on page 369
- [AP secure gateway association success](#) on page 369
- [AP is disconnected from secure gateway](#) on page 370
- [AP secure gateway association failure](#) on page 370

### NOTE

Event codes 601 to 610 are not applicable for vSZ-H.

## Data plane accepted a tunnel request

**TABLE 887** Data plane accepted a tunnel request event

Event	Data plane accepted a tunnel request
Event Type	dpAcceptTunnelRequest
Event Code	601
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName}   dpKey]} accepted a tunnel request from AP [{apName&&apMac}}.
Description	This event occurs when the data plane accepts a tunnel request from the AP.

## Data plane rejected a tunnel request

**TABLE 888** Data plane rejected a tunnel request event

Event	Data plane rejected a tunnel request
Event Type	dpRejectTunnelRequest
Event Code	602
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxxxxxxxxxx"
Displayed on the web interface	Data plane [{dpName}   dpKey] rejected a tunnel request from AP [{apName}&&apMac] because of reason [{reason]}.
Description	This event occurs when the data plane rejects a tunnel request from the AP.

## Data plane terminated a tunnel

**TABLE 889** Data plane terminated a tunnel event

Event	Data plane terminated a tunnel
Event Type	dpTearDownTunnel
Event Code	603
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx", "reason"="xx"
Displayed on the web interface	Data plane [{dpName}   dpKey] terminated a tunnel from AP [{apName}&&apMac]. Reason: [{reason}]
Description	This event occurs when the data plane terminates a tunnel from the AP.

## AP created a tunnel

**TABLE 890** AP created a tunnel event

Event	AP created a tunnel
Event Type	apBuildTunnelSuccess
Event Code	608
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dpIP"="xxx.xxx.xxx.xxx",
Displayed on the web interface	AP [{apName}&&apMac] created a tunnel to data plane [{dpIP]}.
Description	This event occurs when AP creates a tunnel to the data plane.

## AP tunnel disconnected

**TABLE 891** AP tunnel disconnected event

Event	AP tunnel disconnected
Event Type	apTunnelDisconnected
Event Code	610

## Events Types

### Tunnel Events - Access Point (AP)

**TABLE 891** AP tunnel disconnected event (continued)

Event	AP tunnel disconnected
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dplP"="xxx.xxx.xxx.xxx", "reason"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] disconnected from data plane [{dplP}]. Reason: [{reason}]
Description	This event occurs when AP disconnects from the data plane.

#### NOTE

Event codes 601 to 610 are not applicable for vSZ-H.

## AP softGRE tunnel fails over primary to secondary

**TABLE 892** AP softGRE tunnel fails over primary to secondary event

Event	AP softGRE tunnel fails over primary to secondary
Event Type	apSoftGRE TunnelFailoverPtoS
Event Code	611
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "primaryGRE"="xxx.xxx.xxx.xxx", "secondaryGRE"="xxx.xxx.xxx.xxx "
Displayed on the web interface	AP [{apName&&apMac}] fails over from primaryGRE [{primaryGRE}] to secondaryGRE[{secondaryGRE}].
Description	This event occurs when AP moves from a primary to a secondary GRE.

## AP softGRE tunnel fails over secondary to primary

**TABLE 893** AP softGRE tunnel fails over secondary to primary event

Event	AP softGRE tunnel fails over secondary to primary
Event Type	apSoftGRE TunnelFailoverStoP
Event Code	612
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "primaryGRE"="xxx.xxx.xxx.xxx", "secondaryGRE"="xxxx"
Displayed on the web interface	AP [{apName&&apMac}] fails over from secondaryGRE[{secondaryGRE}] to primaryGRE[{primaryGRE}].
Description	This event occurs when AP moves from a secondary to a primary GRE.

## AP softGRE gateway reachable

**TABLE 894** AP softGRE gateway reachable event

Event	AP softGRE gateway reachable
Event Type	apSoftGREGatewayReachable
Event Code	613
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softgreGW"="xxx.xxx.xxx.xxx", "softgreGWAddress"="xxxx"



**TABLE 894** AP softGRE gateway reachable event (continued)

Event	AP softGRE gateway reachable
Displayed on the web interface	AP [{apname&&apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully
Description	This event occurs when AP builds a soft GRE tunnel successfully.

## AP softGRE gateway not reachable

**TABLE 895** AP softGRE gateway not reachable event

Event	AP softGRE gateway not reachable
Event Type	apSoftGREGatewayNotReachable
Event Code	614
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softGREGatewayList"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}].
Description	This event occurs when AP fails to build a soft GRE tunnel either on the primary or the secondary GRE.
Auto Clearance	This event triggers the alarm 614, which is auto cleared by the event code 613.

## Data plane set up a tunnel

**NOTE**

This event is not applicable for vSZ-H.

**TABLE 896** Data plane set up a tunnel event

Event	Data plane set up a tunnel
Event Type	dpSetUpTunnel
Event Code	627
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName}   {dfpMac}] set up a tunnel from AP [{apName&&apMac}].
Description	This event occurs when the data plane sets up a tunnel from the AP.

## AP secure gateway association success

**TABLE 897** AP secure gateway association success event

Event	AP secure gateway association success
Event Type	ipsecTunnelAssociated
Event Code	660
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is able to reach secure gateway [{ipsecGWAddress}] successfully.

**TABLE 897** AP secure gateway association success event (continued)

Event	AP secure gateway association success
Description	This event occurs when the AP is able to reach the secure gateway successfully.

## AP is disconnected from secure gateway

**TABLE 898** AP is disconnected from secure gateway event

Event	AP is disconnected from secure gateway
Event Type	ipsecTunnelDisassociated
Event Code	661
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is disconnected from secure gateway [{ipsecGWAddress}].
Description	This event occurs when the AP is disconnected from secure gateway.

## AP secure gateway association failure

**TABLE 899** AP secure gateway association failure event

Event	AP secure gateway association failure
Event Type	ipsecTunnelAssociateFailed
Event Code	662
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is unable to establish secure gateway with [{ipsecGWAddress}].
Description	This event occurs when the AP is unable to reach the secure gateway.
Auto Clearance	This event triggers the alarm 662, which is auto cleared by the event code 660.

# Tunnel Events - Data Plane

### NOTE

Events 621 and 626 are not applicable for vSZ-H.

Following are the events related to tunnel events on the data plane:

- [DP sGRE GW unreachable](#) on page 371
- [DP sGRE keep alive timeout](#) on page 371
- [DP sGRE GW inactive](#) on page 371
- [DP DHCPRelay no response](#) on page 372
- [DP DHCPRelay failover](#) on page 372
- [DP sGRE new tunnel](#) on page 372
- [DP sGRE del tunnel](#) on page 373

- [DP sGRE keepalive recovery](#) on page 373
- [DP DHCPRelay response recovery](#) on page 373
- [DP sGRE GW reachable](#) on page 373
- [DP sGRE GW active](#) on page 374
- [DP sGRE GW failover](#) on page 374
- [DP switchover](#) on page 374

## DP sGRE GW unreachable

**TABLE 900** DP sGRE GW unreachable event

Event	DP sGRE GW unreachable
Event Type	dpSgreGWUnreachable
Event Code	615
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x "
Displayed on the web interface	Data plane {{dpName   dpKey}} detected Core Gateway {{GatewayIP}} is unreachable.
Description	This event occurs when the data plane detects that a core network gateway is unreachable.

## DP sGRE keep alive timeout

**TABLE 901** DP sGRE keep alive timeout event

Event	DP sGRE keep alive timeout
Event Type	dpSgreKeepAliveTimeout
Event Code	616
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane {{dpName   dpKey}} detected Keepalive packet to Core Gateway {{GatewayIP}} is lost due to timeout
Description	This event occurs when the data plane detects that a keep alive packet to the core network gateway is lost due to a timeout.

## DP sGRE GW inactive

**TABLE 902** DP sGRE GW inactive event

Event	DP sGRE GW inactive
Event Type	dpSgreGWInact
Event Code	617
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane {{dpName   dpKey}} detected {{GatewayIP}} is inactive because there is no RX traffic

## Events Types

### Tunnel Events - Data Plane

**TABLE 902** DP sGRE GW inactive event (continued)

Event	DP sGRE GW inactive
Description	This event occurs when the data plane detects that a core network gateway is inactive.

## DP DHCPRelay no response

**TABLE 903** DP DHCPRelay no response event

Event	DP DHCPRelay no response
Event Type	dpDhcpRelayNoResp
Event Code	618
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane {{dpName   dpKey}} detected no response from DHCP server {{dhcpIP}} for a while
Description	This event occurs when the data plane does not get a response from the DHCP server.

## DP DHCPRelay failover

**TABLE 904** DP DHCPRelay failover event

Event	DP DHCPRelay failover
Event Type	dpDhcpRelayFailOver
Event Code	619
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "preDhcpIP"="x.x.x.x", "curDhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane {{dpName   dpKey}} detected DHCP server fail-over from {{preDhcpIP}} to {{curDhcpIP}}
Description	This event occurs when the data plane detects a DHCP server relay falls.

## DP sGRE new tunnel

**TABLE 905** DP sGRE new tunnel event

Event	DP sGRE new tunnel
Event Type	dpSgreNewTunnel
Event Code	620
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "greType"="L2oGRE, L3oGRE", "apIpAddress"="x.x.x.x"
Displayed on the web interface	Data plane {{dpName   dpKey}} established a {{greType}} tunnel with AP{{apIP}}.
Description	This event occurs when the data plane establishes a tunnel with AP.

## DP sGRE del tunnel

**TABLE 906** DP sGRE del tunnel event

Event	DP sGRE del tunnel
Event Type	dpSgreDelTunnel
Event Code	621
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "greType"="L2oGRE, L3oGRE", "apIpAddress"="x.x.x.x"
Displayed on the web interface	Dataplane [{dpName}   dpKey] lost a [{greType}] tunnel connection to AP[{apIP}]
Description	This event occurs when access tunnel is disconnected due to a timeout.

## DP sGRE keepalive recovery

**TABLE 907** DP sGRE keepalive recovery event

Event	DP sGRE keepalive recovery
Event Type	dpSgreKeepAliveRecovery
Event Code	622
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName}   dpKey] detected KeepAlive packet to Core Gateway [{gatewayIP}] is now responsive.
Description	The event occurs when the core gateway resumes answering to keepalive.

## DP DHCPRelay response recovery

**TABLE 908** DP DHCPRelay response recovery event

Event	DP DHCPRelay response recovery
Event Type	dpDhcpRelayRespRecovery
Event Code	623
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName}   dpKey] detected DHCP server [{dhcpIP}] is now responsive
Description	This event occurs when the DHCP server resumes answering the relay request from data plane.

## DP sGRE GW reachable

**TABLE 909** DP sGRE GW reachable event

Event	DP sGRE GW reachable
Event Type	dpSgreGWReachable
Event Code	624
Severity	Informational

## Events Types

### Tunnel Events - Data Plane

**TABLE 909** DP sGRE GW reachable event (continued)

Event	DP sGRE GW reachable
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName}   dpKey] detected Core Gateway [{gatewayIP}] is now reachable
Description	This event occurs when the core gateway is reachable.

## DP sGRE GW active

**TABLE 910** DP sGRE GW active event

Event	DP sGRE GW active
Event Type	dpSgreGWAct
Event Code	625
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName}   dpKey] detected [{gatewayIP}] is now active
Description	This event occurs when core gateway changes to an active mode.

## DP sGRE GW failover

**TABLE 911** DP sGRE GW failover event

Event	DP sGRE GW failover
Event Type	dpSgreGWFailOver
Event Code	626
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "preGatewayIP"="x.x.x.x", "curGatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName/dpKey}] switched over from CoreGateway[{preGatewayIP}] to CoreGateway[{curGatewayIP}].
Description	This event occurs when the data plane switches to the other gateway due to failover threshold limit.

## DP switchover

**TABLE 912** DP switchover event

Event	DP switchover
Event Type	dpSwitchover
Event Code	628
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apName"="x", "ip"="x.x.x.x"
Description	This event occurs when the data plane switchover to another cluster.

## AP Ethernet Phy Error Count

**TABLE 913** AP Ethernet Phy Error Count event

Event	AP Ethernet Phy Error Count
Event Type	ethPhyError
Event Code	353
Severity	Informational
Attribute	"apName"="xxxx", "apMac"="xx:xx:xx:xx:xx:xx", "linkDs"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] ethPhyDownShift [{linkDs}]
Description	This event triggers when the ethernet PHY error count is more than the threshold value.

## AP Ethernet PHY Down Shift

**TABLE 914** AP Ethernet PHY Down Shift event

Event	AP Ethernet PHY Down Shift
Event Type	ethPhyDownShift
Event Code	354
Severity	Major
Attribute	"apName"="xxxx", "apMac"="xx:xx:xx:xx:xx:xx", "linkDs"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] ethPhyDownShift [{linkDs}]
Description	This event triggers when the ethernet PHY downshift the link speed.

