

Ruckus SmartZone 300 and Virtual SmartZone-High Scale Alarm and Event Reference Guide

Supporting SmartZone 5.0

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. 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 ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS 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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface.....	21
Document Conventions.....	21
Notes, Cautions, and Warnings.....	21
Command Syntax Conventions.....	22
Document Feedback.....	22
Ruckus Product Documentation Resources.....	22
Online Training Resources.....	23
Contacting Ruckus Customer Services and Support.....	23
What Support Do I Need?.....	23
Open a Case.....	23
Self-Service Resources.....	23
About This Guide.....	25
Introduction.....	25
Terminology.....	25
Revision History.....	29
SmartZone Version 5.0.....	29
Alarms in Release 5.0.....	29
Events in Release 5.0.....	30
SmartZone 3.6.1.....	31
New Alarms in Release 3.6.1.....	31
New Events in Release 3.6.1.....	31
SmartZone Version 3.6.....	32
New Events in Release 3.6.....	32
SmartZone Version 3.5.1.....	32
New Event.....	32
SmartZone Version 3.5.....	32
Deprecated Alarm and Event.....	32
New Alarm.....	33
New Event.....	33
SmartZone Version 3.4.1.....	34
SmartZone Version 3.4.....	35
New Alarm.....	35
Displayed on the Web Interface.....	35
New Event.....	35
SmartZone Version 3.2.1.....	35
New Alarm.....	35
New Event.....	36
Event on Web Interface.....	36
SmartZone Version 3.2.....	36
New Alarm.....	36
Attribute Change.....	37
Renamed Alarm.....	37
New Event.....	37
Severity Change.....	38
Attribute Change.....	38

Renamed Event.....	38
Auto Clearance of Event.....	39
SmartZone Version 3.1.1.....	39
New Alarm.....	39
New Event.....	39
Re-added Event.....	40
Renamed Event.....	40
RuckOS Version 3.1.....	40
New Alarm.....	40
Deprecated Alarm.....	41
Renamed Alarm.....	41
New Event.....	41
Modified Event Severity.....	43
Renamed Event.....	43
RuckOS Version 3.0.....	46
New Alarm.....	46
Deprecated Alarm.....	47
Renamed Alarm Type.....	48
Modification of Alarm Severity.....	48
Renamed Alarm.....	48
New Event.....	49
Deprecated Event.....	51
Re-added Event.....	51
Modifications to Event Severity.....	51
Renamed Event Type.....	52
Renamed Event.....	52
Alarm and Event Management.....	55
Overview.....	55
Alarm and Event Management.....	55
Event Categories.....	55
Event Attributes.....	56
Generation of Alarm and Event.....	56
Alarm Types.....	59
Introduction.....	59
Accounting Alarms.....	59
Accounting server not reachable.....	60
Accounting failed over to secondary.....	60
Accounting fallback to primary.....	60
AP accounting message mandatory parameter missing.....	61
AP accounting message decode failed.....	62
AP account message drop while no accounting start message.....	62
Unauthorized CoA/DM message dropped.....	63
AP Authentication Alarms.....	63
RADIUS server unreachable.....	64
LDAP server unreachable.....	64
AD server unreachable.....	64
WeChat ESP authentication server unreachable.....	65
WeChat ESP authentication server unresolvable.....	65
WeChat ESP DNAT server unreachable.....	66

WeChat ESP DNAT server unresolvable.....	66
AP Communication Alarms.....	67
AP rejected.....	67
AP configuration update failed.....	67
AP swap model mismatched.....	68
AP pre-provision model mismatched.....	68
AP firmware update failed.....	69
AP WLAN oversubscribed.....	69
AP join zone failed.....	69
AP image signing failed.....	70
AP LBS Alarms.....	71
No LS responses.....	71
LS authentication failure.....	72
AP failed to connect to LS.....	72
AP State Change Alarms.....	72
AP rebooted by system.....	73
AP disconnected.....	73
AP deleted.....	73
AP cable modem interface down.....	74
AP DHCP service failure.....	74
AP NAT failure.....	75
AP DHCP/NAT DWPDP Ethernet port configuration override.....	75
SZ DHCP/NAT DWPDP Ethernet port configuration override.....	76
Authentication Alarms.....	76
Authentication server not reachable.....	76
Authentication failed over to secondary.....	77
Authentication fallback to primary.....	77
AD/LDAP connectivity failure.....	78
Bind fails with AD/LDAP.....	78
Bind success with LDAP, but unable to find clear text password for the user.....	79
RADIUS fails to connect to AD NPS server.....	79
RADIUS fails to authenticate with AD NPS server.....	80
Fails to establish TLS tunnel with AD/LDAP.....	80
Control and Data Plane Interface Alarms.....	81
GtpManager (DP) disconnected.....	81
Cluster Alarms.....	81
New node failed to join.....	82
Node removal failed.....	83
Node out of service.....	83
Cluster in maintenance state.....	83
Cluster backup failed.....	84
Cluster restore failed.....	84
Cluster upgrade failed.....	85
Cluster application stopped.....	86
Node bond interface down.....	86
Node physical interface down.....	86
Cluster node rebooted.....	87
Cluster node shut down.....	87
Disk usage exceed threshold.....	88
Cluster out of service.....	88

Cluster upload AP firmware failed.....	89
Cluster add AP firmware failed.....	89
Unsync NTP time.....	89
Cluster upload KSP file failed.....	90
Configuration backup failed.....	90
Configuration restore failed.....	90
AP certificate updated.....	91
Upgrade SS table failed.....	91
Cluster redundancy sync configuration failed.....	91
Cluster redundancy restoring configuration failed.....	92
Not all APs rehome after timeout.....	92
Configuration Alarms.....	93
Zone configuration preparation failed.....	93
AP configuration generation failed.....	93
End-of-life AP model detected.....	94
VLAN configuration mismatch on non DHCP/NAT WLAN.....	94
VLAN configuration mismatch on DHCP/NAT WLAN.....	95
Data Plane Alarms.....	95
Data plane configuration update failed.....	96
Data plane disconnected.....	96
Data plane physical interface down.....	96
Data plane rebooted.....	97
Data plane packet pool is under low water mark.....	97
Data plane packet pool is under critical low water mark.....	98
Data plane core dead.....	98
Data plane process restarted.....	98
Data plane license is not enough.....	99
Data plane upgrade failed.....	99
Data plane of data center side fails to connect to the CALEA server.....	100
Data plane fails to connects to the other data plane.....	100
Data plane DHCP IP pool usage rate is 100 percent.....	101
Gn/S2a Interface Alarms.....	101
GGSN restarted.....	102
GGSN not reachable.....	102
GGSN not resolved.....	102
PDNGW could not be resolved.....	103
PDNGW version not supported.....	103
Associated PDNGW down.....	104
Create session response failed.....	104
Decode failed.....	105
Modify bearer response failed.....	105
Delete session response failed.....	106
Delete bearer request failed.....	106
Update bearer request failed.....	106
CGF server not configured.....	107
GR Interface Alarms.....	107
Destination not reachable.....	108
App server down.....	108
App server inactive.....	109
Association establishment failed.....	109

Association down.....	109
Outbound routing failure.....	110
Did allocation failure.....	110
IPMI Alarms.....	111
ipmiVoltage.....	112
ipmiThempBB.....	113
ipmiThempFP.....	113
ipmiThempIOH.....	114
ipmiThempMemP.....	114
ipmiThempPS.....	115
ipmiThempP.....	115
ipmiThempHSBP.....	115
ipmiFan.....	116
ipmiPower.....	116
ipmiCurrent.....	117
ipmiFanStatus.....	117
ipmiPsStatus.....	117
ipmiDrvStatus.....	118
Licensing Alarms.....	118
TTG session critical threshold.....	119
TTG session license exhausted.....	119
License going to expire.....	119
Insufficient license capacity.....	120
Data plane DHCP IP license insufficient.....	120
Data plane NAT session license insufficient.....	121
PMIPv6 Alarms.....	121
Config update failed.....	121
DHCP connection lost.....	122
SCI Alarms.....	122
Connect to SCI failure.....	122
SCI has been disabled.....	123
SCI and FTP have been disabled.....	123
Session Alarms.....	124
Binding failed.....	124
System Alarms.....	124
No LS responses.....	125
LS authentication failure.....	125
{produce.short.name} failed to connect to LS.....	126
Syslog server unreachable.....	126
CSV export FTP maximum retry.....	127
CSV export disk threshold exceeded.....	127
CSV export disk max capacity reached.....	127
Process restart.....	128
Service unavailable.....	128
Keepalive failure.....	128
Resource unavailable.....	129
Unconfirmed program detection.....	129
Diameter peer transport failure.....	130
Diameter CER error.....	130
Process initiated.....	131

PMIPv6 unavailable.....	131
Memory allocation failed.....	132
The last one data plane is disconnected zone affinity profile alarm.....	132
Threshold Alarms.....	133
CPU threshold exceeded.....	133
Memory threshold exceeded.....	133
Disk usage threshold exceeded.....	134
The drop of client count threshold exceeded.....	134
License threshold exceeded.....	135
Rate limit for TOR surpassed.....	135
The number of users exceeded its limit.....	136
The number of devices exceeded its limit.....	136
Tunnel Alarms - Access Point.....	136
AP softGRE gateway not reachable.....	137
AP is disconnected from secure gateway.....	137
AP secure gateway association failure.....	137
Events Types.....	139
3rd Party Access Point Events.....	139
3rd party AP connected.....	139
Accounting Events.....	140
Accounting session disabled.....	140
Accounting server not reachable.....	141
Accounting failed over to secondary.....	141
Accounting fallback to primary.....	142
AP accounting message mandatory parameter missing.....	142
Unknown realm.....	142
AP accounting message decode failed.....	143
AP accounting retransmission message dropped.....	143
AP accounting response while invalid config.....	144
AP account message drop while no accounting start message.....	144
Unauthorized COA/DM message dropped.....	145
AP Authentication Events.....	145
Radius server reachable.....	146
Radius server unreachable.....	146
LDAP server reachable.....	146
LDAP server unreachable.....	147
AD server reachable.....	147
AD server unreachable.....	147
Wechat ESP authentication server reachable.....	148
WeChat ESP authentication server unreachable.....	148
WeChat ESP authentication server resolvable.....	148
WeChat ESP authentication server unresolvable.....	149
WeChat ESP DNAT server reachable.....	149
WeChat ESP DNAT server unreachable.....	149
WeChat ESP DNAT server resolvable.....	150
WeChat ESP DNAT server unresolvable.....	150
AP Communication Events.....	150
AP discovery succeeded.....	151
AP managed.....	151
AP rejected.....	152

AP firmware updated.....	152
AP firmware update failed.....	152
Updating AP firmware.....	153
Updating AP configuration.....	153
AP configuration updated.....	153
AP configuration update failed.....	153
AP pre-provision model mismatched.....	154
AP swap model mismatched.....	154
AP WLAN oversubscribed.....	154
AP join zone failed.....	155
AP illegal to change country code.....	155
AP configuration get failed.....	155
Rogue AP.....	156
SSID-spoofing rogue AP.....	156
MAC-spoofing rogue AP.....	156
Same-network rogue AP.....	157
Ad-hoc network device.....	157
Rogue AP disappeared.....	157
Classified Rogue AP.....	158
AP image signing failed.....	158
AP LBS Events.....	158
No LS responses.....	159
LS authentication failure.....	159
AP connected to LS.....	159
AP failed to connect to LS.....	159
AP started location service.....	160
AP stopped location service.....	160
AP received passive calibration request.....	160
AP received passive footfall request.....	161
AP received unrecognized request.....	161
AP Mesh Events.....	161
EMAP downlink connected to MAP.....	162
EMAP downlink disconnected from MAP.....	162
EMAP uplink connected to MAP.....	163
EMAP uplink disconnected from MAP.....	163
MAP disconnected.....	163
MAP downlink connected.....	163
MAP downlink connected to EMAP.....	164
MAP downlink disconnected from EMAP.....	164
RAP downlink connected to MAP.....	164
MAP uplink connected to EMAP.....	165
MAP uplink disconnected from EMAP.....	165
MAP uplink connected to RAP.....	165
MAP uplink connected to MAP.....	166
Mesh state updated to MAP.....	166
Mesh state updated to MAP no channel.....	166
Mesh state updated to RAP.....	167
Mesh state update to RAP no channel.....	167
MAP downlink connected to MAP.....	167
MAP downlink disconnected from MAP.....	167

RAP downlink disconnected from MAP.....	168
AP State Change Events.....	168
AP rebooted by user.....	169
AP rebooted by system.....	169
AP disconnected.....	169
AP IP address updated.....	170
AP reset to factory default.....	170
AP channel updated.....	170
AP country code updated.....	171
AP channel updated because dynamic frequency selection (DFS) detected a radar.....	171
AP change control plane.....	171
AP connected.....	172
AP deleted.....	172
AP heartbeat lost.....	172
AP tagged as critical.....	173
AP cable modem interface down.....	173
AP brownout.....	173
AP cable modem power-cycled by user.....	173
AP smart monitor turn off WLAN.....	174
AP client load balancing limit reached.....	174
AP client load balancing limit recovered.....	174
AP WLAN state changed.....	175
AP capacity reached.....	175
AP capacity recovered.....	175
AP cable modem interface up.....	176
AP cable modem soft-rebooted by user.....	176
AP cable modem set to factory default by user.....	176
AP health high latency flag.....	177
AP health low capacity flag.....	177
AP health high connection failure flag.....	177
AP health high client count flag.....	178
AP health high latency clear.....	178
AP health low capacity clear.....	178
AP health high connection failure clear.....	179
AP health high client count clear.....	179
Primary DHCP AP is down.....	179
Primary DHCP AP is up.....	180
Secondary DHCP AP is down.....	180
Secondary DHCP AP is up.....	180
Primary or secondary DHCP AP detects 90% of the configured total IPs.....	181
Both primary and secondary DHCP server APs are down.....	181
AP NAT gateway IP failover detected for particular VLAN pool.....	181
AP NAT gateway IP fall back detected for particular VLAN pool.....	182
NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for pa	182
NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP v	182
AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down.....	183
AP health high airtime utilization flag.....	183
AP health high airtime utilization clear.....	184

AP cluster failover.....	184
AP cluster rehome.....	184
AP USB Events.....	185
AP USB software package downloaded.....	185
AP USB software package download failed.....	185
Authentication Events.....	185
Authentication server not reachable.....	186
Unknown realm.....	186
Authentication succeeded.....	187
Authentication failed.....	187
Pseudonym authentication succeeded.....	187
Pseudonym authentication failed.....	188
Fast re-authentication succeeded.....	188
Fast re-authentication failed.....	189
Authentication failed over to secondary.....	189
Authentication fallback to primary.....	190
AD/LDAP connected successfully.....	190
AD/LDAP connectivity failure.....	190
Bind fails with AD/LDAP.....	191
Bind success with LDAP, but unable to find clear text password for the user.....	191
RADIUS fails to connect to AD NPS server.....	191
RADIUS fails to authenticate with AD NPS server.....	192
Successfully established the TLS tunnel with AD/LDAP.....	192
Fails to establish TLS tunnel with AD/LDAP.....	192
Authorization Events.....	193
DM received from AAA.....	193
DM NACK sent to AAA.....	193
DM sent to NAS.....	194
DM NACK received from NAS.....	194
CoA received from AAA.....	194
CoA NACK sent to AAA.....	195
CoA sent NAS.....	195
CoA NAK received NAS.....	195
CoA authorize only access reject.....	196
CoA RWSG MWSG notification failure.....	196
Control and Data Plane Interface.....	197
DP connected.....	197
GtpManager (DP) disconnected.....	197
Session updated at DP.....	198
Session update at DP failed.....	198
Session deleted at DP.....	198
Session delete at DP failed.....	199
C2d configuration failed.....	199
Client Events.....	200
Client authentication failed.....	201
Client joined.....	201
Client failed to join.....	201
Client disconnected.....	202
Client connection timed out.....	202
Client authorization successfully.....	203

Client authorization failed.....	203
Client session expired.....	203
Client roaming.....	204
Client logged out.....	204
3rd party client join	204
3rd party client inactivity timeout	205
3rd party client authorization	205
3rd party client authorization failure	205
3rd party client session expiration	206
3rd party client roaming	206
3rd party client session logout	207
Client roaming disconnected.....	207
Client blocked	207
Client grace period	208
Onboarding registration succeeded	208
Onboarding registration failed	208
Remediation succeeded	209
Remediation failed	209
Force DHCP disconnected	209
WDS device joined	210
WDS device left.....	210
Client is blocked because of barring UE rule.....	210
Client is unblocked by barring UE rule.....	211
Start CALEA mirroring client.....	211
Stop CALEA mirroring client.....	211
Wired client joined.....	212
Wired client failed to join.....	212
Wired client disconnected.....	212
Wired client authorization successfully.....	213
Wired client session expired.....	213
Application identified.....	213
Application denied.....	214
URL filtering server unreachable.....	214
URL filtering server reachable.....	214
Cluster Events.....	215
Cluster created successfully.....	215
New node joined successfully.....	216
New node failed to join.....	216
Node removal completed.....	216
Node removal failed.....	217
Node out of service.....	217
Cluster in maintenance state.....	217
Cluster back in service.....	218
Cluster backup completed.....	218
Cluster backup failed.....	218
Cluster restore completed.....	219
Cluster restore failed.....	219
Cluster node upgrade completed.....	219
Entire cluster upgraded successfully.....	220
Cluster upgrade failed.....	220

Cluster application stopped.....	220
Cluster application started.....	221
Cluster backup started.....	221
Cluster upgrade started.....	221
Cluster leader changed.....	221
Node bond interface down.....	222
Node bond interface up.....	222
Node IP address changed.....	222
Node physical interface down.....	223
Node physical interface up.....	223
Cluster node rebooted.....	223
NTP time synchronized.....	224
Cluster node shutdown.....	224
Cluster upload started.....	224
Cluster upload completed.....	225
Cluster upload failed.....	225
SSH tunnel switched.....	225
Cluster remove node started.....	225
Node back in service.....	226
Disk usage exceed threshold.....	226
Cluster out of service.....	226
Initiated moving APs in node to a new cluster.....	227
Cluster upload vSZ-D firmware started.....	227
Cluster upload vSZ-D firmware completed.....	227
Cluster upload vSZ-D firmware failed.....	228
Cluster upload AP firmware started.....	228
Cluster upload AP firmware completed.....	228
Cluster upload AP firmware failed.....	229
Cluster add AP firmware started.....	229
Cluster add AP firmware completed.....	229
Cluster add AP firmware failed.....	229
Cluster name is changed.....	230
Unsync NTP Time.....	230
Cluster upload KSP file started.....	230
Cluster upload KSP file completed.....	231
Cluster upload KSP file failed.....	231
Configuration backup started.....	231
Configuration backup succeeded.....	232
Configuration backup failed.....	232
Configuration restore succeeded.....	232
Configuration restore failed.....	233
AP Certificate Expired.....	233
AP Certificate Updated.....	233
Configuration restore started.....	234
Upgrade SSTable failed.....	234
Reindex elastic search finished.....	234
Initiated APs contact APR.....	234
All nodes back in service.....	235
Not management service ready.....	235
Management service ready.....	235

Configuration sync failed.....	236
Node IPv6 address added.....	236
Node IPv6 address deleted.....	236
Configuration Events.....	236
Configuration updated.....	237
Configuration update failed.....	237
Configuration receive failed.....	238
Incorrect flat file configuration.....	238
Zone configuration preparation failed.....	238
AP configuration generation failed.....	239
End-of-life AP model detected.....	239
VLAN configuration mismatch on non-DHCP/NAT WLAN.....	239
VLAN configuration mismatch on DHCP/NAT WLAN.....	240
Generation failed during CCM GPB generation	240
Preparation failed during AP knowledge generation.....	240
Generation failed during AP knowledge generation.....	241
End-of-life AP model detected during AP knowledge generation.....	241
Notification failed during AP knowledge generation.....	241
Data Plane Events.....	242
Data plane discovered.....	242
Data plane discovery failed.....	243
Data plane configuration updated.....	243
Data plane configuration update failed.....	243
Data plane rebooted.....	244
Data plane heartbeat lost.....	244
Data plane IP address updated.....	244
Data plane updated to a new control plane.....	244
Data plane status update failed.....	245
Data plane statistics update failed.....	245
Data plane connected.....	245
Data plane disconnected.....	246
Data plane physical interface down.....	246
Data plane physical interface up.....	246
Data plane packet pool is under low water mark.....	247
Data plane packet pool is under critical low water mark.....	247
Data plane packet pool is above high water mark.....	247
Data plane core dead.....	248
Data plane process restarted.....	248
Data plane discovery succeeded.....	248
Data plane managed.....	249
Data plane deleted.....	249
Data plane license is not enough.....	249
Data plane upgrade started.....	250
Data plane upgrading.....	250
Data plane upgrade succeeded.....	250
Data plane upgrade failed.....	250
Data plane of data center side successfully connects to the CALEA server.....	251
Data plane of data center side fails to connect to the CALEA server.....	251
Data Plane of data center side disconnects to CALEA server.....	252
Data plane successfully connects to the other data plane.....	252

Data plane fails to connect to the other data plane.....	252
Data plane disconnects to the other data plane.....	253
Start CALEA mirroring client in data plane.....	253
Stop CALEA mirroring client in data plane.....	253
Data plane DHCP IP pool usage rate is 100 percent.....	254
Data plane DHCP IP pool usage rate is 80 percent.....	254
Data plane NAT session capacity usage rate is 80 percent.....	255
Data plane NAT session capacity usage rate is 100 percent.....	255
Data plane DHCP IP capacity usage rate is 80 percent.....	255
Data plane DHCP IP capacity usage rate is 100 percent.....	256
DHCP Events.....	256
DHCP inform received.....	256
DHCP dcln received.....	257
GA Interface Events.....	257
CGF keepalive not responded	257
CDR transfer succeeded.....	258
Gn/S2a Interface Events.....	258
GGSN restarted.....	259
GGSN not reachable.....	259
Echo response not received.....	259
GGSN not resolved.....	260
PDP context established.....	260
PDP create failed.....	260
PDP update by HLR succeeded.....	261
PDP update by HLR failed.....	261
PDP update by roaming succeeded.....	261
PDP update by roaming failed.....	262
PDP update by GGSN succeeded.....	262
PDP update by GGSN failed.....	262
PDP delete by TTG succeeded.....	263
PDP delete by TTG failed.....	263
PDP delete by GGSN succeeded.....	264
PDP delete by GGSN failed.....	264
IP assigned.....	264
IP not assigned.....	265
Unknown UE.....	265
PDP update success COA.....	265
PDP update fail COA.....	266
PDNGW could not be resolved.....	266
PDNGW version not supported.....	266
Associated PDNGW down.....	267
Create session response failed.....	267
Decode failed.....	268
Modify bearer response failed.....	268
Delete session response failed.....	268
Delete bearer request failed.....	269
Update bearer request failed.....	269
CGF server not configured.....	269
Gr Interface Event.....	270
Destination not reachable.....	270

Destination available.....	271
App server down.....	271
App server inactive.....	271
App server active.....	272
Association establishment failed.....	272
Association down.....	273
Association up.....	273
Send auth info success.....	273
Auth info sending failed.....	274
GPRS location update succeeded.....	274
GPRS location update failed.....	274
Insert sub data success.....	275
Insert sub data failed.....	275
Outbound routing failure.....	275
Did allocation failure.....	276
Restore data success.....	276
Restore data failed.....	276
IPMI Events.....	277
ipmiVoltage.....	277
ipmiThempBB.....	277
ipmiThempFP.....	278
ipmiThempIOH.....	278
ipmiThempMemP.....	279
ipmiThempPS.....	279
ipmiThempP.....	279
ipmiThempHSBP.....	280
ipmiFan.....	280
ipmiPower.....	280
ipmiCurrent.....	281
ipmiFanStatus.....	281
ipmiPsStatus.....	281
ipmiDrvStatus.....	282
ipmiREVotage.....	282
ipmiREThempBB.....	282
ipmiREThempFP.....	283
ipmiREThempIOH.....	283
ipmiREThempMemP.....	283
ipmiREThempPS.....	283
ipmiREThempP.....	284
ipmiREThempHSBP.....	284
ipmiREFan.....	284
ipmiREPower.....	285
ipmiRECurrent.....	285
ipmiREFanStatus.....	285
ipmiREPsStatus.....	286
ipmiREDrvStatus.....	286
Licensing Interface Events.....	286
TTG session warning threshold.....	287
TTG session major threshold.....	287
TTG session critical threshold.....	287

TTG session license exhausted.....	288
License sync succeeded.....	288
License sync failed.....	288
License import succeeded.....	289
License import failed.....	289
License data changed.....	289
License going to expire.....	290
Insufficient license capacity.....	290
Data plane DHCP IP license insufficient.....	290
Data plane NAT session license insufficient.....	291
AP number limit exceeded.....	291
Insufficient license capacity.....	291
Location Delivery Events.....	292
Unavailable location info requested.....	292
Incapable location info requested.....	292
Unsupported location delivery request.....	293
PMIPv6 Events.....	293
Config update failed.....	293
LMA ICMP reachable.....	294
LMA server unreachable.....	294
DHCP connected.....	294
DHCP connection lost.....	294
SCI Events.....	295
Connect to SCI.....	295
Disconnect to SCI.....	295
Connect to SCI failure.....	296
SCI has been disabled.....	296
SCI and FTP have been disabled.....	296
Session Events.....	297
Session timeout.....	297
Delete all sessions.....	297
Binding succeeded.....	298
Binding failed.....	298
Binding time expired.....	299
Binding revoked.....	299
Binding released.....	299
STA Interface Events.....	300
STA successful authentication.....	300
STA session termination {produce.short.name} initiated success.....	300
STA session termination AAA initiated success.....	301
STA session termination AAA initiated failed.....	301
STA re-authorization successful.....	302
System Events.....	302
No LS responses.....	303
LS authentication failure.....	303
{produce.short.name} connected to LS.....	304
{produce.short.name} failed to connect to LS.....	304
{produce.short.name} received passive request.....	304
{produce.short.name} sent controller information report.....	305
{produce.short.name} received management request.....	305

{produce.short.name} sent AP info by venue report.....	305
{produce.short.name} sent query venues report.....	305
{produce.short.name} sent associated client report.....	306
{produce.short.name} forwarded calibration request to AP.....	306
{produce.short.name} forwarded footfall request to AP.....	306
{produce.short.name} received unrecognized request.....	307
Syslog server reachable.....	307
Syslog server unreachable.....	307
Syslog server switched.....	308
Generate AP config for plane load rebalance succeeded.....	308
Generate AP config for plane load rebalance failed.....	308
FTP transfer.....	309
FTP transfer error.....	309
CSV export FTP transfer.....	309
CSV export FTP transfer error.....	310
CSV export FTP transfer maximum retry.....	310
CSV export disk threshold exceeded.....	310
CSV export disk max capacity reached.....	311
CSV export disk threshold back to normal.....	311
File upload.....	311
Email sent successfully.....	311
Email sent failed.....	312
SMS sent successfully.....	312
SMS sent failed.....	312
Process restart.....	313
Service unavailable.....	313
Keepalive failure.....	313
Resource unavailable.....	314
HIP started.....	314
HIP stopped.....	314
Standby HIP restarted.....	315
HIP cache cleaned.....	315
All data planes in the zone affinity profile are disconnected.....	316
CALEA UE Matched.....	316
Diameter peer transport failure.....	316
Diameter CER error.....	317
Diameter CER success.....	317
Diameter invalid version.....	318
Diameter peer add successful.....	318
ZD AP migrating.....	318
ZD AP migrated.....	319
ZD AP rejected.....	319
ZD AP migration failed.....	319
Database error.....	320
Recover cassandra error.....	320
Process initiated.....	320
PMIPv6 unavailable.....	321
Memory allocation failed.....	321
Process stopped.....	321
Password expiration.....	322

Admin account logout.....	322
Admin session expired.....	322
Disable inactive admins.....	323
Two factor auth failed.....	323
Switch Events.....	323
Switch critical message.....	324
Switch alert message.....	324
Switch warning message.....	324
Threshold Events.....	324
CPU threshold exceeded.....	325
Memory threshold exceeded.....	325
Disk usage threshold exceeded.....	326
CPU threshold back to normal.....	326
Memory threshold back to normal.....	326
Disk threshold back to normal.....	326
License threshold exceeded.....	327
The drop of client count threshold exceeded.....	327
Rate limit threshold surpassed.....	327
Rate limit threshold restored.....	328
Rate limit for TOR surpassed.....	328
The number of users exceed its limit.....	329
The number of devices exceeded its limit.....	329
Tunnel Events - Access Point (AP).....	329
Data plane accepted a tunnel request.....	330
Data plane rejected a tunnel request.....	330
Data plane terminated a tunnel.....	331
AP created a tunnel.....	331
AP tunnel disconnected.....	331
AP softGRE tunnel fails over primary to secondary.....	332
AP softGRE tunnel fails over secondary to primary.....	332
AP softGRE gateway reachable.....	332
AP softGRE gateway not reachable.....	332
Data plane set up a tunnel.....	333
AP secure gateway association success.....	333
AP is disconnected from secure gateway.....	333
AP secure gateway association failure.....	334
Tunnel Events - Data Plane.....	334
DP sGRE GW unreachable.....	335
DP sGRE keep alive timeout.....	335
DP sGRE GW inactive.....	335
DP DHCPRelay no response.....	336
DP DHCPRelay failover.....	336
DP sGRE new tunnel.....	336
DP sGRE del tunnel.....	336
DP sGRE keepalive recovery.....	337
DP DHCPRelay response recovery.....	337
DP sGRE GW reachable.....	337
DP sGRE GW active.....	338
DP sGRE GW failover.....	338

Preface

- Document Conventions..... 21
- Command Syntax Conventions..... 22
- Document Feedback..... 22
- Ruckus Product Documentation Resources..... 22
- Online Training Resources..... 23
- Contacting Ruckus Customer Services and Support..... 23

Document Conventions

The following tables list the text and notice 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>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>Ruckus Small Cell Release Notes</i> for more information

Notes, Cautions, and 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.



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
bold text	Identifies command names, keywords, and command options.
<i>italic</i> text	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[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: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
 - Ruckus Small Cell Alarms Guide SC Release 1.3
 - Part number: 800-71306-001
 - Page 88

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 documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into 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 Ruckus 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 Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the 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. Request 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, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.

Self-Service Resources

The Support Portal at <https://support.ruckuswireless.com/contact-us> 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>

Preface

Contacting Ruckus Customer Services and Support

- [Software Downloads and Release Notes](https://support.ruckuswireless.com/software)—<https://support.ruckuswireless.com/software>
- [Security Bulletins](https://support.ruckuswireless.com/security)—<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

About This Guide

- Introduction..... 25
- Terminology..... 25

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>.

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
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

TABLE 2 Terms used (continued)

Term	Description
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
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

TABLE 2 Terms used (continued)

Term	Description
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)
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
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

TABLE 2 Terms used (continued)

Term	Description
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

Revision History

- SmartZone Version 5.0..... 29
- SmartZone 3.6.1..... 31
- SmartZone Version 3.6..... 32
- SmartZone Version 3.5.1..... 32
- SmartZone Version 3.5..... 32
- SmartZone Version 3.4.1..... 34
- SmartZone Version 3.4..... 35
- SmartZone Version 3.2.1..... 35
- SmartZone Version 3.2..... 36
- SmartZone Version 3.1.1..... 39
- RuckOS Version 3.1..... 40
- RuckOS Version 3.0..... 46

SmartZone Version 5.0

Alarms in Release 5.0

TABLE 3 Alarms added in release 5.0

Alarm Code	Alarm
868	upgradeSSTableFailed
874	clusterRedundancySyncCfgFailed
877	clusterRedundantRestoreCfgFailed
881	clusterRedundancyApRehomeIncomplete
1019	Unconfirmed Program Detection
1026	apCfgDhcpNatDwpdEthPortConfigOverride
1027	sZCfgDhcpNatManualEthPortConfigOverride
1277	dpDhcpIpLicenseNotEnough
1278	dpNatSessionLicenseNotEnough

TABLE 4 Deprecated alarms in release 5.0

Alarm Code	Alarm
1016	hipFailover
1401	diaInitializeErr
1407	diaPeerAddError
1409	diaPeerRemoveSuccess
1410	diaRealmEntryErr
1411	diaFailOverToAltPeer
1412	diaFailbackToPeer
1414	diaCEAUnknownPeer

TABLE 4 Deprecated alarms in release 5.0 (continued)

Alarm Code	Alarm
1415	diaNoCommonApp
1551	staAuthFailedTransDown
1552	staAuthFailedFailureResp
1553	staAuthFailedDecodeFailure
1558	staReAuthFailed
1559	staResponseTimerExpired
1560	retransmitExhausted
1610	cnxnToCgfFailed
1614	cdrTxfrFailed
1615	cdrGenerationFailed
5006	lmalcmpUnreachable
5008	lmaFailOver
5010	bindingFailure

Events in Release 5.0

TABLE 5 Events added in release 5.0

Event Code	Event
1277	dpDhcpIpLicenseNotEnough
1278	dpNatSessionLicenseNotEnough
1283	dpNatSessionCapacityUsageRate80
1284	dpNatSessionCapacityUsageRate100
1285	dpDhcpIpCapacityUsageRate80
1286	dpDhcpIpCapacityUsageRate100
1287	dpDhcpIpLicenseRemoved
1288	dpNatSessionLicenseRemoved
8012	AdminSessionExpired
8013	DisableInactiveAdmins
8014	TwoFactorAuthFailed
20000	SwitchCriticalMessage
20001	SwitchAlertMessage
20002	SwitchWarningMessage

TABLE 6 Deprecated events in release 5.0

Event Code	Event
1016	hipFailover
1232	accSessStarted
1233	accSessStartFailed
1246	accSessStopSucc
1247	accSessStopFail
1248	accSessInterimFail

TABLE 6 Deprecated events in release 5.0 (continued)

Event Code	Event
1401	diaNitalizeErr
1402	diaInitialization
1407	diaPeerAddError
1409	diaPeerRemoveSuccess
1410	diaRealmEntryErr
1411	diaFailOverToAltPeer
1412	diaFailbackToPeer
1414	diaCEAUnknownPeer
1415	diaNoCommonApp
1551	staAuthFailedTransDown
1552	staAuthFailedFailureResp
1553	staAuthFailedDecodeFailure
1558	staReAuthFailed
1559	staResponseTimerExpired
1560	retransmitExhausted
1610	cnxnToCgffFailed
1614	cdrTxfrFailed
1615	cdrGenerationFailed
5006	lmalcmpUnreachable
5008	lmaFailOver
5010	bindingFailure

SmartZone 3.6.1

New Alarms in Release 3.6.1

Alarm Code	Alarm
956	clientCountDropThresholdExceeded

New Events in Release 3.6.1

Event Code	Event
956	clientCountDropThresholdExceeded
1280	apConnectionTerminatedDueToInsufficientLicense
1281	urlFilteringLicenseInsufficient
8010	passwordExpiration
8011	adminAccountLockout

SmartZone Version 3.6

New Events in Release 3.6

Event Code	Event
186	generalRogueAPDetected
187	apSigningInformation
349	apClusterFailover
350	apRehomeFailover
872	allServiceOutOfService
873	allServiceInService
874	clusterRedundancySyncCfgFailed
8001	application of user is identified
8002	application of user is denied
8003	urlFilteringServerUnreachable
8004	urlFilteringServerReachable

SmartZone Version 3.5.1

The following are the changes for version 3.5.1.

New Event

Event Code	Event
2802	wiredClientJoin
2803	wiredClientJoinFailure
2804	wiredClientDisconnect
2806	wiredClientAuthorization
2808	wiredClientSessionExpiration

SmartZone Version 3.5

The following are the changes for version 3.5.

Deprecated Alarm and Event

Code	Type	Replace With
Alarm 835 and Event 837	resyncNTPTIME	Alarm and Event 855 - unsyncNTPTIME

New Alarm

Alarm Code	Alarm
341	apDHCPServiceFailure
346	apNATFailureDetectedbySZ NOTE Description for Alarm 346 is changed.
855	unsyncNTPTime
858	clusterUploadKspFileFailed
974	csvFtpTransferMaxRetryReached
975	csvDiskThresholdExceeded
976	csvDiskMaxCapacityReached
1024	apCfgNonDhcpNatWlanVlanConfigMismatch
1025	apCfgDhcpNatWlanVlanConfigMismatch
1258	dpDcToCaleaConnectFail
1261	dpP2PTunnelConnectFail
1265	dpDhcpIpPoolUsageRate100
1267	zoneAffinityLastDpDisconnected
1762	racADLDAPTLSFailed
4003	disabledSciDueToUpgrade
4005	diabledSciAndFtpDueToMutuallyExclusive

New Event

Event Code	Event
117	apGetConfigFailed
228	clientBlockByBarringUERule
229	clientUnBlockByBarringUERule
328	apHealthLatencyFlag
329	apHealthCapacityFlag
330	apHealthConnectionFailureFlag
331	apHealthClientCountFlag
333	apHealthCapacityFlag
334	apHealthConnectionFailureClear
335	apHealthClientCountClear
336	apDHCPFailoverDetected
337	apDHCPFallbackDetected
338	apSecondaryDHCPAPDown
339	apSecondaryDHCPAPUp
340	apDHCIPIPPoolMaxThresholdReached
341	apDHCPServiceFailure
342	apNATFailoverDetected

Revision History

SmartZone Version 3.4.1

Event Code	Event
343	apNATFallbackDetected
344	apNATVlanCapacityAffected
345	apNATVlanCapacityRestored
346	apNATFailureDetectedbySZ
347	apHealthAirUtilizationFlag
348	apHealthAirUtilizationClear
855	unsyncNTPTime
869	Reindex ElasticSearch finished
870	clusterInitContactApr
972	csvFtpTransfer
973	csvFtpTransferError
974	csvFtpTransferMaxRetryReached
975	csvDiskThresholdExceeded
976	csvDiskMaxCapacityReached
977	csvDiskThresholdBackToNormal
1024	apCfgNonDhcpNatWlanVlanConfigMismatch
1025	apCfgDhcpNatWlanVlanConfigMismatch
1257	dpDcToCaleaConnected
1258	dpDcToCaleaConnectFail
1259	dpDcToCaleaDisconnected
1260	dpP2PTunnelConnected
1261	dpP2PTunnelConnectFail
1262	dpP2PTunnelDisconnected
1263	dpStartMirroringClient
1264	dpStopMirroringClient
1265	dpDhcpIpPoolUsageRate100
1266	dpDhcpIpPoolUsageRate80
1267	zoneAffinityLastDpDisconnected
1268	dpCaleaUeInterimMatched
1761	racADLDAPTLSSuccess
1762	racADLDAPTLSTFailed
4001	connectedToSci
4002	disconnectedFromSci
4003	disabledSciDueToUpgrade
4004	disabledSciDueToUpgrade
4005	disabledSciAndFtpDueToMutuallyExclusive

SmartZone Version 3.4.1

No changes in this release.

SmartZone Version 3.4

The following are the changes for version 3.4.

New Alarm

Alarm Code	Alarm
850	clusterUploadAPFirmwareFailed
853	clusterAddAPFirmwareFailed
1021	zoneCfgPrepareFailed
1022	apCfgGenFailed
1023	cfgGenSkippedDueToEolAp

Displayed on the Web Interface

Alarm Code	Attribute	Attribute Change
107	Added failure reason	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}] failure reason [{reason}]

New Event

Event Code	Event
848	clusterUploadAPFirmwareStart
849	clusterUploadAPFirmwareSuccess
850	clusterUploadAPFirmwareFailed
851	clusterAddAPFirmwareStart
852	clusterAddAPFirmwareSuccess
853	clusterAddAPFirmwareFailed
854	clusterNameChanged
1021	zoneCfgPrepareFailed
1022	apCfgGenFailed
1023	cfgGenSkippedDueToEolAp

SmartZone Version 3.2.1

The following are the changes for version 3.2.1.

New Alarm

Alarm Code	Alarm
865	apCertificateExpire

New Event

Event Code	Event
226	wdsDeviceJoin
227	wdsDeviceLeave
865	apCertificateExpire
866	apCertificateExpireClear
3011	recoverCassandraError

Event on Web Interface

Event Code	Existing Display	New Display
513	Data plane [{dpName&&dpKey}] disconnected from {produce.short.name} [{cpName} wsgIP].	Data plane [{dpName&&dpKey}] disconnected from {produce.short.name} [{cpName} wsgIP], Reason: [{reason}].

SmartZone Version 3.2

The following are the changes for version 3.2.

New Alarm

Alarm Code	Alarm
538	dpLicenseInsufficient
553	dpUpgradeFailed
751	syslogServerUnreachable
835	resyncNTPTime
1255	licenseGoingToExpire
1256	apConnectionTerminatedDueToInsufficientLicense
1752	racADLDAPFail
1753	racADLDAPBindFail
1754	racLDAPFailToFindPassword
1755	racADNPSFail
1756	racADNPSFailToAuthenticate
2102	radiusServerUnreachable
2122	ldapServerUnreachable
2142	adServerUnreachable
2152	espAuthServerUnreachable
2154	espAuthServerUnResolvable
2162	espDNATServerUnreachable
2164	espDNATServerUnresolvable

Attribute Change

Module	Attribute	Attribute Change
Data Plane	dpMac	dpKey

Renamed Alarm

Alarm Code	Alarm Name	Renamed To
1202	DP Disconnected	GtpManager (DP) disconnected
7003	The number of users exceeded it's limit	The number of users exceeded its limit
7004	The number of devices exceeded it's limit	The number of devices exceeded its limit

New Event

Event Code	Event
370	apUsbSoftwarePackageDownloaded
371	apUsbSoftwarePackageDownloadFailed
530	dpDiscoverySuccess
532	dpStatusManaged
537	dpDeleted
538	dpLicenseInsufficient
550	dpUpgradeStart
551	dpUpgrading
552	dpUpgradeSuccess
553	dpUpgradeFailed
750	syslogServerReachable
751	syslogServerUnreachable
752	syslogServerSwitched
770	planeLoadingRebalancingSucceeded
771	planeLoadingRebalancingFailed
845	clusterUploadVDPFirmwareStart
846	uploadClusterVDPFirmwareSuccess
847	uploadClusterVDPFirmwareFailed
1255	licenseGoingToExpire
1256	apConnectionTerminatedDueToInsufficientLicense
1751	racADLDAPSuccess
1752	racADLDAPFail
1753	racADLDAPBindFail
1754	racLDAPFailToFindPassword
1755	racADNPSFail

Event Code	Event
1756	racADNPSFailToAuthenticate
2151	espAuthServerReachable
2152	espAuthServerUnreachable
2153	espAuthServerResolvable
2154	espAuthServerUnResolvable
2161	espDNATServerReachable
2162	espDNATServerUnreachable
2163	espDNATServerResolvable
2164	espDNATServerUnresolvable

Severity Change

Event Code and Event	Severity Changed From	Severity Changed To
516 - dpPktPoolLow	Major	Informational
517 - dpPktPoolCriticalLow	Critical	Major
519 - dpCoreDead	Critical	Major
837 - resyncNTPTime	Informational	Major
2102 - radiusServerUnreachable	Informational	Major
2122 - ldapServerUnreachable	Informational	Major
2142 - adServerUnreachable	Informational	Major

Attribute Change

Module	Attribute	Attribute Change
Data Plane	dpMac	dpKey
AP Communication Events	"model"="ZF7343"	"model"="R700"
System Events	"model"="ZF7962", "firmware"="3.0.0.0"	"model"="R700", "firmware"="3.2.0.0.x"

Renamed Event

Event Code	Event Name	Renamed To
320	AP CLB limit reached	AP client load balancing limit reached
321	AP CLB limit recovered	AP client load balancing limit recovered
615	DP softGRE GW unreachable	DP sGRE GW unreachable
616	DP softGRE keep alive timeout	DP sGRE keep alive timeout
617	DP softGRE GW inactive	DP sGRE GW inactive

Event Code	Event Name	Renamed To
620	DP softGRE new tunnel	DP sGRE new tunnel
621	DP softGRE del tunnel	DP sGRE del tunnel
622	DP softGRE keepalive recovery	DP sGRE keepalive recovery
624	DP softGRE GW reachable	DP sGRE GW reachable
625	DP softGRE GW active	DP sGRE GW active
626	DP softGRE GW failover	DP sGRE GW failover
1202	DP Disconnected	GtpManager (DP) disconnected

Auto Clearance of Event

Event Code	Event Name
2102	This event triggers the alarm 2102, which is auto cleared by the event code 2101
2122	This event triggers the alarm 2122, which is auto cleared by the event code 2121
2142	This event triggers the alarm 2142, which is auto cleared by the event code 2141.

SmartZone Version 3.1.1

The following are the changes for version 3.1.1.

New Alarm

Alarm Code	Alarm
661	ipsecTunnelDisAssociated
662	ipsecTunnelAssociateFailed

New Event

Event Code	Event
326	cmResetByUser
327	cmResetFactoryByUser
660	ipsecTunnelAssociated
661	ipsecTunnelDisassociated
662	ipsecTunnelAssociateFailed
844	clusterInitiatedMovingAp
2101	radiusServerReachable
2102	radiusServerUnreachable
2121	ldapServerReachable
2122	ldapServerUnreachable

Event Code	Event
2141	adServerReachable
2142	adServerUnreachable
2201	zoneInitiatedMovingAp
2501	nodeIPv6Added
2502	nodeIPv6Deleted

Re-added Event

Event Code	Event
101	apDiscoverySuccess

Renamed Event

Event Code	Event Name	Renamed To
318	AP cable modem rebooted by user	AP cable modem power-cycled by user

RuckOS Version 3.1

The following are the changes for version 3.1.

New Alarm

Alarm Code	Alarm
516	dpPktPoolLow
517	dpPktPoolCriticalLow
519	dpCoreDead
520	dpProcessRestar
862	clusterCfgBackupFailed
864	clusterCfgRestoreFailed
1401	dialnitalizeErr
1403	diaPeerTransportFailure
1404	diaCERError
1407	diaPeerAddError
1409	diaPeerRemoveSuccess
1410	diaRealmEntryErr
1411	diaFailOverToAltPeer
1412	diaFailbackToPeer
1414	diaCEAUnknownPeer
1415	diaNoCommonApp

Alarm Code	Alarm
1551	staAuthFailedTransDown
1552	staAuthFailedFailureResp
1553	staAuthFailedDecodeFailure
1558	staReAuthFailed
1559	staResponseTimerExpired
1560	retransmitExhausted
1651	authFailedOverToSecondary
1652	authFallbackToPrimary
1653	accFailedOverToSecondary
1654	accFallbackToPrimary
7003	tooManyUsers
7004	tooManyDevices

Deprecated Alarm

Alarm Code	Alarm
1008	cfgUpdFailed
1902	unknownRealmAccounting
1909	apAcctRespWhileInvalidConfig

Renamed Alarm

Alarm Code	Alarm Type	Renamed To
701	No LS Responses	No LS responses
721	No LS Responses	No LS responses
1623	App Server Down	App server down
1624	App Server Inactive	App server inactive
1627	Association Down	Association down
1636	Outbound Routing Failure	Outbound routing failure
1637	Did Allocation Failure	Did allocation failure
1960	CGF Server Not Configured	CGF server not configured
1242	TTG Session Critical Threshold	TTG session critical threshold
1243	TTG Session License Exhausted	TTG session license exhausted
1302	Rate Limit for TOR surpassed	Rate limit for TOR surpassed
1911	Unauthorized CoA/DM message dropped	Unauthorized COA/DM message dropped

New Event

Event Code	Event
223	remediationSuccess

Revision History
RuckOS Version 3.1

Event Code	Event
224	remediationFailure
325	cableModemUp
520	dpProcessRestart
626	dpSgreGWFailOver
627	dpSetUpTunnel
860	clusterCfgBackupStart
861	clusterCfgBackupSuccess
862	clusterCfgBackupFailed
863	clusterCfgRestoreSuccess
864	clusterCfgRestoreSuccess
926	ipmiREVote
927	ipmiRETempBB
928	ipmiRETempFP
929	ipmiRETempIOH
930	ipmiRETempMemP
931	ipmiRETempPS
932	ipmiRETempP
933	ipmiRETempHSBP
934	ipmiREFan
935	ipmiREPower
936	ipmiRECurrent
937	ipmiREFanStatus
938	ipmiREPsStatus
939	ipmiREDrvStatus
953	cpuThresholdBackToNormal
954	memoryThresholdBackToNormal
955	diskUsageThresholdBackToNormal
1401	dialnitalizeErr
1402	dialnitialization
1403	diaPeerTransportFailure
1404	diaCERError
1405	diaCERSuccess
1406	dialinvalidVer
1407	diaPeerAddError
1408	diaPeerAddSuccess
1409	diaPeerRemoveSuccess
1410	diaRealmEntryErr
1411	diaFailOverToAltPeer
1412	diaFailbackToPeer
1414	diaCEAUnknownPeer
1415	diaNoCommonApp
1550	staSuccessfulAuthentication

Event Code	Event
1551	staAuthFailedTransDown
1552	staAuthFailedFailureResp
1553	staAuthFailedDecodeFailure
1554	staSessionTermSCGInitSuccess
1555	staSessionTermAAAInitSucess
1556	staSessionTermAAAInitFail
1557	staReAuthSuccess
1558	staReAuthFailed
1559	staResponseTimerExpired
1560	retransmitExhausted
1651	authFailedOverToSecondary
1652	authFallbackToPrimary
1653	accFailedOverToSecondary
1654	accFallbackToPrimary
1655	unavailableLocInfoRequested
1656	incapableLocInfoRequested
1657	unSupportedLocDeliveryRequest
7001	tooManyUsers
7002	tooManyDevices

Modified Event Severity

Event Code	Event	Severity	Changed To
516	dpPktPoolLow	Informational	Major
517	dpPktPoolCriticalLow	Major	Critical
519	dpCoreDead	Major	Critical
5006	lmalcmpUnreachable	Debug	Major

Renamed Event

Event Code	Event Name	Renamed To
181	Ssid-spoofing rogue AP	SSID-spoofing rogue AP
209	Client Roaming	Client roaming
211	3rd Party Client Join	3rd party client join
212	3rd Party Client Inactivity Timeout	3rd party client inactivity timeout
213	3rd Party Client Authorization	3rd party client authorization
214	3rd Party Client Authorization Failure	3rd party client authorization failure
215	3rd Party Client Session Expiration	3rd party client session expiration
216	3rd Party Client Roaming	3rd party client roaming

Revision History
RuckOS Version 3.1

Event Code	Event Name	Renamed To
217	3rd Party Client Session Logout	3rd party client session logout
220	Client Grace Period	Client grace period
308	AP channel updated because Dynamic Frequency Selection (DFS) detected a radar event	AP channel updated because dynamic frequency selection (DFS) detected a radar event
317	AP Brownout	AP brownout
323	AP capacity Reached	AP capacity reached
405	eMAP downlink connected to MAP	EMAP downlink connected to MAP
406	eMAP downlink disconnected from MAP	EMAP downlink disconnected from MAP
407	eMAP uplink connected to MAP	EMAP uplink connected to MAP
408	eMAP uplink disconnected from MAP	EMAP uplink disconnected from MAP
422	Mesh state updated to MAP No Channel	Mesh state updated to MAP no channel
424	Mesh state update to RAP No Channel	Mesh state update to RAP no channel
515	Data plane physical Interface Up	Data plane physical interface up
615	DP SoftgreGW Unreachable	DP softGRE GW unreachable
616	DP Softgre Keep Alive Timeout	DP softGRE keep alive timeout
617	DP SoftgreGW Inact	DP softGRE GW inactive
618	DP DhcpRelay No Resp	DP DHCPRelay no response
619	DP DhcpRelay FailOver	DP DHCPRelay failOver
620	DP SoftGRE New Tunnel	DP softGRE new tunnel
621	DP SoftGRE Del Tunnel	DP softGRE del tunnel
622	DP SoftGRE Keepalive Recovery	DP softGRE keepalive recovery
623	DP DhcpRelay Resp Recovery	DP DHCPRelay response recovery
624	DP SoftGRE GW Reachable	DP softGRE GW reachable
625	DP SoftGRE GW Active	DP softGRE GW active
701	No LS Responses	No LS responses
707	AP received Passive Calibration Request	AP received passive calibration request
708	AP received Passive Footfall Request	AP received passive footfall request
709	AP received Unrecognized Request	AP received unrecognized request
721	No LS Responses	No LS responses
725	SCG received Passive Request	SCG received passive request
727	SCG sent Controller Information report	SCG sent controller information report
728	SCG received Management Request	SCG received management request
729	SCG sent AP Info by Venue Report	SCG sent AP info by venue report
730	SCG sent Query Venues Report	SCG sent query venues report

Event Code	Event Name	Renamed To
731	SCG sent Associated Client Report	SCG sent associated client report
732	SCG forwarded Calibration Request to AP	SCG forwarded calibration request to AP
733	SCG forwarded Footfall Request to AP	SCG forwarded footfall request to AP
734	SCG received Unrecognized Request	SCG received unrecognized request
833	SSH Tunnel Switched	SSH tunnel switched
970	FTP Transfer	FTP transfer
971	FTP Transfer Error	FTP transfer error
980	File Upload	File upload
981	Email Sent Successfully	Email sent successfully
982	Email Sent Failed	Email sent failed
983	SMS Sent Successfully	SMS sent successfully
984	SMS Sent Failed	SMS sent failed
1012	Incorrect Flat File Configuration	Incorrect flat file configuration
1220	PDP update by Roaming succeeded	PDP update by roaming succeeded
1221	PDP update by Roaming failed	PDP update by roaming failed
1244	PDP Update Success COA	PDP update success COA
1245	PDP Update Fail COA	PDP update fail COA
1647	CoA Sent NAS	CoA sent NAS
1648	CoA NAK Received NAS	CoA NAK received NAS
1649	CoA Authorize Only Access Reject	CoA authorize only access reject
1650	CoA RWSG MWSG Notification Failure	CoA RWSG MWSG notification failure
1960	CGF Server Not Configured	CGF server not configured
2001	ZD AP Migrating	ZD AP migrating
2002	ZD AP Migrated	ZD AP migrated
2003	ZD AP Rejected	ZD AP rejected
2004	ZD AP Migration Failed	ZD AP migration failed
1302	Rate Limit for TOR surpassed	Rate limit for TOR surpassed
1911	Unauthorized CoA/DM message dropped	Unauthorized COA/DM message dropped
1238	DHCP Inform Received	DHCP inform received
1239	DHCP Dcln Received	DHCP decline received
1240	TTG Session Warning Threshold	TTG session warning threshold
1241	TTG Session Major Threshold	TTG session major threshold
1242	TTG Session Critical Threshold	TTG session critical threshold
1243	TTG Session License Exhausted	TTG session license exhausted
1620	Destination Available	Destination available
1623	App Server Down	App server down
1624	App Server Inactive	App server inactive

Event Code	Event Name	Renamed To
1625	App Server Active	App server active
1627	Association Down	Association down
1628	Association Up	Association up
1630	Send Auth Info Success	Send auth info success
1634	Insert Sub Data Success	Insert sub data success
1635	Insert Sub Data Failed	Insert sub data failed
1636	Outbound Routing Failure	Outbound routing failure
1637	Did Allocation Failure	Did allocation failure
1639	Restore Data Success	Restore data success
1640	Restore Data Failed	Restore data failed
1641	DM Received from AAA	DM received from AAA
1643	DM Sent to NAS	DM sent to NAS
1644	DM NACK Received from NAS	DM NACK received from NAS
1645	CoA Received from AAA	CoA received from AAA
1801	3rdParty AP Connected	3rd party AP connected

RuckOS Version 3.0

The following are the changes for version RuckOS 3.0.

New Alarm

Alarm Code	Alarm
115	apJoinZoneFailed
510	dpReboot
614	apSoftGREGatewayNotReachable
701	apLBSNoResponses
702	apLBSAuthFailed
704	apLBSConnectFailed
721	scgLBSNoResponse
722	scgLBSAuthFailed
724	scgLBSConnectFailed
834	diskUsageExceed
1008	cfgUpdFailed
1302	rateLimitMORSurpassed
5001	processInit
5002	pmipUnavailable
5003	unallocatedMemory
5004	updateCfgFailed
5006	lmalcmpUnreachable

Alarm Code	Alarm
5008	ImaFailOver
5010	bindingFailure
5102	lostCnxnToDHCP

Deprecated Alarm

Alarm Code	Alarm
106	apDiscoveryFail
109	apFirmwareUpdated
110	apConfUpdated
301	apRebootByUser
304	apFactoryReset
305	apConnected
307	apHeartbeatLost
309	cmRebootByUser
505	dpUpdateStatusFailed
506	dpUpdateStatisticFailed
507	dpConnected
508	dpPhyInterfaceUp
509	dpConfUpdated
603	dpTearDownTunnel
608	apBuildTunnelSuccess
609	apBuildTunnelFailed
610	apTunnelDisconnected
611	apSoftGRETunnelFailoverPtoS
612	apSoftGRETunnelFailoverStoP
812	upgradeClusterNodeSuccess
814	clusterLeaderChanged
815	upgradeEntireClusterSuccess
816	nodeBondInterfaceUp
817	nodePhyInterfaceUp
818	clusterBackToInService
819	backupClusterSuccess
820	newNodeJoinSuccess
821	clusterAppStart
822	removeNodeSuccess
823	restoreClusterSuccess
824	nodeBackToInService
833	sshTunnelSwitched
971	ftpTransferError
1010	smfRegFailed

Renamed Alarm Type

Alarm Code	Alarm Type	Renamed To
108	apWlanMismatched	apWlanOversubscribed
1242	sessionCriticalThreshold	ttgSessionCriticalThreshold
1243	sessionLicenseExhausted	ttgSessionLicenseExhausted
1302	rateLimitTORSurpassed	rateLimitMORSurpassed
1626	assocCantStart	assocEstbFailed
1960	CGFServerNotConfigured	cgfServerNotConfigured
5004	updateCgffailed	updateCfgFailed

Modification of Alarm Severity

Alarm Code	Alarm	Severity	Severity Modified To
108	apWlanMismatched	Informational	Major
614	apSoftGREGatewayNotReachable	Major	Critical
960	licenseThresholdExceeded	Warning	Critical and Major
1636	outboundRoutingFailure	Major	Critical
1952	pdnGwVersionNotSupportedMsgReceived	Critical	Major

Renamed Alarm

Code	Alarm Name	Renamed To
104	AP model different with swap AP configuration	AP swap model mismatched
105	AP model different with pre-provision configuration	AP pre-provision model mismatched
108	AP WLAN mismatched	AP WLAN oversubscribed
809	Control plane interface down	Node bond interface down
810	Control plane physical interface down	Node physical interface down
952	Disk Usage threshold exceeded	Disk usage threshold exceeded
1003	Keep alive failure	Keepalive failure
1016	HIP Failover	HIP failed over
1202	Lost connection to Data plane	DP disconnected
1302	Rate Limit for Total Outstanding Requests (TOR) Surpassed	Rate Limit for MOR surpassed
1618	Destination Not reachable	Destination not reachable
1626	Association cannot Start	Association establishment failed
1902	Unknown realm accounting	Unknown realm
1909	apAcctRespWhileInvalidConfig	AP accounting response while invalid config
1910	apAcctMsgDropNoAcctStartMsg	AP account message drop while no accounting start message

Code	Alarm Name	Renamed To
1911	unauthorizedCoaDmMessageDropped	Unauthorized CoA/DM message dropped
1960	CGFServerNotConfigured	CGF Server Not Configured
5001	Initial Process	Process initiated
5002	PMIPv6 is Unavailable	PMIPv6 unavailable
5004	Update config failed	Config update failed
5006	LMA ICMP is unreachable	LMA ICMP unreachable
5008	LMA failover	LMA failed over
5010	Binding failure	Binding failed
5102	Lost DHCP connection	DHCP connection lost

New Event

Event Code	Event
115	apJoinZoneFailed
116	apIllegalToChangeCountryCode
180	genericRogueAPDetected
181	ssid-spoofingRogueAPDetected
182	mac-spoofingRogueAPDetected
183	same-networkRogueAPDetected
184	ad-hoc-networkRogueAPDetected
185	maliciousRogueAPTimeout
218	smartRoamDisconnect
219	clientBlockByDeviceType
220	clientGracePeriod
221	onboardingRegistrationSuccess
222	onboardingRegistrationFailure
225	forceDHCPDisconnect
319	319##smartMonitorTurnOffWLAN
320	apCLBlimitReached
321	apCLBlimitRecovered
322	apWLANStateChanged
323	apCapacityReached
324	apCapacityRecovered
516	dpPktPoolLow
517	dpPktPoolCriticalLow
518	dpPktPoolRecover
519	dpCoreDead
611	apSoftGREtunnelFailoverPtoS
612	apSoftGREtunnelFailoverStoP
613	apSoftGREGatewayReachable
614	apSoftGREGatewayNotReachable

Revision History
RuckOS Version 3.0

Event Code	Event
701	apLBSNoResponses
702	apLBSAuthFailed
703	apLBSConnectSuccess
704	apLBSConnectFailed
705	apLBSStartLocationService
706	apLBSStopLocationService
707	apLBSRcvdPassiveCalReq
708	apLBSRcvdPassiveFFReq
709	apLBSRcvdUnrecognizedRequest
721	scgLBSNoResponse
722	scgLBSAuthFailed
723	scgLBSConnectSuccess
724	scgLBSConnectFailed
725	scgLBSStartLocationService
726	scgLBSRcvdNoPayload
727	scgLBSsentControllerInfo
728	scgLBSRcvdMgmtRequest
729	scgLBSsendAPInfoByVenueReport
730	scgLBSsendVenuesReport
731	scgLBSsendClientInfo
732	scgLBSFwdPassiveCalReq
733	scgLBSFwdPassiveFFReq
734	scgLBSRcvdUnrecognizedRequest
837	resyncNTPTime
838	diskUsageExceed
981	mailSendSuccess
982	mailSendFailed
983	smsSendSuccess
984	smsSendFailed
1250	licenseSyncSuccess
1251	licenseSyncFail
1252	licenseImportSuccess
1253	licenseImportFail
1254	licenseChanged
1300	rateLimitThresholdSurpassed
1301	rateLimitThresholdRestored
1302	rateLimitMORSurpassed
2001	zdAPMigrating
2002	zdAPMigrated
2003	zdAPRejected
2004	zdAPMigrationFailed
5001	processInit

Event Code	Event
5002	pmipUnavailable
5003	unallocatedMemory
5004	updateCfgFailed
5005	lmalcmpReachable
5006	lmalcmpUnreachable
5007	lmaHbUnreachable
5008	lmaFailOver
5009	bindingSuccess
5010	bindingFailure
5011	bindingExpired
5012	bindingRevoked
5013	bindingReleased
5100	processTerminated
5101	connectedToDHCP
5102	lostCnxnToDHCP

Deprecated Event

Event Code	Event
101	apDiscoverySuccess
102	apDiscoveryFail
609	apBuildTunnelFailed
1004	keepAliveMissed
1010	smfRegFailed
1011	eventRegFailed

Re-added Event

Event Code	Event
827	ntpTimeSynched

Modifications to Event Severity

Event Code	Event Code	Severity	Changed To
114	apWlanOversubscribed	Informational	Major
320	apCLBlimitReached	Informational	Warning
835	nodeBackToInService	Major	Informational
960	licenseThresholdExceeded	Informational	Warning
1007	cfgUpdSuccess	Debug	Informational
1008	cfgUpdFailed	Major	Debug
1009	cfgRcvFailed	Major	Debug

Event Code	Event Code	Severity	Changed To
1201	connectedToDblade	Debug	Informational
1209	c2dCfgFailed	Informational	Warning
1301	rateLimitThresholdRestored	Major	Informational
1603	unknownRealm	Major	Debug
1908	apAcctRetransmittedMsgDropped	Major	Debug
1910	apAcctMsgDropNoAcctStartMsg	Major	Critical
1911	unauthorizedCoaDmMessageDropped	Major	Critical
1952	pdnGwVersionNotSupportedMsgReceived	Critical	Major
5006	lmalcmpUnreachable	Debug	Major

Renamed Event Type

Event Code	Event Name	Renamed To
114	apWlanMismatched	apWlanOversubscribed
416	rmapDlinkConnectWithMap	rapDlinkConnectWithMap
511	dpUpdateStatisticFalied	dpUpdateStatisticFailed
1017	standbyHipRestart	hipStandbyRestart
1240	sessionWarningThreshold	ttgSessionWarningThreshold
1241	sessionMajorThreshold	ttgSessionMajorThreshold
1242	sessionCriticalThreshold	ttgSessionCriticalThreshold
1243	sessionLicenseExhausted	ttgSessionLicenseExhausted
1302	rateLimitTORSurpassed	rateLimitMORSurpassed
1626	assocCantStart	assocEstbFailed
1960	CGFServerNotConfigured	cgfServerNotConfigured

Renamed Event

Code	Event Name	Renamed To
103	AP status changed to Managed	AP managed
112	AP model different with pre-provision configuration	AP pre-provision model mismatched
113	AP model different with swap AP configuration	AP swap model mismatched
114	AP WLAN mismatched	AP WLAN oversubscribed
202	Client joined successfully	Client joined
205	Client connection timed out due to inactivity	Client connection timed out
210	Client session logout	Client logged out
218	Client Roaming Disconnect	Client roaming disconnected
303	AP connection lost	AP disconnected
305	AP reset to factory default settings, new:	AP reset to factory default

Code	Event Name	Renamed To
311	AP change control plane	AP changed control plane
501	Data plane discovered successfully	Data plane discovered
620	DP Softgre New Tunnel	DP SoftGRE New Tunnel
621	DP Softgre Del Tunnel	DP SoftGRE Del Tunnel
622	DP Softgre KeepAlive Recovery	DP SoftGRE Keepalive Recovery
624	DP SoftgreGW Reachable	DP SoftGRE GW Reachable
625	DP SoftgreGW Active	DP SoftGRE GW Active
826	Cluster Node rebooted	Cluster node rebooted
828	Cluster node shutdown	Cluster node shut down
1003	Keep alive failure	Keepalive failure
1014	HIP Started	HIP started
1015	HIP Stopped	HIP stopped
1016	HIP Failover	HIP failed over
1017	Hip Restart	Standby HIP restarted
1018	HIP Cache Cleanup	HIP cache cleaned
1007	Configuration update success	Configuration updated
1201	Connected to Data plane	DP connected
1202	Lost connection to Data plane	DP disconnected
1205	Session updated at Data plane	Session updated at DP
1206	Session update error at Data plane	Session update at DP failed
1207	Session deleted at Data plane	Session deleted at DP
1208	Session delete error at Data plane	Session delete at DP failed
1217	Create PDP Failed	PDP create failed
1218	Initial PDP updated successfully HLR	PDP update by HLR succeeded
1219	Initial PDP updated fail HLR	PDP update by HLR failed
1220	Initial PDP updated successfully Roam	PDP update by Roaming succeeded
1221	Initial PDP updated fail Roam	PDP update by Roaming failed
1222	Received PDP update successfully GGSN	PDP update by GGSN succeeded
1223	Received PDP update fail GGSN	PDP update by GGSN failed
1224	Initial PDP deleted successfully	PDP delete by TTG succeeded
1225	Initial PDP deleted fail	PDP delete by TTG failed
1226	Received PDP deleted successfully	PDP delete by GGSN succeeded
1227	Received PDP deleted fail	PDP delete by GGSN failed
1229	ipAssigned	IP assigned
1300	Rate Limit Threshold Surpassed	Rate limit threshold surpassed
1301	Rate Limit Threshold Restored	Rate limit threshold restored
1302	Rate Limit for Total Outstanding Requests (TOR) Surpassed	Rate Limit for TOR surpassed
1604	Authentication success	Authentication succeeded
1606	Pseudonym authentication success	Pseudonym authentication succeeded
1608	Fast re-authentication success	Fast re-authentication succeeded

Revision History
RuckOS Version 3.0

Code	Event Name	Renamed To
1612	CGF keep alive not responded	CGF keepalive not responded
1613	CDR transfer successful	CDR transfer succeeded
1618	Destination Not Reachable	Destination not reachable
1623	AppServer Down	App Server Down
1624	AppServer Inactive	App Server Inactive
1625	AppServer Active	App Server Active
1626	Association can not Start	Association establishment failed
1631	send Auth Info Failed	Auth info sending failed
1632	Update GPRS Location Success	GPRS location update succeeded
1633	Update GPRS Location Failed	GPRS location update failed
1902	Unknown realm accounting	Unknown realm
5001	Initial Process	Process initiated
5002	PMIPv6 is Unavailable	PMIPv6 unavailable
5004	Update config failed	Config update failed
5005	LMA ICMP is reachable	LMA ICMP reachable
5006	LMA ICMP is unreachable	LMA ICMP unreachable
5007	LMA server is unreachable	LMA server unreachable
5008	LMA failover	LMA failed over
5009	Binding success	Binding succeeded
5010	Binding failure	Binding failed
5012	Revoke binding	Binding revoked
5013	Release binding	Binding released
5100	Stop process	Process stopped
5101	Connect To DHCP	DHCP connected
5102	Lost DHCP connection	DHCP connection lost

Alarm and Event Management

- [Overview](#)..... 55
- [Alarm and Event Management](#)..... 55

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 25 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 55
- [Event Attributes](#) on page 56
- [Generation of Alarm and Event](#) on page 56

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@D4:6B: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@FD: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:

- 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.
- 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

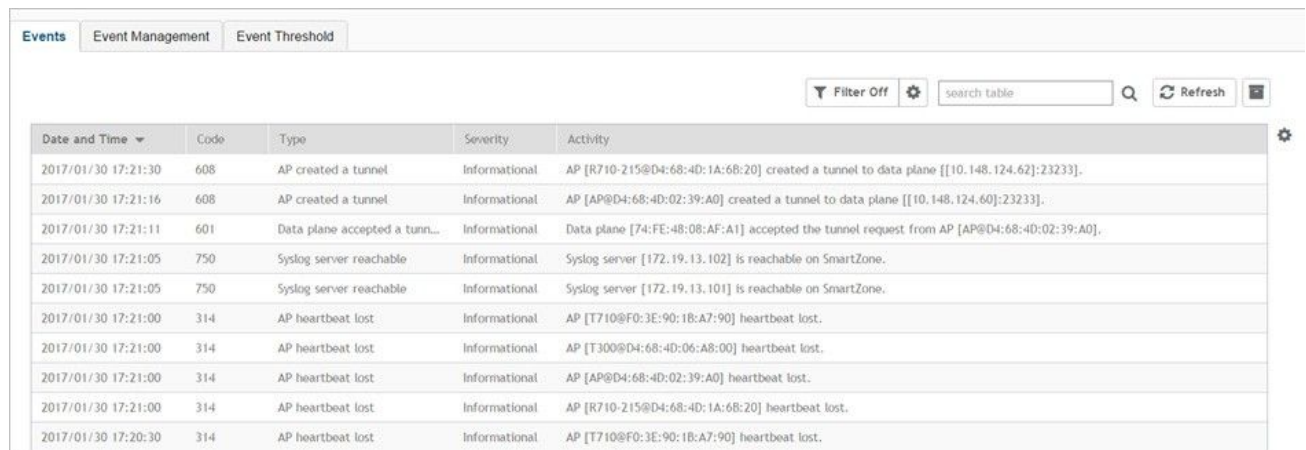
Event Management lists the disabled events that are filtered at the source whenever possible to minimize resources for processing events. The SMTP server is disabled by default. You must enable and configure the SMTP server so notification emails can be delivered successfully.

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 is a 'Filter Off' button, 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 several 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 59 and [Events Types](#) on page 139 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.....	59
• Accounting Alarms.....	59
• AP Authentication Alarms.....	63
• AP Communication Alarms.....	67
• AP LBS Alarms.....	71
• AP State Change Alarms.....	72
• Authentication Alarms.....	76
• Control and Data Plane Interface Alarms.....	81
• Cluster Alarms.....	81
• Configuration Alarms.....	93
• Data Plane Alarms.....	95
• Gn/S2a Interface Alarms.....	101
• GR Interface Alarms.....	107
• IPMI Alarms.....	111
• Licensing Alarms.....	118
• PMIPv6 Alarms.....	121
• SCI Alarms.....	122
• Session Alarms.....	124
• System Alarms.....	124
• Threshold Alarms.....	133
• Tunnel Alarms - Access Point.....	136

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 60
- [Accounting fallback to primary](#) on page 60
- [Accounting fallback to primary](#) on page 60
- [AP accounting message mandatory parameter missing](#) on page 61
- [AP accounting message decode failed](#) on page 62
- [AP account message drop while no accounting start message](#) on page 62
- [Unauthorized CoA/DM message dropped](#) on page 63

Accounting server not reachable

TABLE 7 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	"mvsold"=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 8 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	"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"
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 9 Accounting fallback to primary alarm

Alarm	Accounting fallback to primary
Alarm Type	accFallbackToPrimary

TABLE 9 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	"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"
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 10 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	"mvsold"="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"
Displayed on the web interface	[{srcProcess}] Mandatory attribute missing in Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}], with username [{uelmsi}@{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 11 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, "zoneld"="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"
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 12 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", "zoneld"="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 Acct Interim/Stop message as account start is not received from the AP.

TABLE 12 AP account message drop while no accounting start message alarm (continued)

Alarm	AP account message drop while no accounting start message
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 13 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	"mvnold"="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.

NOTE

Refer to [Accounting Events](#) on page 140.

AP Authentication Alarms

Following are the alarms related to AP authentication.

- [RADIUS server unreachable](#) on page 64
- [LDAP server unreachable](#) on page 64
- [AD server unreachable](#) on page 64
- [WeChat ESP authentication server unreachable](#) on page 65
- [WeChat ESP authentication server unresolvable](#) on page 65
- [WeChat ESP DNAT server unreachable](#) on page 66
- [WeChat ESP DNAT server unresolvable](#) on page 66

RADIUS server unreachable

TABLE 14 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"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
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 15 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"="ZF7982","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 16 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.

TABLE 16 AD server unreachable alarm (continued)

Alarm	AD server unreachable
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"=""
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 17 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 18 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

Alarm Types

AP Authentication Alarms

TABLE 18 WeChat ESP authentication server unresolvable alarm (continued)

Alarm	WeChat ESP authentication server unresolvable
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 19 WeChat ESP DNAT server unreachable alarm

Alarm	WeChat ESP DNAT server unreachable
Alarm Type	espDNATServerUnreachable
Alarm Code	2162
Severity	Major
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 20 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.

NOTE

Refer to [AP Authentication Events](#) on page 145.

AP Communication Alarms

Following are the alarms related to access point communications.

- [AP rejected](#) on page 67
- [AP configuration update failed](#) on page 67
- [AP swap model mismatched](#) on page 68
- [AP pre-provision model mismatched](#) on page 68
- [AP firmware update failed](#) on page 69
- [AP WLAN oversubscribed](#) on page 69
- [AP join zone failed](#) on page 69
- [AP image signing failed](#) on page 70

AP rejected

TABLE 21 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 22 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.

Alarm Types

AP Communication Alarms

TABLE 22 AP configuration update failed alarm (continued)

Alarm	AP configuration update failed
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 23 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.
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 24 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 25 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 26 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 wlans. 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"> • 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. • Find the WLAN group used by the AP and reduce the number of WLAN.

AP join zone failed

NOTE

This alarm is not applicable for vSZ-H.

TABLE 27 AP join zone failed alarm

Alarm	AP join zone failed
Alarm Type	apJoinZoneFailed

TABLE 27 AP join zone failed alarm (continued)

Alarm	AP join zone failed
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 28 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"> • Category 1: AP firmware images for releases prior to 3.4.x is in the format USI (Un Signed Image) • Category 2: AP firmware images for releases 3.4.x and 3.5.x is in the format ISI (Intermediate Signed Image) • Category 3: AP firmware images for releases 3.6 and above is in the format FSI (Fully Signed Image) <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</p>

TABLE 28 AP image signing failed alarm (continued)

Alarm	AP Image signing failed
	<p>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"> • Step 1: Configure FTP or TFTP server in the network with any image (even FSI for 3.6.x is allowed) • Step 2: 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. • Step 3: Execute the command <code>fw update</code> • Step 4: On completion of step 3 you can now upgrade the API image to ISI > FSI using the controller web user interface.

NOTE

Refer to [AP Communication Events](#) on page 150.

AP LBS Alarms

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

- [No LS responses](#) on page 71
- [LS authentication failure](#) on page 72
- [AP failed to connect to LS](#) on page 72

No LS responses

TABLE 29 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 a maintenance mode. Report this to the location server owner.

LS authentication failure

TABLE 30 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 31 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"=""
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.

NOTE

Refer to [AP LBS Events](#) on page 158.

AP State Change Alarms

Following are the alarms related to access point state changes.

- [AP rebooted by system](#) on page 73
- [AP disconnected](#) on page 73
- [AP deleted](#) on page 73

- [AP cable modem interface down](#) on page 74
- [AP DHCP service failure](#) on page 74
- [AP NAT failure](#) on page 75
- [AP DHCP/NAT DWPD Ethernet port configuration override](#) on page 75
- [SZ DHCP/NAT DWPD Ethernet port configuration override](#) on page 76

AP rebooted by system

TABLE 32 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 33 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 34 AP deleted alarm

Alarm	AP deleted
Alarm Type	apDeleted

Alarm Types

AP State Change Alarms

TABLE 34 AP deleted alarm (continued)

Alarm	AP deleted
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 35 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
Description	This alarm is triggered when the AP cable modem interface is down.
Recommended Actions	Check cable modem. Try rebooting the cable modem.

NOTE

Refer to [AP State Change Events](#) on page 168.

AP DHCP service failure

TABLE 36 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 xxx 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.

TABLE 36 AP DHCP service failure alarm (continued)

Alarm	Both primary and secondary DHCP server APs 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 37 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 38 AP DHCP/NAT DWPD Ethernet port configuration override alarm

Alarm	AP DHCP/NAT DWPD Ethernet port configuration override
Alarm Type	clusterRedundancyApRehomeIncomplete
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 DWPD configuration.
Description	This alarm is triggered when the AP does not have an available Ethernet port for LAN.

SZ DHCP/NAT DWPD Ethernet port configuration override

TABLE 39 SZ DHCP/NAT DWPD Ethernet port configuration override alarm

Alarm	SZ DHCP/NAT DWPD 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.

NOTE

Refer to [GUID-B6B14CB5-72F5-46DB-A27C-2DF2F5417ACA](#).

Authentication Alarms

The following are the alarms related to authentication.

- [Authentication server not reachable](#) on page 76
- [Authentication failed over to secondary](#) on page 77
- [Authentication fallback to primary](#) on page 77
- [AD/LDAP connectivity failure](#) on page 78
- [Bind fails with AD/LDAP](#) on page 78
- [Bind success with LDAP, but unable to find clear text password for the user](#) on page 79
- [RADIUS fails to connect to AD NPS server](#) on page 79
- [RADIUS fails to authenticate with AD NPS server](#) on page 80
- [Fails to establish TLS tunnel with AD/LDAP](#) on page 80

Authentication server not reachable

TABLE 40 Authentication server not reachable alarm

Alarm	Authentication server not reachable
Alarm Type	authSrvrNotReachable
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" "authSrvrIp"="20.20.20.20" "SCGMgmtIp"="2.2.2.2"

TABLE 40 Authentication server not reachable alarm (continued)

Alarm	Authentication server not reachable
Displayed on the web interface	Authentication Server [{{authSrvrIp}}] 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 41 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 42 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 43 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.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=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"> • Check whether AD/LDAP server instance is running on the target machine • Check whether the AD/LDAP server can be reached from the controller • Verify if AD/LDAP server instances are listening on ports 3268 and 389 • Verify if the requests are reaching AD/LDAP servers by any packet capture tool (tcpdump, wireshark)

Bind fails with AD/LDAP

TABLE 44 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", "mvnold"=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"> • Verify the base and administrator domain names as configured in the controller web interface • Verify the administrator user name and password as configured in the controller web interface • Verify whether the configured administrator user name and password is authenticated by the AD/LDAP servers

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

TABLE 45 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.
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 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 46 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", "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 alarm is triggered when the RADIUS server fails to connect to the AD NPS server.
Recommended Actions	<ul style="list-style-type: none"> Verify if the configured NPS server instance is up and running (Network Policy Server) Verify if the NPS server instance is communicating on the standard RADIUS port 1812 Ensure that Windows server where AD/NPS server is provisioned can be reached from the controller web interface

RADIUS fails to authenticate with AD NPS server

TABLE 47 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", "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 alarm is triggered when the RADIUS server fails to authenticate with the AD NPS server.
Recommended Actions	<ul style="list-style-type: none"> The shared secret for NPS server should be same as that of administrator password provisioned in the controller web interface for AD server NPS should be configured to accept request (CHAP and MSCHAPv2) from the controller For CHAP authentication to work the AD server should store the password in reversible encryption format Ensure that NPS is registered with AD server

NOTE

Refer to [Authentication Events](#) on page 185.

Fails to establish TLS tunnel with AD/LDAP

TABLE 48 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", "mvnold"=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.

NOTE

Refer to [Authentication Events](#) on page 185.

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 81

GtpManager (DP) disconnected

TABLE 49 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", "ctrlBladelp"="1.1.1.1", "dataBladelp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2
Displayed on the web interface	The connectivity between Control plane [{ctrlBladelp}] and Data plane [{dataBladelp}] 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 Control and Data Plane Interface on page 197 event 1201.

NOTE

Refer to [Control and Data Plane Interface](#) on page 197.

Cluster Alarms

Following are the alarms related to cluster.

- [New node failed to join](#) on page 82
- [Node removal failed](#) on page 83
- [Node out of service](#) on page 83
- [Cluster in maintenance state](#) on page 83
- [Cluster backup failed](#) on page 84
- [Cluster restore failed](#) on page 84
- [Cluster upgrade failed](#) on page 85
- [Cluster application stopped](#) on page 86
- [Node bond interface down](#) on page 86

- [Node physical interface down](#) on page 86
- [Cluster node rebooted](#) on page 87
- [Cluster node shut down](#) on page 87
- [Disk usage exceed threshold](#) on page 88
- [Cluster out of service](#) on page 88
- [Cluster upload AP firmware failed](#) on page 89
- [Cluster add AP firmware failed](#) on page 89
- [Unsync NTP time](#) on page 89
- [Cluster upload KSP file failed](#) on page 90
- [Configuration backup failed](#) on page 90
- [Configuration restore failed](#) on page 90
- [AP certificate updated](#) on page 91
- [Upgrade SS table failed](#) on page 91
- [Cluster redundancy sync configuration failed](#) on page 91
- [Cluster redundancy restoring configuration failed](#) on page 92
- [Not all APs rehome after timeout](#) on page 92

New node failed to join

TABLE 50 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 join process . 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"> • 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. • 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.

Node removal failed

TABLE 51 Node removal failed alarm

Alarm	Node removal failed
Alarm Type	removeNodeFailed
Alarm Code	802
Severity	Major
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 52 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 53 Cluster in maintenance state alarm

Alarm	Cluster in maintenance state
Alarm Type	clusterInMaintenanceState
Alarm Code	804
Severity	Critical

TABLE 53 Cluster in maintenance state alarm (continued)

Alarm	Cluster in maintenance state
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
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"> The entire system backup is in process. In a two-node cluster, the remove-node process is working. <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 54 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"> Insufficient disk space. Communication between nodes may be broken. Errors due to the underlying Python script.

Cluster restore failed

TABLE 55 Cluster restore failed alarm

Alarm	Cluster restore failed
Alarm Type	restoreClusterFailed
Alarm Code	806

TABLE 55 Cluster restore failed alarm (continued)

Alarm	Cluster restore failed
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}].
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 56 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	"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}]. 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. Possible causes:</p> <ul style="list-style-type: none"> • Insufficient disk space • Communication between nodes might be broken. • Errors due to the underlying Python script.

Cluster application stopped

TABLE 57 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	"appName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
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 58 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 59 Node physical interface down alarm

Alarm	Node physical interface down
Alarm Type	nodePhyInterfaceDown

TABLE 59 Node physical interface down alarm (continued)

Alarm	Node physical interface down
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: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.
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 60 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 61 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.

TABLE 61 Cluster node shut down alarm (continued)

Alarm	Cluster node shut down
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.

Disk usage exceed threshold

TABLE 62 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 63 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"
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 64 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 65 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 66 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 67 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 68 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 69 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.

TABLE 69 Configuration restore failed alarm (continued)

Alarm	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 70 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 Administration > AP Certificate replacement page to verify and follow the certificate refresh process.

Upgrade SS table failed

TABLE 71 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"
Displayed on the web interface	Node [[nodeName]] upgrade SSTable failed.
Description	This alarm is triggered when the SS table upgrade fails.

NOTE

Refer to [GUID-684F0A10-0CC1-43AB-94E1-5B89C835A612](#).

Cluster redundancy sync configuration failed

TABLE 72 Cluster redundancy sync configuration failed alarm

Alarm	Cluster redundancy sync configuration failed
Alarm Type	clusterRedundancySyncCfgFailed

TABLE 72 Cluster redundancy sync configuration failed alarm (continued)

Alarm	Cluster redundancy sync configuration failed
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 73 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 74 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"
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.

NOTE

Refer to [Cluster Events](#) on page 215.

Configuration Alarms

Following are the alarms related to configuration.

- [Zone configuration preparation failed](#) on page 93
- [AP configuration generation failed](#) on page 93
- [End-of-life AP model detected](#) on page 94
- [VLAN configuration mismatch on non DHCP/NAT WLAN](#) on page 94
- [VLAN configuration mismatch on DHCP/NAT WLAN](#) on page 95

Zone configuration preparation failed

TABLE 75 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 76 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 77 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"> Reset the APs to a factory setting using the AP command line Delete these APs through the controller Web Interface > Configuration AP List

NOTE

Refer to [Configuration Events](#) on page 236.

VLAN configuration mismatch on non DHCP/NAT WLAN

TABLE 78 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 1024 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 79 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
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"="xxx", "wlanID"="xxx", "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.

NOTE

Refer to [Configuration Events](#) on page 236.

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 96
- [Data plane disconnected](#) on page 96
- [Data plane physical interface down](#) on page 96
- [Data plane rebooted](#) on page 97
- [Data plane packet pool is under low water mark](#) on page 97
- [Data plane packet pool is under critical low water mark](#) on page 98
- [Data plane core dead](#) on page 98
- [Data plane process restarted](#) on page 98
- [Data plane license is not enough](#) on page 99
- [Data plane upgrade failed](#) on page 99
- [Data plane of data center side fails to connect to the CALEA server](#) on page 100
- [Data plane fails to connects to the other data plane](#) on page 100
- [Data plane DHCP IP pool usage rate is 100 percent](#) on page 101

Data plane configuration update failed

TABLE 80 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
Attribute	"dpKey"="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 81 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", "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 82 Data plane physical interface down alarm

Alarm	Data plane physical interface down
Alarm Type	dpPhyInterfaceDown
Alarm Code	504
Severity	Critical

TABLE 82 Data plane physical interface down alarm (continued)

Alarm	Data plane physical interface down
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"
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 83 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 84 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 85 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: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.
Recommended Actions	The operator needs to check for network looping.

Data plane core dead

TABLE 86 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: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 87 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: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.

TABLE 87 Data plane process restarted alarm (continued)

Alarm	Data plane process restarted
Recommended Actions	No action required.

Data plane license is not enough

NOTE

Alarm 538 is applicable only for vSZ-H.

TABLE 88 Data plane license is not enough alarm

Alarm	Data plane license is not enough
Alarm Type	dpLicenseInsufficient
Alarm Code	538
Severity	Major
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 89 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	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.

TABLE 89 Data plane upgrade failed alarm (continued)

Alarm	Data plane upgrade failed
	<p>The operator can use the following vSZ-D CLI commands to:</p> <ul style="list-style-type: none"> View the previous upgrade status and reason in case of a failure - <code>ruckus# show upgrade-state / ruckus# show upgrade-history</code> Save the debug file for viewing - <code>ruckus (debug) # save-log</code> Check the connection status between vSZ and vSZ-D - <code>ruckus# show status</code> Check the current vSZ-D software version - <code>ruckus # show version</code> <p>NOTE 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 90 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 91 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}}

TABLE 91 Data plane fails to connects to the other data plane alarm (continued)

Alarm	Data plane fails to connects to the other data plane
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 92 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"
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%
Recommended Actions	Increase the size of the DHCP IP address pool, or reduce the number of stations requiring addresses.

NOTE

Refer to [Data Plane Events](#) on page 242.

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 102
- [GGSN not reachable](#) on page 102
- [GGSN not resolved](#) on page 102
- [PDNGW could not be resolved](#) on page 103
- [PDNGW version not supported](#) on page 103
- [Associated PDNGW down](#) on page 104
- [Create session response failed](#) on page 104
- [Decode failed](#) on page 105
- [Modify bearer response failed](#) on page 105
- [Delete session response failed](#) on page 106
- [Delete bearer request failed](#) on page 106
- [Update bearer request failed](#) on page 106

- [CGF server not configured](#) on page 107

GGSN restarted

TABLE 93 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	"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 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 94 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	"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} (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 95 GGSN not resolved alarm

Alarm	GGSN not resolved
Alarm Type	ggsnNotResolved

TABLE 95 GGSN not resolved alarm (continued)

Alarm	GGSN not resolved
Alarm Code	1215
Severity	Major
Aggregation Policy	From the event code 1215 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", "gtppclp"="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 96 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	mvnold"=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 97 PDNGW version not supported alarm

Alarm	PDNGW version not supported
Alarm Type	pdnGwVersionNotSupportedMsgReceived
Alarm Code	1952
Severity	Major

TABLE 97 PDNGW version not supported alarm (continued)

Alarm	PDNGW version not supported
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" "gtpclp"="5.5.5.5" "pgwlp"="1.1.1.1" "SCGMgmtlp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} Version not supported message received from PDN GW with IP {{pgwlp}} on {produce.short.name} {{SCGMgmtlp}}.
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 98 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" "pgwlp"="1.1.1.1" "SCGMgmtlp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} Association with PDN GW with IP {{pgwlp}} from {produce.short.name} {{SCGMgmtlp}} 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 99 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	"mvsold"="12" "wlanId"="1" "zoneld"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "gtpclp"="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>"

TABLE 99 Create session response failed alarm (continued)

Alarm	Create session response failed
Displayed on the web interface	{{srcProcess}} Create Session response from PDN GW with IP {{pgwlp}} on {produce.short.name} {{SCGMgmtlp}} failed, for UE with username {{uelmsi}@{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 100 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" "gtpclp"="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 101 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	"mvnold"="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" "pgwlp"="1.1.1.1" "SCGMgmtlp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "uelmsi"="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 {{uelmsi}@{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 102 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.
Attribute	"mvsold"="12" "wlanid"="1" "zoned"="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 103 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 104 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.

TABLE 104 Update bearer request failed alarm (continued)

Alarm	Update bearer request failed
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "gtpclp"="5.5.5.5" "pgwlp"="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 {{pgwlp}} 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 105 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	"mvnold"="12" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="CIP" "realm"="NA" "ggsnIp"="10.10.10.10" "SCGMgmtIp"="2.2.2.2" "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="1.1.1.1"
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 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.

NOTE

Refer to [Gn/S2a Interface Events](#) on page 258.

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 108
- [App server down](#) on page 108
- [App server inactive](#) on page 109
- [Association establishment failed](#) on page 109
- [Association down](#) on page 109

- [Outbound routing failure](#) on page 110
- [Did allocation failure](#) on page 110

Destination not reachable

TABLE 106 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.
Attribute	"mvnold"="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 107 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	"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 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 108 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	"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 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 109 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	"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	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 110 Association down alarm

Alarm	Association down
Alarm Type	assocDown

TABLE 110 Association down alarm (continued)

Alarm	Association down
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	"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 alarm is triggered when the stream control transmission protocol (SCTP) association is down.
Recommended Actions	Manual intervention is required.

Outbound routing failure

TABLE 111 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	"mvnold"="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 112 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.

TABLE 112 Did allocation failure alarm (continued)

Alarm	Did allocation failure
Attribute	"mvmold"="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.

NOTE

Refer to [Gr Interface Event](#) on page 270.

IPMI Alarms

NOTE

This section is not applicable for vSZ-H.

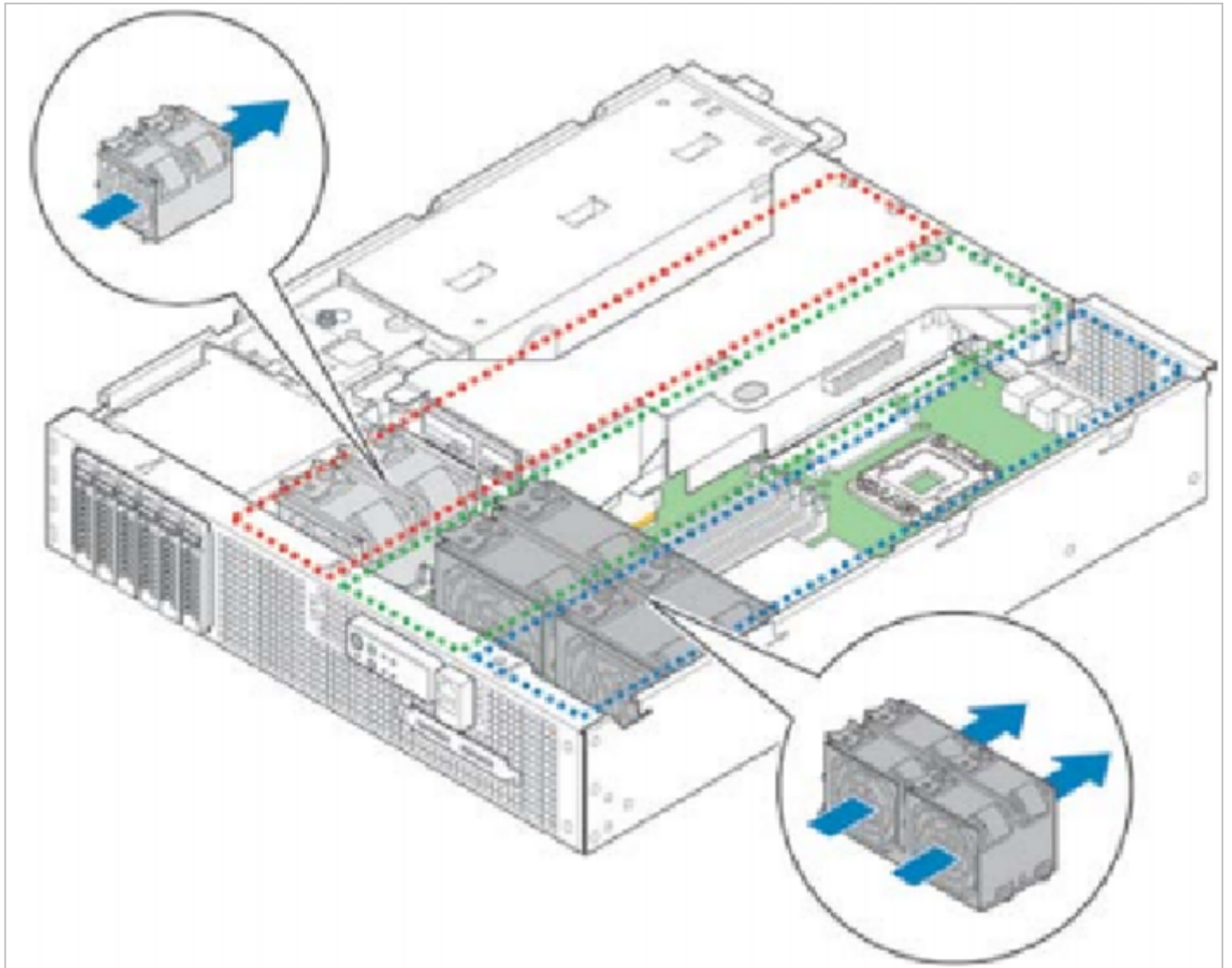
Following are the alarms related to IPMIs.

- [ipmiVoltage](#) on page 112
- [ipmiThempBB](#) on page 113
- [ipmiThempFP](#) on page 113
- [ipmiThempIOH](#) on page 114
- [ipmiThempMemP](#) on page 114
- [ipmiThempPS](#) on page 115
- [ipmiThempP](#) on page 115
- [ipmiThempHSBP](#) on page 115
- [ipmiFan](#) on page 116
- [ipmiPower](#) on page 116
- [ipmiCurrent](#) on page 117
- [ipmiFanStatus](#) on page 117
- [ipmiPsStatus](#) on page 117
- [ipmiDrvStatus](#) on page 118

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 113 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"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"

TABLE 113 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"> • Critical high - 66⁰ C • Non critical high - 61⁰ C • Non critical low - 10⁰ C • Critical low - 5⁰ C
Recommended Actions	Replace the power supply cord. If it does not work, the motherboard needs replacement.

ipmiThempBB

TABLE 114 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:xx"
Displayed on the web interface	Baseboard temperature [{status}] on control plane [{nodeMac}]
Description	<p>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 10⁰ Celsius to 61⁰ Celsius. The default threshold is 61⁰C.</p>
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiThempFP

TABLE 115 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:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}]

TABLE 115 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 ⁰ Celsius to 44 ⁰ Celsius. The default threshold is 44 ⁰ C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiThempIOH

TABLE 116 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: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 ⁰ Celsius to 5 ⁰ Celsius. The default threshold is 5 ⁰ C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiThempMemP

TABLE 117 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: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 ⁰ Celsius to 5 ⁰ Celsius. The default threshold is 5 ⁰ C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiThempPS

TABLE 118 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: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 ⁰ Celsius to 5 ⁰ Celsius. The default threshold is 5 ⁰ C.
Recommended Actions	Replace the power supply cord. If the problem persists, decrease the ambient temperature.

ipmiThempP

TABLE 119 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: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 ⁰ Celsius. The default threshold is 55 ⁰ C.
Recommended Actions	Check and replace the CPU fan module if required. Decrease the ambient temperature if the fan module is working.

ipmiThempHSBP

TABLE 120 ipmiThempHSBP alarm

Alarm	ipmiThempHSBP
Alarm Type	ipmiThempHSBP
Alarm Code	908
Severity	Major

TABLE 120 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: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 ^o Celsius to 55 ^o Celsius. The default threshold is 55 ^o C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiFan

TABLE 121 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: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 122 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: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.

TABLE 122 ipmiPower alarm (continued)

Alarm	ipmiPower
Recommended Actions	Replace the power supply cord.

ipmiCurrent

TABLE 123 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: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 124 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: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 125 ipmiPsStatus alarm

Alarm	ipmiPsStatus
Alarm Type	ipmiPsStatus
Alarm Code	913

TABLE 125 ipmiPsStatus alarm (continued)

Alarm	ipmiPsStatus
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:xx"
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 126 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: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.

NOTE

Refer to [IPMI Events](#) on page 277.

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 119
- [TTG session license exhausted](#) on page 119
- [License going to expire](#) on page 119
- [Insufficient license capacity](#) on page 120
- [Data plane DHCP IP license insufficient](#) on page 120

- [Data plane NAT session license insufficient](#) on page 121

TTG session critical threshold

TABLE 127 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 128 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 129 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.

TABLE 129 License going to expire alarm (continued)

Alarm	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 alarm is triggered when the validity of the license is going to expire.
Recommended Actions	Check the validity of licenses. You would need to purchase additional licenses if validity expires.

Insufficient license capacity

TABLE 130 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 131 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 132 Data pane NAT session license insufficient alarm

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

NOTE

Refer to [GUID-D48C7CC9-F644-424B-87BD-7E5D1096E1CC](#).

PMIPv6 Alarms

NOTE

This section is not applicable for vSZ-H.

Following are the alarms related to PMIPv6.

- [Config update failed](#) on page 121
- [DHCP connection lost](#) on page 122

Config update failed

TABLE 133 Config update failed alarm

Alarm	Config update failed
Alarm Type	updateCfgFailed
Alarm Code	5004
Severity	Major
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 logged when the PMIPv6 gets an error or a negative acknowledgment or improper/incomplete information from the D-bus client.

TABLE 133 Config update failed alarm (continued)

Alarm	Config update failed
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 is it is missing.

DHCP connection lost

NOTE

This alarm is not applicable for vSZ-H.

TABLE 134 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 logged 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.

NOTE

Refer to [PMIPv6 Events](#) on page 293.

SCI Alarms

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

- [Connect to SCI failure](#) on page 122
- [SCI has been disabled](#) on page 123
- [SCI and FTP have been disabled](#) on page 123

Connect to SCI failure

TABLE 135 Connect to SCI failure alarm

Alarm	Connect to SCI failure
Alarm Type	connectToSciFailure
Alarm Code	4003
Severity	Major

TABLE 135 Connect to SCI failure alarm (continued)

Alarm	Connect to SCI failure
Aggregation Policy	From the event code xxx 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 xxx.
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.
Recommended Actions	

SCI has been disabled

TABLE 136 SCI has been disabled alarm

Alarm	SCI has been disabled
Alarm Type	disabledSciDueToUpgrade
Alarm Code	4004
Severity	Warning
Aggregation Policy	From the event code xxx 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 xxx.
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 137 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 xxx 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 xxx.
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.
Recommended Actions	

NOTE

Refer to [Events Types](#) on page 139.

Session Alarms

NOTE

This section is not applicable for vSZ-H.

Following is the alarm related to session.

- [Binding failed](#) on page 124

Binding failed

TABLE 138 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", "ueIpAddr"="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 logged when the mobile node binding fails.
Recommended Actions	No action is required.

NOTE

Refer to [Session Events](#) on page 297.

System Alarms

Following are the alarms with the system log severity.

NOTE

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

- [No LS responses](#) on page 125
- [LS authentication failure](#) on page 125
- [{produce.short.name} failed to connect to LS](#) on page 126
- [Syslog server unreachable](#) on page 126
- [CSV export FTP maximum retry](#) on page 127
- [CSV export disk threshold exceeded](#) on page 127
- [CSV export disk max capacity reached](#) on page 127
- [Process restart](#) on page 128

- [Service unavailable](#) on page 128
- [Keepalive failure](#) on page 128
- [Resource unavailable](#) on page 129
- [GUID-7721D2C7-68C6-4747-B02E-0E33AADB6CAD](#)
- [Unconfirmed program detection](#) on page 129
- [GUID-0785E235-36A0-4794-B0DB-8F1687268E45](#)
- [Diameter peer transport failure](#) on page 130
- [Diameter CER error](#) on page 130
- [GUID-10D0B2FF-87AB-4AE1-A144-022CD2ED7898](#)
- [GUID-1372D30E-502C-46ED-9E57-4FCA250FCFF1](#)
- [GUID-23F896B3-DE65-42B1-93E2-24D0E6852634](#)
- [GUID-D12CD131-0DEC-4895-A2A4-6C84E18B1DD8](#)
- [GUID-C64C2AA3-9E32-4ABE-BE17-BF3F4CB2047E](#)
- [GUID-0A07D673-FD30-49C2-9C4A-0315D838B016](#)
- [GUID-729365BF-B4F0-475F-AD9B-C3E00E087A47](#)
- [Process initiated](#) on page 131
- [PMIPv6 unavailable](#) on page 131
- [Memory allocation failed](#) on page 132

No LS responses

TABLE 139 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 140 LS authentication failure alarm

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

TABLE 140 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 141 {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 142 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.xxx.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 143 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 144 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 145 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 145 CSV export disk max capacity reached alarm (continued)

Alarm	CSV export disk max capacity reached
Recommended Actions	

Process restart

TABLE 146 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 147 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 148 Keepalive failure alarm

Alarm	Keepalive failure
Alarm Type	keepAliveFailure

TABLE 148 Keepalive failure alarm (continued)

Alarm	Keepalive failure
Alarm Code	1003
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 mon/nc 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 149 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 br1 interface is running.

Unconfirmed program detection

TABLE 150 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]]

TABLE 150 Unconfirmed program detection alarm (continued)

Alarm	Unconfirmed program detection
Description	This alarm is triggered when the controller detects an unconfirmed program on the control plane.

Diameter peer transport failure

NOTE

This alarm is not applicable for vSZ-H.

TABLE 151 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 152 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.

TABLE 152 Diameter CER error alarm (continued)

Alarm	Diameter CER error
Recommended Actions	Check if the transport is up for the peer. Peer application may not be running.

Process initiated

NOTE

This alarm is not applicable for vSZ-H.

TABLE 153 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 logged 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 154 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 logged 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 155 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 logged when the memory allocation fails in the PMIPv6 process.
Recommended Actions	Check the PMIPv6d application log and status from the controller web interface.

NOTE

Refer to [System Alarms](#) on page 124.

The last one data plane is disconnected zone affinity profile alarm

TABLE 156 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"
Displayed on the web interface	The Last one Data Plane[{dpName}&&dpKey}] is disconnected Zone Affinity profile[{zoneAffinityProfileId}].
Description	This alarm is logged when the last data plane is disconnected from the zone affinity.
Recommended Actions	

NOTE

Refer to [System Events](#) on page 302.

Threshold Alarms

Following are the alarms related to threshold system set.

- [CPU threshold exceeded](#) on page 133
- [Memory threshold exceeded](#) on page 133
- [Disk usage threshold exceeded](#) on page 134
- [The drop of client count threshold exceeded](#) on page 134
- [License threshold exceeded](#) on page 135
- [Rate limit for TOR surpassed](#) on page 135
- [The number of users exceeded its limit](#) on page 136
- [The number of devices exceeded its limit](#) on page 136

CPU threshold exceeded

TABLE 157 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	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. Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.

Memory threshold exceeded

TABLE 158 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.

TABLE 158 Memory threshold exceeded alarm (continued)

Alarm	Memory threshold exceeded
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 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 159 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 160 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.

TABLE 160 The drop of client count threshold exceeded alarm (continued)

Alarm	The drop of client count threshold exceeded
Description	This alarm is triggered when client count drop exceeds the threshold limit.

License threshold exceeded

TABLE 161 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: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.

Rate limit for TOR surpassed

TABLE 162 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.
Auto Clearance	The alarm code is auto cleared with the event code 1301.
Attribute	"mvtold"="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", "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 163 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 164 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.

NOTE

Refer to [Threshold Events](#) on page 324.

Tunnel Alarms - Access Point

Following are the alarms related to tunnel.

- [AP softGRE gateway not reachable](#) on page 137
- [AP is disconnected from secure gateway](#) on page 137
- [AP secure gateway association failure](#) on page 137

AP softGRE gateway not reachable

TABLE 165 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"
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}]
Description	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 166 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 167 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}]

Alarm Types

Tunnel Alarms - Access Point

TABLE 167 AP secure gateway association failure alarm (continued)

Alarm	AP secure gateway association failure
Description	This alarm is triggered when the AP is unable to connect to the secure gateway.
Recommended Actions	No action required.

NOTE

Refer to [Tunnel Events - Access Point \(AP\)](#) on page 329.

Events Types

- 3rd Party Access Point Events..... 139
- Accounting Events..... 140
- AP Authentication Events..... 145
- AP Communication Events..... 150
- AP LBS Events..... 158
- AP Mesh Events..... 161
- AP State Change Events..... 168
- AP USB Events..... 185
- Authentication Events..... 185
- Authorization Events..... 193
- Control and Data Plane Interface..... 197
- Client Events..... 200
- Cluster Events..... 215
- Configuration Events..... 236
- Data Plane Events..... 242
- DHCP Events..... 256
- GA Interface Events..... 257
- Gn/S2a Interface Events..... 258
- Gr Interface Event..... 270
- IPMI Events..... 277
- Licensing Interface Events..... 286
- Location Delivery Events..... 292
- PMIPv6 Events..... 293
- SCI Events..... 295
- Session Events..... 297
- STA Interface Events..... 300
- System Events..... 302
- Switch Events..... 323
- Threshold Events..... 324
- Tunnel Events - Access Point (AP)..... 329
- Tunnel Events - Data Plane..... 334

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 139

3rd party AP connected

TABLE 168 3rdparty AP connected event

Event	3rd party AP connected
Event Type	3rdPartyAPConnected

TABLE 168 3rdparty AP connected event (continued)

Event	3rd party AP connected
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 140
- [Accounting server not reachable](#) on page 141
- [Accounting failed over to secondary](#) on page 141
- [Accounting fallback to primary](#) on page 142
- [AP accounting message mandatory parameter missing](#) on page 142
- [Unknown realm](#) on page 142
- [AP accounting message decode failed](#) on page 143
- [AP accounting retransmission message dropped](#) on page 143
- [AP accounting response while invalid config](#) on page 144
- [AP account message drop while no accounting start message](#) on page 144
- [Unauthorized COA/DM message dropped](#) on page 145

Accounting session disabled

NOTE

This event is not applicable for vSZ-H.

TABLE 169 Accounting session disabled event

Event	Accounting session disabled
Event Type	accSessDisabled
Event Code	1234
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" "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}]

TABLE 169 Accounting session disabled event (continued)

Event	Accounting session disabled
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 170 Accounting server not reachable event

Event	Accounting server not reachable
Event Type	accSrvrNotReachable
Event Code	1602
Severity	Major
Attribute	"mvnold"="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 171 Accounting failed over to secondary event

Event	Accounting failed over to secondary
Event Type	accFailedOverToSecondary
Event Code	1653
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 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 172 Accounting fallback to primary event

Event	Accounting fallback to primary
Event Type	accFallbackToPrimary
Event Code	1654
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 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 173 AP accounting message mandatory parameter missing event

Event	AP accounting message mandatory parameter missing
Event Type	apAcctMsgMandatoryPrmMissing
Event Code	1901
Severity	Critical
Attribute	"mvsold"="12","wlanId"="1","zoned"="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 174 Unknown realm event

Event	Unknown realm
Event Type	unknownRealmAccounting

TABLE 174 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 175 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 176 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", "ueMsi"="12345", "ueMsisdn"="98787" "apIpAddress"="10.1.4.11"

TABLE 176 AP accounting retransmission message dropped event (continued)

Event	AP accounting retransmission message dropped
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.
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 177 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,"zoneld"="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 178 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,"zoneld"="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 179 Unauthorized COA/DM message dropped event

Event	Unauthorized COA/DM message dropped
Event Type	unauthorizedCoaDmMessageDropped
Event Code	1911
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", "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.

NOTE

Refer to [Accounting Alarms](#) on page 59.

AP Authentication Events

Following are the events related to authentication.

- [Radius server reachable](#) on page 146
- [Radius server unreachable](#) on page 146
- [LDAP server reachable](#) on page 146
- [LDAP server unreachable](#) on page 147
- [AD server reachable](#) on page 147
- [AD server unreachable](#) on page 147
- [Wechat ESP authentication server reachable](#) on page 148
- [WeChat ESP authentication server unreachable](#) on page 148
- [WeChat ESP authentication server resolvable](#) on page 148
- [WeChat ESP authentication server unresolvable](#) on page 149
- [WeChat ESP DNAT server reachable](#) on page 149
- [WeChat ESP DNAT server unreachable](#) on page 149
- [WeChat ESP DNAT server resolvable](#) on page 150
- [WeChat ESP DNAT server unresolvable](#) on page 150

Radius server reachable

TABLE 180 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 181 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 182 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 183 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 184 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 185 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 186 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 187 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 188 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 189 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 190 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 191 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

WeChat ESP DNAT server resolvable

TABLE 192 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 193 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

NOTE

Refer to [AP Authentication Alarms](#) on page 63.

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 151
- [AP managed](#) on page 151
- [AP rejected](#) on page 152
- [AP firmware updated](#) on page 152
- [AP firmware update failed](#) on page 152
- [Updating AP firmware](#) on page 153

- [Updating AP configuration](#) on page 153
- [AP configuration updated](#) on page 153
- [AP configuration update failed](#) on page 153
- [AP pre-provision model mismatched](#) on page 154
- [AP swap model mismatched](#) on page 154
- [AP WLAN oversubscribed](#) on page 154
- [AP join zone failed](#) on page 155
- [AP illegal to change country code](#) on page 155
- [AP configuration get failed](#) on page 155
- [Rogue AP](#) on page 156
- [SSID-spoofing rogue AP](#) on page 156
- [MAC-spoofing rogue AP](#) on page 156
- [Same-network rogue AP](#) on page 157
- [Ad-hoc network device](#) on page 157
- [Rogue AP disappeared](#) on page 157
- [Classified Rogue AP](#) on page 158
- [AP image signing failed](#) on page 158

AP discovery succeeded

TABLE 194 AP discovery succeeded event

Event	AP discovery succeeded
Event Type	apDiscoverySuccess
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 195 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 196 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 197 AP firmware updated event

Event	AP firmware updated
Event Type	apFirmwareUpdated
Event Code	106
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}] 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 198 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 199 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 200 Updating AP configuration event

Event	Updating AP configuration
Event Type	apConfApplying
Event Code	109
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234"
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 201 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 202 AP configuration update failed event

Event	AP configuration update failed
Event Type	apConfUpdateFailed
Event Code	111

TABLE 202 AP configuration update failed event (continued)

Event	AP configuration update failed
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 203 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]
Description	This event occurs when the AP model differs from the configuration model.

AP swap model mismatched

TABLE 204 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 205 AP WLAN oversubscribed event

Event	AP WLAN oversubscribed
Event Type	apWlanOversubscribed
Event Code	114

TABLE 205 AP WLAN oversubscribed event (continued)

Event	AP WLAN oversubscribed
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 wlans. 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 206 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.

AP illegal to change country code

TABLE 207 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 208 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"

TABLE 208 AP configuration get failed event (continued)

Event	AP configuration get failed
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 209 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"="xxxxxxxxxx", "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.

SSID-spoofing rogue AP

TABLE 210 SSID-spoofing rogue AP event

Event	SSID-spoofing rogue AP
Event Type	ssid-spoofingRogueAPDetected
Event Code	181
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxxxx", "channel"="xx"
Displayed on the web interface	SSID-spoofing AP[{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}].
Description	This event occurs when the AP detects a rogue AP with the same service set identifier (SSID).

MAC-spoofing rogue AP

TABLE 211 MAC-spoofing rogue AP event

Event	MAC-spoofing rogue AP
Event Type	mac-spoofingRogueAPDetected
Event Code	182
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxxxx", "channel"="xx"
Displayed on the web interface	MAC-spoofing AP[{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}].

TABLE 211 MAC-spoofing rogue AP event (continued)

Event	MAC-spoofing rogue AP
Description	This event occurs when the AP detects a rogue AP having the same basic service set identifier (BSSID).

Same-network rogue AP

TABLE 212 Same-network rogue AP event

Event	Same-network rogue AP
Event Type	same-networkRogueAPDetected
Event Code	183
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxx", "channel"="xx"
Displayed on the web interface	Same-network AP[{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}]
Description	This event occurs when the AP detects a rogue AP which has the same network.

Ad-hoc network device

TABLE 213 Ad-hoc network rogue device event

Event	Ad-hoc network device
Event Type	ad-hoc-networkRogueAPDetecte
Event Code	184
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxx", "channel"="xx"
Displayed on the web interface	Ad-hoc network device[{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}]
Description	This event occurs when the AP detects an ad-hoc network device.

Rogue AP disappeared

TABLE 214 Rogue AP disappeared event

Event	Rogue AP disappeared
Event Type	maliciousRogueAPTimeout
Event Code	185
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 215 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 216 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.

NOTE

Refer to [AP Communication Alarms](#) on page 67.

AP LBS Events

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

- [No LS responses](#) on page 159
- [LS authentication failure](#) on page 159
- [AP connected to LS](#) on page 159
- [AP failed to connect to LS](#) on page 159
- [AP started location service](#) on page 160
- [AP stopped location service](#) on page 160
- [AP received passive calibration request](#) on page 160
- [AP received passive footfall request](#) on page 161
- [AP received unrecognized request](#) on page 161

No LS responses

TABLE 217 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 218 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 219 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 220 AP failed to connect to LS event

Event	AP failed to connect to LS
Event Type	apLBSConnectFailed

TABLE 220 AP failed to connect to LS event (continued)

Event	AP failed to connect to LS
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 221 AP started location service event

Event	AP started location service
Event Type	apLBSStartLocationService
Event Code	705
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 222 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 223 AP received passive calibration request event

Event	AP received passive calibration request
Event Type	apLBSRcvdPassiveCalReq
Event Code	707
Severity	Informational

TABLE 223 AP received passive calibration request event (continued)

Event	AP received passive calibration request
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 224 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 225 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.

NOTE

Refer to [AP LBS Alarms](#) on page 71.

AP Mesh Events

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

- [EMAP downlink connected to MAP](#) on page 162
- [EMAP downlink disconnected from MAP](#) on page 162
- [EMAP uplink connected to MAP](#) on page 163
- [EMAP uplink disconnected from MAP](#) on page 163
- [MAP disconnected](#) on page 163

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

EMAP downlink connected to MAP

TABLE 226 EMAP downlink connected to MAP event

Event	EMAP downlink connected to MAP
Event Type	emapDlinkConnectWithMap
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 227 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 228 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 229 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}}]
Description	This event occurs when Ethernet Mesh AP uplink disconnects from MAP.

MAP disconnected

TABLE 230 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 231 MAP downlink connected event

Event	MAP downlink connected
Event Type	mapDlinkConnected
Event Code	412
Severity	Informational

TABLE 231 MAP downlink connected event (continued)

Event	MAP downlink connected
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 232 MAP downlink connected to EMAP event

Event	MAP downlink connected to EMAP
Event Type	mapDlinkConnectWithMap
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 233 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 234 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 235 MAP uplink connected to EMAP event

Event	MAP uplink connected to EMAP
Event Type	mapUlinkConnectToeMap
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 236 MAP uplink disconnected from EMAP event

Event	MAP uplink disconnected from EMAP
Event Type	mapUlinkDisconnectToeMap
Event Code	418
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 237 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 238 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 239 Mesh state updated to MAP event

Event	Mesh state updated to MAP
Event Type	meshStateUpdateToMap
Event Code	421
Severity	Informational
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 240 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 241 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 242 Mesh state update to RAP no channel event

Event	Mesh state update to RAP no channel
Event Type	meshStateUpdateToRapNoChannel
Event Code	424
Severity	Informational
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 243 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 244 MAP downlink disconnected from MAP event

Event	MAP downlink disconnected from MAP
Event Type	mapDlinkDisconnectWithMap
Event Code	426

TABLE 244 MAP downlink disconnected from MAP event (continued)

Event	MAP downlink disconnected from MAP
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 245 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
AP rebooted by user on page 169	AP rebooted by system on page 169	AP disconnected on page 169
AP IP address updated on page 170	AP reset to factory default on page 170	AP channel updated on page 170
AP country code updated on page 171	AP channel updated because dynamic frequency selection (DFS) detected a radar on page 171	AP change control plane on page 171
AP connected on page 172	AP deleted on page 172	AP heartbeat lost on page 172
AP tagged as critical on page 173	AP cable modem interface down on page 173	AP brownout on page 173
AP cable modem power-cycled by user on page 173	AP smart monitor turn off WLAN on page 174	AP client load balancing limit reached on page 174
AP client load balancing limit recovered on page 174	AP WLAN state changed on page 175	AP capacity reached on page 175
AP capacity recovered on page 175	AP cable modem interface up on page 176	AP cable modem soft-rebooted by user on page 176
AP cable modem set to factory default by user on page 176	AP health high latency flag on page 177	AP health low capacity flag on page 177
AP health high connection failure flag on page 177	AP health high client count flag on page 178	AP health high latency clear on page 178
AP health low capacity clear on page 178	AP health high connection failure clear on page 179	AP health high client count clear on page 179
Primary DHCP AP is down on page 179	Primary DHCP AP is up on page 180	Secondary DHCP AP is down on page 180

Event	Event	Event
Secondary DHCP AP is up on page 180	Primary or secondary DHCP AP detects 90% of the configured total IPs on page 181	Both primary and secondary DHCP server APs are down on page 181
AP NAT gateway IP failover detected for particular VLAN pool on page 181	AP NAT gateway IP fall back detected for particular VLAN pool on page 182	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 on page 182
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 on page 182	AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down on page 183	AP health high airtime utilization flag on page 183
AP health high airtime utilization clear on page 184	AP cluster failover on page 184	AP cluster rehome on page 184

AP rebooted by user

TABLE 246 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"
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 247 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 248 AP disconnected event

Event	AP disconnected
Event Type	apConnectionLost (detected on the server)
Event Code	303
Severity	Major

TABLE 248 AP disconnected event (continued)

Event	AP disconnected
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 249 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.

AP reset to factory default

TABLE 250 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 251 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}]

TABLE 251 AP channel updated event (continued)

Event	AP channel updated
Description	This event occurs when the AP detects the radio interference and switches to another channel.

AP country code updated

TABLE 252 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 253 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
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 254 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"

TABLE 254 AP change control plane event (continued)

Event	AP change control plane
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 255 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 256 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"
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 257 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 258 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 259 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 260 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 261 AP cable modem power-cycled by user event

Event	AP cable modem power-cycled by user
Event Type	cmRebootByUser
Event Code	318

TABLE 261 AP cable modem power-cycled by user event (continued)

Event	AP cable modem power-cycled by user
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 262 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 263 AP client load balancing limit reached event

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

Event	AP client load balancing limit recovered
Event Type	apCLBlimitRecovered
Event Code	321
Severity	Informational

TABLE 264 AP client load balancing limit recovered event (continued)

Event	AP client load balancing limit recovered
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 265 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 266 AP capacity reached event

Event	AP capacity reached
Event Type	apCapacityReached
Event Code	323
Severity	Informational
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 267 AP capacity recovered event

Event	AP capacity recovered
Event Type	apCapacityRecovered
Event Code	324
Severity	Informational

TABLE 267 AP capacity recovered event (continued)

Event	AP capacity recovered
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 268 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 269 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 270 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.

NOTE

Refer to [AP State Change Alarms](#) on page 72.

AP health high latency flag

TABLE 271 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 272 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 273 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 274 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 275 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.

AP health low capacity clear

TABLE 276 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 277 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 278 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 279 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 280 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 281 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.

Secondary DHCP AP is up

TABLE 282 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 283 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	apDHCIPIPPoolMaxThresholdReached
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 284 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 285 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
Event Code	342
Severity	Major
Attribute	"natGatewayIP"="10.1.2.2", "vlanId"="2", "natGatewayMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx: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 286 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:xx", "apMac"="xx: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 287 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", "natGatewayIP3"= 192.168.10.4", "vlanId"="2", "apMac"="xx: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 288 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

TABLE 288 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 (continued)

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
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 289 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 290 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}].
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 291 AP health high airtime utilization clear event

Event	AP health high airtime utilization clear
Event Type	apHealthAirUtilizationClear
Event Code	348
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}}] 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 292 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 293 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}}].
Description	This event occurs when an AP is rehomed from a standby to a primary cluster.

NOTE

Refer to [AP State Change Alarms](#) on page 72.

AP USB Events

Following are the events related to AP USB (Universal Serial Bus).

- [AP USB software package downloaded](#) on page 185
- [AP USB software package download failed](#) on page 185

AP USB software package downloaded

TABLE 294 AP USB software package downloaded event

Event	AP USB software package downloaded
Event Type	apUsbSoftwarePackageDownloaded
Event Code	370
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 295 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 186
- [Unknown realm](#) on page 186
- [Authentication succeeded](#) on page 187
- [Authentication failed](#) on page 187
- [Pseudonym authentication succeeded](#) on page 187
- [Pseudonym authentication failed](#) on page 188
- [Fast re-authentication succeeded](#) on page 188
- [Fast re-authentication failed](#) on page 189

Events Types

Authentication Events

- [Authentication failed over to secondary](#) on page 189
- [Authentication fallback to primary](#) on page 190
- [AD/LDAP connected successfully](#) on page 190
- [AD/LDAP connectivity failure](#) on page 190
- [Bind fails with AD/LDAP](#) on page 191
- [Bind success with LDAP, but unable to find clear text password for the user](#) on page 191
- [RADIUS fails to connect to AD NPS server](#) on page 191
- [RADIUS fails to authenticate with AD NPS server](#) on page 192
- [Successfully established the TLS tunnel with AD/LDAP](#) on page 192
- [Fails to establish TLS tunnel with AD/LDAP](#) on page 192

Authentication server not reachable

TABLE 296 Authentication server not reachable event

Event	Authentication server not reachable
Event Type	authSvrNotReachable
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" "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 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 297 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 298 Authentication succeeded event

Event	Authentication succeeded
Event Type	authSuccess
Event Code	1604
Severity	Debug
Attribute	"mvsold"=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 299 Authentication failed event

Event	Authentication failed
Event Type	authFailed
Event Code	1605
Severity	Debug
Attribute	"mvsold"=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	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 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 300 Pseudonym authentication succeeded event

Event	Pseudonym authentication succeeded
Event Type	pseudonymAuthSuccess
Event Code	1606
Severity	Debug
Attribute	"mvsold"=12 "wlanId"=1,"zoneId"=10" ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org"

TABLE 300 Pseudonym authentication succeeded event (continued)

Event	Pseudonym authentication succeeded
	"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	Pseudonym ID based 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 is applicable when the controller acts as a host AAA server and is applicable only for TTG/PDG session. Note: The attribute Pseudonym ID is used for authentication.

Pseudonym authentication failed

NOTE

This event is not applicable for vSZ-H.

TABLE 301 Pseudonym authentication failed event

Event	Pseudonym authentication failed
Event Type	pseudonymAuthFailed
Event Code	1607
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" "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). Note: The attribute Pseudonym ID is used for authentication.

Fast re-authentication succeeded

NOTE

This event is not applicable for vSZ-H.

TABLE 302 Fast re-authentication succeeded event

Event	Fast re-authentication succeeded
Event Type	fastReauthSuccess
Event Code	1608
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"

TABLE 302 Fast re-authentication succeeded event (continued)

Event	Fast re-authentication succeeded
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. Note: FastReauth ID is used for authentication.

Fast re-authentication failed

NOTE

This event is not applicable for vSZ-H.

TABLE 303 Fast re-authentication failed event

Event	Fast re-authentication failed
Event Type	fastReauthFailed
Event Code	1609
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" "cause"="<Cause of failure>" "authType"="EAP-SIM/ AKA"
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). Note: Attribute FastReauthID is used for reauthentication.

Authentication failed over to secondary

TABLE 304 Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651
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 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 305 Authentication fallback to primary event

Event	Authentication fallback to primary
Event Type	authFallbackToPrimary
Event Code	1652
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 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 306 AD/LDAP connected successfully event

Event	AD/LDAP connected successfully
Event Type	racADLDAPSuccess
Event Code	1751
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvIp"= "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[{authSrvIp}] successfully from SCG[{SCGMgmtIp}]
Description	This event occurs when RADIUS connection to AD/LDAP server is successful.

AD/LDAP connectivity failure

TABLE 307 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", "mvnold"=12, "srcProcess"="RAC", "authSrvIp"="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[{authSrvIp}] fails from SCG[{SCGMgmtIp}]
Description	This event occurs when RADIUS fails to connect to AD/LDAP server.

Bind fails with AD/LDAP

TABLE 308 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", "mvnold"=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 309 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
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 310 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 311 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 312 Successfully established the TLS tunnel with AD/LDAP event

Event	Successfully established the TLS tunnel with AD/LDAP
Event Type	racADNPSFailToAuthenticate
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 313 Fails to establish TLS tunnel with AD/LDAP event

Event	Fails to establish TLS tunnel with AD/LDAP
Event Type	racADLDAPTLSTLSFailed
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.

NOTE

Refer to [Authentication Alarms](#) on page 76.

Authorization Events

The following are the events related to authorization (DM/CoA).

- [DM received from AAA](#) on page 193
- [DM NACK sent to AAA](#) on page 193
- [DM sent to NAS](#) on page 194
- [DM NACK received from NAS](#) on page 194
- [CoA received from AAA](#) on page 194
- [CoA NACK sent to AAA](#) on page 195
- [CoA sent NAS](#) on page 195
- [CoA NAK received NAS](#) on page 195
- [CoA authorize only access reject](#) on page 196
- [CoA RWSG MWSG notification failure](#) on page 196

DM received from AAA

TABLE 314 DM received from AAA event

Event	DM received from AAA
Event Type	dmRcvdAAA
Event Code	1641
Severity	Debug
Attribute	"mvpnoid"="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 315 DM NACK sent to AAA event

Event	DM NACK sent to AAA
Event Type	dmNackSntAAA
Event Code	1642
Severity	Debug
Attribute	"mvpnoid"="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"

TABLE 315 DM NACK sent to AAA event (continued)

Event	DM NACK sent to AAA
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 316 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 317 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 318 CoA received from AAA event

Event	CoA received from AAA
Event Type	coaRcvdAAA
Event Code	1645
Severity	Debug

TABLE 318 CoA received from AAA event (continued)

Event	CoA received from AAA
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 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 319 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 320 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 321 CoA NAK received NAS event

Event	CoA NAK received NAS
Event Type	coaNakRcvdNas
Event Code	1648

TABLE 321 CoA NAK received NAS event (continued)

Event	CoA NAK received NAS
Severity	Debug
Attribute	"mvpold"="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 322 CoA authorize only access reject event

Event	CoA authorize only access reject
Event Type	coaAuthorizeOnlyAccessReject
Event Code	1649
Severity	Critical
Attribute	"mvpold"="12" "wlanId"="1", "zoneld"="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 323 CoA RWSG MWSG notification failure event

Event	CoA RWSG MWSG notification failure
Event Type	coaRWSGMWSGNotifFailure
Event Code	1650
Severity	Major
Attribute	mvpold"=12 "wlanId"=1 "zoneld"="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 197
- [GtpManager \(DP\) disconnected](#) on page 197
- [Session updated at DP](#) on page 198
- [Session update at DP failed](#) on page 198
- [Session deleted at DP](#) on page 198
- [Session delete at DP failed](#) on page 199
- [C2d configuration failed](#) on page 199

DP connected

TABLE 324 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 325 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 326 Session updated at DP event

Event	Session updated at DP
Event Type	sessUpdatedAtDblade
Event Code	1205
Severity	Debug
Attribute	"mvpnold"="12", "wlanId"="1", "zoneld"="10", "srcProcess"="aut", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "realm"="realm sent by UE", "ctrlBladelp"="1.1.1.1", "dataBladelp"="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 [{dataBladelp}] by Control plane [{ctrlBladelp}] 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 327 Session update at DP failed event

Event	Session update at DP failed
Event Type	sessUpdateErrAtDblade
Event Code	1206
Severity	Debug
Attribute	"mvpnold"="12", "wlanId"="1", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "zoneld"="10", "realm"="realm sent by UE", "ctrlBladelp"="1.1.1.1", "dataBladelp"="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 [{dataBladelp}] by Control plane [{ctrlBladelp}] 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 328 Session deleted at DP event

Event	Session deleted at DP
Event Type	sessDeletedAtDblade
Event Code	1207
Severity	Debug
Attribute	"mvpnold"="12", "wlanId"="1", "zoneld"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="realm sent

TABLE 328 Session deleted at DP event (continued)

Event	Session deleted at DP
	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 329 Session delete at DP failed event

Event	Session delete at DP failed
Event Type	sessDeleteErrAtDblade
Event Code	1208
Severity	Debug
Attribute	"mvnold"="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 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 330 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.

NOTE

Refer to [Control and Data Plane Interface](#) on page 197.

Client Events

All client events from the AP will be appended with tenant ID ("tenantUUID":"xxxxx"). Following are the events related to clients.

- [Client authentication failed](#) on page 201
- [Client joined](#) on page 201
- [Client failed to join](#) on page 201
- [Client disconnected](#) on page 202
- [Client connection timed out](#) on page 202
- [Client authorization successfully](#) on page 203
- [Client authorization failed](#) on page 203
- [Client session expired](#) on page 203
- [Client roaming](#) on page 204
- [Client logged out](#) on page 204
- [3rd party client join](#) on page 204
- [3rd party client inactivity timeout](#) on page 205
- [3rd party client authorization](#) on page 205
- [3rd party client authorization failure](#) on page 205
- [3rd party client session expiration](#) on page 206
- [3rd party client roaming](#) on page 206
- [3rd party client session logout](#) on page 207
- [Client roaming disconnected](#) on page 207
- [Client blocked](#) on page 207
- [Client grace period](#) on page 208
- [Onboarding registration succeeded](#) on page 208
- [Onboarding registration failed](#) on page 208
- [Remediation succeeded](#) on page 209
- [Remediation failed](#) on page 209
- [Force DHCP disconnected](#) on page 209
- [WDS device joined](#) on page 210
- [WDS device left](#) on page 210
- [Client is blocked because of barring UE rule](#) on page 210
- [Client is unblocked by barring UE rule](#) on page 211
- [Start CALEA mirroring client](#) on page 211
- [Stop CALEA mirroring client](#) on page 211
- [Wired client joined](#) on page 212
- [Wired client failed to join](#) on page 212
- [Wired client disconnected](#) on page 212
- [Wired client authorization successfully](#) on page 213
- [Wired client session expired](#) on page 213

- [Application identified](#) on page 213
- [Application denied](#) on page 214
- [URL filtering server unreachable](#) on page 214
- [URL filtering server reachable](#) on page 214

Client authentication failed

TABLE 331 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.
Description	This event occurs when the client fails to join WLAN on the AP due to an authentication failure.

Client joined

TABLE 332 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 333 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"

TABLE 333 Client failed to join event (continued)

Event	Client failed to join
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 334 Client disconnected event

Event	Client disconnected
Event Type	clientDisconnect
Event Code	204
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] 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 335 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", "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"="", "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 336 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.
Description	This event occurs when the client on WLAN AP is authorized.

Client authorization failed

TABLE 337 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 338 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 339 Client roaming event

Event	Client roaming
Event Type	clientRoaming
Event Code	209
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	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 340 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 341 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}]

TABLE 341 3rd party client join event (continued)

Event	3rd party client join
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 342 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 343 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 344 3rd party client authorization failure event

Event	3rd party client authorization failure
Event Type	3rdPtyClientAuthorizationFailure

TABLE 344 3rd party client authorization failure event (continued)

Event	3rd party client authorization failure
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"
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 345 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 346 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 347 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 log out.

Client roaming disconnected

TABLE 348 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", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "wlanId"="", "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 349 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 349 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 350 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 351 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"="xxx", "groupName"="xxxx", "vlanId"="xxxx", "osType"="xxxx", "userAgent"="xxxx"
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 352 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",

TABLE 352 Onboarding registration failed event (continued)

Event	Onboarding registration failed
	"apLocation"="xxxx", "groupName"="xxxx", "vlanId"="xxxx", "osType"="xxxx", "userAgent"="xxxx", "reason"="xxxxx"
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 353 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 354 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 355 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"="", "vlanId"="xxxxx", "tenantUID"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "vlanId"="", "radio"="", "encryption"=""

TABLE 355 Force DHCP disconnected event (continued)

Event	Force DHCP disconnected
Displayed on the web interface	Client [{userName} IP clientMac] disconnected from WLAN [{ssid}] on AP [{apName}&&apMac] due to force-dhcp.
Description	This event occurs when the client disconnects by force from the dynamic host configuration protocol.

WDS device joined

TABLE 356 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", "wdsDevicetMac"="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 357 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", "wdsDevicetMac"="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 358 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
Attr ibute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"

TABLE 358 Client is blocked because of barring UE rule event (continued)

Event	Client is blocked because of barring UE rule
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 temporally blocked by the UE barring rule.

Client is unblocked by barring UE rule

TABLE 359 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 360 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 361 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}].

TABLE 361 Stop CALEA mirroring client event (continued)

Event	Stop CALEA mirroring client
Description	This event occurs when CALEA stops mirroring the client image.

Wired client joined

TABLE 362 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"="xxxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxxx", "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 363 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"="xxxx", "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 364 Wired client disconnected event

Event	Wired client disconnected
Event Type	wiredClientDisconnect
Event Code	2804
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"

TABLE 364 Wired client disconnected event (continued)

Event	Wired client disconnected
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 365 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", "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 366 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 367 Application identified event

Event	Application identified
Event Type	application of user is identified
Event Code	8001
Severity	Informational

TABLE 367 Application identified event (continued)

Event	Application identified
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 368 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 369 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 370 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.

Cluster Events

Following are the events related to clusters.

Event	Event	Event
Cluster created successfully on page 215	New node joined successfully on page 216	New node failed to join on page 216
Node removal completed on page 216	Node removal failed on page 217	Node out of service on page 217
Cluster in maintenance state on page 217	Cluster back in service on page 218	Cluster backup completed on page 218
Cluster backup failed on page 218	Cluster restore completed on page 219	Cluster restore failed on page 219
Cluster node upgrade completed on page 219	Entire cluster upgraded successfully on page 220	Cluster upgrade failed on page 220
Cluster application stopped on page 220	Cluster application started on page 221	Cluster backup started on page 221
Cluster upgrade started on page 221	Cluster leader changed on page 221	Node bond interface down on page 222
Node bond interface up on page 222	Node IP address changed on page 222	Node physical interface down on page 223
Node physical interface up on page 223	Cluster node rebooted on page 223	NTP time synchronized on page 224
Cluster node shutdown on page 224	Cluster upload started on page 224	Cluster upload completed on page 225
Cluster upload failed on page 225	SSH tunnel switched on page 225	Cluster remove node started on page 225
Node back in service on page 226	Disk usage exceed threshold on page 226	Cluster out of service on page 226
Initiated moving APs in node to a new cluster on page 227	Cluster upload vSZ-D firmware started on page 227	Cluster upload vSZ-D firmware completed on page 227
Cluster upload vSZ-D firmware failed on page 228	Cluster upload AP firmware started on page 228	Cluster upload AP firmware completed on page 228
Cluster upload AP firmware failed on page 229	Cluster add AP firmware started on page 229	Cluster add AP firmware completed on page 229
Cluster add AP firmware failed on page 229	Cluster name is changed on page 230	Unsync NTP Time on page 230
Cluster upload KSP file started on page 230	Cluster upload KSP file completed on page 231	Cluster upload KSP file failed on page 231
Configuration backup started on page 231	Configuration backup succeeded on page 232	Configuration backup failed on page 232
Configuration restore succeeded on page 232	Configuration restore failed on page 233	AP Certificate Expired on page 233
AP Certificate Updated on page 233	Configuration restore started on page 234	Upgrade SSTable failed on page 234
Reindex elastic search finished on page 234	Initiated APs contact APR on page 234	All nodes back in service on page 235
Not management service ready on page 235	Management service ready on page 235	Configuration sync failed on page 236
Node IPv6 address deleted on page 236	Node IPv6 address added on page 236	

Cluster created successfully

TABLE 371 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}]

TABLE 371 Cluster created successfully event (continued)

Event	Cluster created successfully
Description	This event occurs when a cluster and a node are created.

New node joined successfully

TABLE 372 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 373 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 374 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}]

TABLE 374 Node removal completed event (continued)

Event	Node removal completed
Description	This event occurs when a node is removed from the cluster session.

Node removal failed

TABLE 375 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 376 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 377 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

TABLE 377 Cluster in maintenance state event (continued)

Event	Cluster 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 378 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 379 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 380 Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810
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 381 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 382 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 383 Cluster node upgrade completed event

Event	Cluster node upgrade completed
Event Type	upgradeClusterNodeSuccess
Event Code	813
Severity	Informational
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 384 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 385 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 386 Cluster application stopped event

Event	Cluster application stopped
Event Type	clusterAppStop
Event Code	816
Severity	Critical
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 387 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 388 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 389 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",
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 390 Cluster leader changed event

Event	Cluster leader changed
Event Type	clusterLeaderChanged

TABLE 390 Cluster leader changed event (continued)

Event	Cluster leader changed
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 391 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 392 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 393 Node IP address changed event

Event	Node IP address changed
Event Type	nodeIPChanged
Event Code	823
Severity	Informational

TABLE 393 Node IP address changed event (continued)

Event	Node IP address changed
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 394 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 395 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 396 Cluster node rebooted event

Event	Cluster node rebooted
Event Type	nodeRebooted
Event Code	826
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

TABLE 396 Cluster node rebooted event (continued)

Event	Cluster node rebooted
Description	This event occurs when the node, belonging to a cluster reboots.

NTP time synchronized

TABLE 397 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 398 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 399 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}].
Description	This event occurs when the cluster upload process starts.

Cluster upload completed

TABLE 400 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 401 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 402 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 403 Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834

TABLE 403 Cluster remove node started event (continued)

Event	Cluster remove node started
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 404 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 405 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 406 Cluster out of service event

Event	Cluster out of service
Event Type	clusterOutOfService
Event Code	843
Severity	Critical
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.

TABLE 406 Cluster out of service event (continued)

Event	Cluster 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 407 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 408 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 409 Cluster upload vSZ-D firmware completed event

Event	Cluster upload vSZ-D firmware completed
Event Type	uploadClusterVDPFirmwareSuccess
Event Code	846
Severity	Informational
Attribute	"clusterName"="xxx" "status"="StartTime:yyyy-MM-dd hh:mm:ss, EndTime:yyyy-MM-dd hh:mm:ss, Duration:hh:mm:ss"

TABLE 409 Cluster upload vSZ-D firmware completed event (continued)

Event	Cluster upload vSZ-D firmware completed
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 410 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 411 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 412 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 413 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 414 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 415 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 416 Cluster add AP firmware failed event

Event	Cluster add AP firmware failed
Event Type	clusterAddAPFirmwareFailed
Event Code	853

TABLE 416 Cluster add AP firmware failed event (continued)

Event	Cluster add AP firmware failed
Severity	Major
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 417 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 (Configuration > System > Event Management) 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 418 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 419 Cluster upload KSP file started event

Event	Cluster upload KSP file started
Event Type	clusterUploadKspFileStart
Event Code	856

TABLE 419 Cluster upload KSP file started event (continued)

Event	Cluster upload KSP file started
Severity	Informational
Attribute	"clusterName"="xxx",
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 420 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 421 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.

Configuration backup started

TABLE 422 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.

TABLE 422 Configuration backup started event (continued)

Event	Configuration backup started
Description	This event occurs when cluster configuration backup starts.

Configuration backup succeeded

TABLE 423 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 424 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 425 Configuration restore succeeded event

Event	Configuration restore succeeded
Event Type	clusterCfgRestoreSuccess
Event Code	863
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 426 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 427 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 428 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.
Description	This event occurs when the AP certificates are updated.

Configuration restore started

TABLE 429 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 430 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 431 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 432 Initiated APs contact APR event

Event	Initiated APs contact APR
Event Type	clusterInitContactApr
Event Code	870
Severity	Major

TABLE 432 Initiated APs contact APR event (continued)

Event	Initiated APs contact APR
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 433 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 434 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 435 Management service ready event

Event	Managementl service ready
Event Type	allServiceInService
Event Code	873
Severity	Informational
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 436 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 437 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.

Node IPv6 address deleted

TABLE 438 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.

NOTE

Refer to [Cluster Alarms](#) on page 81.

Configuration Events

Following are the events related to configuration.

- [Configuration updated](#) on page 237

- [Configuration update failed](#) on page 237
- [Configuration receive failed](#) on page 238
- [Incorrect flat file configuration](#) on page 238
- [Zone configuration preparation failed](#) on page 238
- [AP configuration generation failed](#) on page 239
- [End-of-life AP model detected](#) on page 239
- [VLAN configuration mismatch on non-DHCP/NAT WLAN](#) on page 239
- [VLAN configuration mismatch on DHCP/NAT WLAN](#) on page 240
- [Generation failed during CCM GPB generation](#) on page 240
- [Preparation failed during AP knowledge generation](#) on page 240
- [Generation failed during CCM GPB generation](#) on page 240
- [Notification failed during AP knowledge generation](#) on page 241

Configuration updated

TABLE 439 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 440 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 441 Configuration receive failed event

Event	Configuration receive failed
Event Type	cfgRcvFailed
Event Code	1009
Severity	Debug
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 442 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"="xxxx", "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 443 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 444 AP configuration generation failed event

Event	AP configuration generation failed
Event Type	apCfgGenFailed
Event Code	1022
Severity	Major
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 445 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 93.

VLAN configuration mismatch on non-DHCP/NAT WLAN

TABLE 446 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: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.

TABLE 446 VLAN configuration mismatch on non-DHCP/NAT WLAN event (continued)

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN.
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 447 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
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 448 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 449 Preparation failed during AP knowledge generation event

Event	Preparation failed during AP knowledge generation
Event Type	ccmApTraversalPrepareFailed
Event Code	9021
Severity	Major

TABLE 449 Preparation failed during AP knowledge generation event (continued)

Event	Preparation failed during AP knowledge generation
Attribute	topicName = "SimpleTopic"
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 450 Generation failed during AP knowledge generation event

Event	Generation failed during AP knowledge generation
Event Type	ccmApTraversalGenerateFailed
Event Code	9022
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 451 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 452 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.

NOTE

Refer to [Configuration Alarms](#) on page 93.

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 data plane.

Event	Event	Event
Data plane discovered on page 242	Data plane discovery failed on page 243	Data plane configuration updated on page 243
Data plane configuration update failed on page 243	Data plane rebooted on page 244	Data plane heartbeat lost on page 244
Data plane IP address updated on page 244	Data plane updated to a new control plane on page 244	Data plane status update failed on page 245
Data plane statistics update failed on page 245	Data plane connected on page 245	Data plane disconnected on page 246
Data plane physical interface down on page 246	Data plane physical interface up on page 246	Data plane packet pool is under low water mark on page 247
Data plane packet pool is under critical low water mark on page 247	Data plane packet pool is above high water mark on page 247	Data plane core dead on page 248
Data plane process restarted on page 248	Data plane discovery succeeded on page 248	Data plane managed on page 249
Data plane deleted on page 249	Data plane license is not enough on page 249	Data plane upgrade started on page 250
Data plane upgrading on page 250	Data plane upgrade succeeded on page 250	Data plane upgrade failed on page 250
Data plane of data center side successfully connects to the CALEA server on page 251	Data plane of data center side fails to connect to the CALEA server on page 251	Data Plane of data center side disconnects to CALEA server on page 252
Data plane successfully connects to the other data plane on page 252	Data plane fails to connect to the other data plane on page 252	Data plane disconnects to the other data plane on page 253
Start CALEA mirroring client in data plane on page 253	Stop CALEA mirroring client in data plane on page 253	Data plane DHCP IP pool usage rate is 100 percent on page 254
Data plane DHCP IP pool usage rate is 80 percent on page 254	Data plane NAT session capacity usage rate is 80 percent on page 255	Data plane NAT session capacity usage rate is 100 percent on page 255
Data plane DHCP IP capacity usage rate is 80 percent on page 255	Data plane DHCP IP capacity usage rate is 100 percent on page 256	

Data plane discovered

TABLE 453 Data plane discovered event

Event	Data plane discovered
Event Type	dpDiscoverySuccess (server side detect)
Event Code	501
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}].

TABLE 453 Data plane discovered event (continued)

Event	Data plane discovered
Description	This event occurs when the data plane successfully connects to the controller.

Data plane discovery failed

TABLE 454 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", "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 455 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", "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 456 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", "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 457 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: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 458 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: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 459 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: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 460 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

TABLE 460 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 461 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 462 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 463 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"

TABLE 463 Data plane connected event (continued)

Event	Data plane connected
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 464 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 465 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 466 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.

TABLE 466 Data plane physical interface up event (continued)

Event	Data plane physical interface 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 467 Data plane packet pool is under low water mark event

Event	Data plane packet pool is under low water mark
Event Type	dpPktPoolLow
Event Code	516
Severity	Informational
Attribute	"dpKey"="xx: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 468 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: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 469 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: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 470 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:xx"
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 471 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: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 472 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: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 473 Data plane managed event

Event	Data plane managed
Event Type	dpStatusManaged
Event Code	532
Severity	Informational
Attribute	"dpKey"="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 474 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 475 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 476 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"
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 477 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 478 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 479 Data plane upgrade failed event

Event	Data plane upgrade failed
Event Type	dpUpgradeFailed
Event Code	553
Severity	Major

TABLE 479 Data plane upgrade failed event (continued)

Event	Data plane upgrade failed
Attribute	"dpKey"="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 480 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", "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 481 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", "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 482 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}]
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 483 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", "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}] successfully connects to the other Data Plane[{targetDpKey&&targetDpIp}]
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 484 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", "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}]

TABLE 484 Data plane fails to connect to the other data plane event (continued)

Event	Data plane fails to connect to the other data plane
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 485 Data plane disconnects to the other data plane event

Event	Data plane disconnects to the other data plane
Event Type	dpP2PTunnelDisconnected
Event Code	1262
Severity	Major
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}}] disconnects to the other Data Plane[{{targetDpKey&&targetDpIp}}]
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 486 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", "dpIP"="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 487 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", "dpIP"="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 488 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: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 489 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"="xxxxxxxx", "dpKey"="xx: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 490 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: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 491 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 492 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

TABLE 492 Data plane DHCP IP capacity usage rate is 80 percent event (continued)

Event	Data plane DHCP IP capacity usage rate is 80 percent
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 493 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"
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%.

NOTE

Refer to [Data Plane Alarms](#) on page 95.

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 256
- [DHCP dcln received](#) on page 257

DHCP inform received

TABLE 494 DHCP inform received event

Event	DHCP inform received
Event Type	dhcpInfmRcvd
Event Code	1238

TABLE 494 DHCP inform received event (continued)

Event	DHCP inform received
Severity	Informational
Attribute	"mvnold"=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 495 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').

- [GUID-FA82C09B-FE08-4877-9FF9-10CC5F632C68](#)
- [CGF keepalive not responded](#) on page 257
- [CDR transfer succeeded](#) on page 258
- [GUID-80DE3888-A558-48F6-AEDA-2F97F5E010E2](#)
- [GUID-1D06F561-F183-4274-9CA3-1284BCF6B663](#)

CGF keepalive not responded

TABLE 496 CGF keepalive not responded event

Event	CGF keepalive not responded
Event Type	cgfKeepAliveNotResponded
Event Code	1612
Severity	Informational

TABLE 496 CGF keepalive not responded event (continued)

Event	CGF keepalive not responded
Attribute	"mvnoid"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA","radSrvrlp"="7.7.7.7" "cgfSrvrlp"="40.40.40.40" "SCGMgmtlp"="2.2.2.2"
Displayed on the web interface	Heartbeat missed between RAD Server [{radSrvrlp}] and CGF Server [{cgfSrvrlp}] in {produce.short.name} [{SCGMgmtlp}]
Description	This event occurs when channel interface processor does not receive an acknowledgment for a keep alive request.

CDR transfer succeeded

TABLE 497 CDR transfer succeeded event

Event	CDR transfer succeeded
Event Type	cdrTxfrSuccessful
Event Code	1613
Severity	Debug
Attribute	"mvnoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="wlan.3gppnetwork.org" "radSrvrlp"="7.7.7.7" "cgfSrvrlp"="40.40.40.40" "SCGMgmtlp"="2.2.2.2"
Displayed on the web interface	CDR Transfer successful from RAD Server [{radSrvrlp}] to CGF [{cgfSrvrlp}] on {produce.short.name} [{SCGMgmtlp}]
Description	This event occurs when the call details record is successfully transferred.

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
GGSN restarted on page 259	GGSN not reachable on page 259	Echo response not received on page 259
GGSN not resolved on page 260	PDP context established on page 260	PDP create failed on page 260
PDP update by HLR succeeded on page 261	PDP update by HLR failed on page 261	PDP update by roaming succeeded on page 261
PDP update by roaming failed on page 262	PDP update by GGSN succeeded on page 262	PDP update by GGSN failed on page 262
PDP delete by TTG succeeded on page 263	PDP delete by TTG failed on page 263	PDP delete by GGSN succeeded on page 264
PDP delete by GGSN failed on page 264	IP assigned on page 264	IP not assigned on page 265
Unknown UE on page 265	PDP update success COA on page 265	PDP update fail COA on page 266
PDNGW could not be resolved on page 266	PDNGW version not supported on page 266	Associated PDNGW down on page 267
Create session response failed on page 267	Decode failed on page 268	Modify bearer response failed on page 268
Delete session response failed on page 268	Delete bearer request failed on page 269	Update bearer request failed on page 269
CGF server not configured on page 269		

GGSN restarted

TABLE 498 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 499 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", "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 event occurs when echo request is timed out.

Echo response not received

TABLE 500 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", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{{ggsnIp}}] 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 501 GGSN not resolved event

Event	GGSN not resolved
Event Type	ggsnNotResolved
Event Code	1215
Severity	Major
Attribute	"mvnold"="12", "wlanId"="1", "zoneld"="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" "uelmsi"="12345" "ueMsisdn"="98787"
Displayed on the web interface	Failed to resolve GGSN from APN [{apn}] for UE with IMSI [{uelmsi}] and MSISDN [{ueMsisdn}]
Description	This even occurs when access point name is unable to resolve to gateway GPRS support node.

PDP context established

TABLE 502 PDP context established event

Event	PDP context established
Event Type	pdpCtxtEstablished
Event Code	1216
Severity	Debug
Attribute	"mvnold"=12,"wlanId"=1 "zoneld"="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" "uelmsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	PDP context created for UE with IMSI [{uelmsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol is established.

PDP create failed

TABLE 503 PDP create failed event

Event	PDP create failed
Event Type	crtPdpFailed
Event Code	1217
Severity	Debug
Attribute	"mvnold"=12 "wlanId"=1,"zoneld"="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" "uelmsi"="12345","ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	PDP context create failed for UE with IMSI [{uelmsi}] 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 504 PDP update by HLR succeeded event

Event	PDP update by HLR succeeded
Event Type	initPdpUpdSuccHlr
Event Code	1218
Severity	Debug
Attribute	"mvsidn"=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" "uelmsi"="12345","ueMsisdn"="98787" "hlrEvent"="<event received from HLR>"
Displayed on the web interface	PDP context updated for UE with IMSI [{uelmsi}] 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 505 PDP update by HLR failed event

Event	PDP update by HLR failed
Event Type	initPdpUpdFailureHlr
Event Code	1219
Severity	Debug
Attribute	"mvsidn"=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" "uelmsi"="12345","ueMsisdn"="98787" "cause"="cause of error" "hrlEvent"="<event received from HLR>"
Displayed on the web interface	PDP context update initiated because of HLR Event [{hrlEvent}] failed for UE with IMSI [{uelmsi}] 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 506 PDP update by roaming succeeded event

Event	PDP update by roaming succeeded
Event Type	initPdpUpdSuccRoam
Event Code	1220
Severity	Debug
Attribute	"mvsidn"=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" "uelmsi"="12345" "ueMsisdn"="98787"

TABLE 506 PDP update by roaming succeeded event (continued)

Event	PDP update by roaming succeeded
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 507 PDP update by roaming failed event

Event	PDP update by roaming failed
Event Type	initPdpUpdFailureRoam
Event Code	1221
Severity	Debug
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" "cause"="cause of error"
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 508 PDP update by GGSN succeeded event

Event	PDP update by GGSN succeeded
Event Type	recvPdpUpdSuccGgsn
Event Code	1222
Severity	Debug
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	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 509 PDP update by GGSN failed event

Event	PDP update by GGSN failed
Event Type	recvPdpUpdFailureGgsn

TABLE 509 PDP update by GGSN failed event (continued)

Event	PDP update by GGSN failed
Event Code	1223
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 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 510 PDP delete by TTG succeeded event

Event	PDP delete by TTG succeeded
Event Type	initPdpDelSucc
Event Code	1224
Severity	Debug
Attribute	"mvsold"=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	{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 511 PDP delete by TTG failed event

Event	PDP delete by TTG failed
Event Type	initPdpDelFailure
Event Code	1225
Severity	Debug
Attribute	"mvsold"=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"
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 512 PDP delete by GGSN succeeded event

Event	PDP delete by GGSN succeeded
Event Type	recvPdpDelSucc
Event Code	1226
Severity	Debug
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	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 513 PDP delete by GGSN failed event

Event	PDP delete by GGSN failed
Event Type	recvPdpDelFailure
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 514 IP assigned event

Event	IP assigned
Event Type	ipAssigned
Event Code	1229
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" "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 515 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 516 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 517 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" "gtPcIp"="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}]

TABLE 517 PDP update success COA event (continued)

Event	PDP update success COA
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 518 PDP update fail COA event

Event	PDP update fail COA
Event Type	pdpUpdFailCOA
Event Code	1245
Severity	Debug
Attribute	"mvmold"=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" "uelmsi"="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 [{gtpclp}] failed for UE with IMSI [{uelmsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Failure Cause [{cause}]
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 519 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" "uelmsi"="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 [{uelmsi}@{realm}]
Description	This event occurs when the access point name is unable to resolve to PDN GW.

PDNGW version not supported

TABLE 520 PDNGW version not supported event

Event	PDNGW version not supported
Event Type	pdnGwVersionNotSupportedMsgReceived
Event Code	1952

TABLE 520 PDNGW version not supported event (continued)

Event	PDNGW version not supported
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" "uelmsi"="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 521 Associated PDNGW down event

Event	Associated PDNGW down
Event Type	pdnGwAssociationDown
Event Code	1953
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" "uelmsi"="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 522 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" "uelmsi"="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 {uelmsi}@{realm} because [[cause]]
Description	This event occurs when create session response from PDN GW fails with a cause.

Decode failed

TABLE 523 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" "uelmsi"="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 524 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" "uelmsi"="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 {{uelmsi}@{realm}} because {{cause}}
Description	This event occurs when modify bearer response from PDN GW fails with a cause.

Delete session response failed

TABLE 525 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" "uelmsi"="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 {{uelmsi}@{realm}} because {{cause}}
Description	This event occurs when the delete session response from PDN GW fails.

Delete bearer request failed

TABLE 526 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" "uelmsi"="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 {{uelmsi}@{realm}} because {{cause}}
Description	This event occurs when the delete bearer request from PDN GW fails with decode error.

Update bearer request failed

TABLE 527 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 528 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

TABLE 528 CGF server not configured event (continued)

Event	CGF server 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.

NOTE

Refer to [Gn/S2a Interface Alarms](#) on page 101.

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 270
- [Destination available](#) on page 271
- [App server down](#) on page 271
- [App server inactive](#) on page 271
- [App server active](#) on page 272
- [Association establishment failed](#) on page 272
- [Association down](#) on page 273
- [Association up](#) on page 273
- [Send auth info success](#) on page 273
- [Auth info sending failed](#) on page 274
- [GPRS location update succeeded](#) on page 274
- [GPRS location update failed](#) on page 274
- [Insert sub data success](#) on page 275
- [Insert sub data failed](#) on page 275
- [Outbound routing failure](#) on page 275
- [Did allocation failure](#) on page 276
- [Restore data success](#) on page 276
- [Restore data failed](#) on page 276

Destination not reachable

TABLE 529 Destination not reachable event

Event	Destination not reachable
Event Type	destNotRecheable
Event Code	1618
Severity	Critical
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "pointCode"="1.1.1"

TABLE 529 Destination not reachable event (continued)

Event	Destination not reachable
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 530 Destination available event

Event	Destination available
Event Type	destAvailable
Event Code	1620
Severity	Critical
Attribute	"mvnold"="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 531 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 532 App server inactive event

Event	App server inactive
Event Type	appServerInactive
Event Code	1624

TABLE 532 App server inactive event (continued)

Event	App server inactive
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 533 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 534 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 535 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 536 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 537 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" "uelmsi"="04844624203918"
Displayed on the web interface	MAP-SendAuthInfo Operation successful from IMSI [{{uelmsi}}] with [{{hlrInstance}}]
Description	This event occurs when authentication parameters are successfully retrieved.

Auth info sending failed

TABLE 538 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" "uelmsi"="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-SendAuthInfo Operation Failed for IMSI [{uelmsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to retrieve the authentication parameters.

GPRS location update succeeded

TABLE 539 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" "uelmsi"="04844624203918"
Displayed on the web interface	MAP-UpdateGprsLocation Operation Successful for IMSI [{uelmsi}] with [{hlrInstance}]
Description	This event occurs when it successfully updates the GPRS location operation.

GPRS location update failed

TABLE 540 GPRS location update failed event

Event	GPRS location update failed
Event Type	updateGprsLocFailed
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 541 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 542 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 543 Outbound routing failure event

Event	Outbound routing failure
Event Type	outboundRoutingFailure
Event Code	1636
Severity	Major
Attribute	"mvnold"="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 544 Did allocation failure event

Event	Did allocation failure
Event Type	didAllocationFailure
Event Code	1637
Severity	Critical
Attribute	"mvnold"="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 545 Restore data success event

Event	Restore data success
Event Type	restoreDataSuccess
Event Code	1639
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-RestoreData Operation Successful for IMSI [{{uelmsi}}] with [{{hlrInstance}}]
Description	This event occurs when it successfully restores the data operation.

Restore data failed

TABLE 546 Restore data failed event

Event	Restore data failed
Event Type	restoreDataFailed
Event Code	1640
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-RestoreData Operation Failed for IMSI [{{uelmsi}}] with [{{hlrInstance}}], cause [{{cause}}]
Description	This event occurs when it fails to restore the data operation.

NOTE

Refer to [GR Interface Alarms](#) on page 107.

IPMI Events

NOTE

This section is not applicable for vSZ-H.

Following are the events related to IPMIs.

Event	Event	Event
ipmiVoltage on page 277	ipmiThempBB on page 277	ipmiThempFP on page 278
ipmiThempIOH on page 278	ipmiThempMemP on page 279	ipmiThempPS on page 279
ipmiThempP on page 279	ipmiThempHSBP on page 280	ipmiFan on page 280
ipmiPower on page 280	ipmiCurrent on page 281	ipmiFanStatus on page 281
ipmiPsStatus on page 281	ipmiDrvStatus on page 282	ipmiREVotage on page 282
ipmiREThempBB on page 282	ipmiREThempFP on page 283	ipmiREThempIOH on page 283
ipmiREThempMemP on page 283	ipmiREThempPS on page 283	ipmiREThempP on page 284
ipmiREThempHSBP on page 284	ipmiREFan on page 284	ipmiREPower on page 285
ipmiREPower on page 285	ipmiREFanStatus on page 285	ipmiREPsStatus on page 286
ipmiREDrvStatus on page 286		

ipmiVoltage

TABLE 547 ipmiVoltage event

Event	ipmiVoltage
Event Type	ipmiVoltage
Event Code	901
Severity	Major
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 due to under /over voltage on the control plane. Baseboard threshold temperatures are: Critical high - 66 ⁰ C Non critical high - 61 ⁰ C Non critical low - 10 ⁰ C Critical low - 5 ⁰ C
Auto Clearance	This event triggers the alarm 901, which is auto cleared by the event code 926.

ipmiThempBB

TABLE 548 ipmiThempBB event

Event	ipmiThempBB
Event Type	ipmiThempBB
Event Code	902

TABLE 548 ipmiThempBB event (continued)

Event	ipmiThempBB
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ Celsius to 61 ⁰ Celsius. The default threshold is 61 ⁰ C.
Auto Clearance	This event triggers the alarm 902, which is auto cleared by the event code 927.

ipmiThempFP

TABLE 549 ipmiThempFP event

Event	ipmiThempFP
Event Type	ipmiThempFP
Event Code	903
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ Celsius to 44 ⁰ Celsius. The default threshold is 44 ⁰ C.
Auto Clearance	This event triggers the alarm 903, which is auto cleared by the event code 928.

ipmiThempIOH

TABLE 550 ipmiThempIOH event

Event	ipmiThempIOH
Event Type	ipmiThempIOH
Event Code	904
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ Celsius to 5 ⁰ Celsius. The default threshold is 5 ⁰ C.
Auto Clearance	This event triggers the alarm 904, which is auto cleared by the event code 929.

ipmiThempMemP

TABLE 551 ipmiThempMemP event

Event	ipmiThempMemP
Event Type	ipmiThempMemP
Event Code	905
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ Celsius to 5 ⁰ Celsius. The default threshold is 5 ⁰ C.
Auto Clearance	This event triggers the alarm 905, which is auto cleared by the event code 930.

ipmiThempPS

TABLE 552 ipmiThempPS event

Event	ipmiThempPS
Event Type	ipmiThempPS
Event Code	906
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ Celsius to 5 ⁰ Celsius. The default threshold is 5 ⁰ C.
Auto Clearance	This event triggers the alarm 906, which is auto cleared by the event code 931.

ipmiThempP

TABLE 553 ipmiThempP event

Event	ipmiThempP
Event Type	ipmiThempP
Event Code	907
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ to 11 ⁰ Celsius. The default threshold is 11 ⁰ C.
Auto Clearance	This event triggers the alarm 907, which is auto cleared by the event code 932.

ipmiThempHSBP

TABLE 554 ipmiThempHSBP event

Event	ipmiThempHSBP
Event Type	ipmiThempHSBP
Event Code	908
Severity	Majorf
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 ⁰ Celsius to 55 ⁰ Celsius. The default threshold is 55 ⁰ C.
Auto Clearance	This event triggers the alarm 908, which is auto cleared by the event code 933.

ipmiFan

TABLE 555 ipmiFan event

Event	ipmiFan
Event Type	ipmiFan
Event Code	909
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 556 ipmiPower event

Event	ipmiPower
Event Type	ipmiPower
Event Code	910
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 557 ipmiCurrent event

Event	ipmiCurrent
Event Type	ipmiCurrent
Event Code	911
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 558 ipmiFanStatus event

Event	ipmiFanStatus
Event Type	ipmiFanStatus
Event Code	912
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 559 ipmiPsStatus event

Event	ipmiPsStatus
Event Type	ipmiPsStatus
Event Code	913
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 560 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 561 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 562 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 563 ipmiREThempFP event

Event	ipmiREThempFP
Event Type	ipmiREThempFP
Event Code	928
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 564 ipmiREThempIOH event

Event	ipmiREThempIOH
Event Type	ipmiREThempIOH
Event Code	929
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 565 ipmiREThempMemP event

Event	ipmiREThempMemP
Event Type	ipmiREThempMemP
Event Code	930
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 566 ipmiREThempPS event

Event	ipmiREThempPS
Event Type	ipmiREThempPS

TABLE 566 ipmiREThempPS event (continued)

Event	ipmiREThempPS
Event Code	931
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 comes back to the normal status.

ipmiREThempP

TABLE 567 ipmiREThempP event

Event	ipmiREThempP
Event Type	ipmiREThempP
Event Code	932
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 568 ipmiREThempHSBP event

Event	ipmiREThempHSBP
Event Type	ipmiREThempHSBP
Event Code	933
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 569 ipmiREFan event

Event	ipmiREFan
Event Type	ipmiREFan
Event Code	934
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"

TABLE 569 ipmiREFan event (continued)

Event	ipmiREFan
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 570 ipmiREPower event

Event	ipmiREPower
Event Type	ipmiREPower
Event Code	935
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 571 ipmiRECurrent event

Event	ipmiRECurrent
Event Type	ipmiRECurrent
Event Code	936
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 572 ipmiREFanStatus event

Event	ipmiREFanStatus
Event Type	ipmiREFanStatus
Event Code	937
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 573 ipmiREPsStatus event

Event	ipmiREPsStatus
Event Type	ipmiREPsStatus
Event Code	938
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx: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 574 ipmiREDrvStatus event

Event	ipmiREDrvStatus
Event Type	ipmiREDrvStatus
Event Code	939
Severity	Informational
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 comes back to the normal status.

NOTE

Refer to [IPMI Alarms](#) on page 111.

Licensing Interface Events

Following are the events related to licensing.

- [TTG session warning threshold](#) on page 287
- [TTG session major threshold](#) on page 287
- [TTG session critical threshold](#) on page 287
- [TTG session license exhausted](#) on page 288
- [License sync succeeded](#) on page 288
- [License sync failed](#) on page 288
- [License import succeeded](#) on page 289
- [License import failed](#) on page 289
- [License data changed](#) on page 289
- [License going to expire](#) on page 290
- [Insufficient license capacity](#) on page 290
- [AP number limit exceeded](#) on page 291

- [Insufficient license capacity](#) on page 291

TTG session warning threshold

NOTE

This event is not applicable for vSZ-H.

TABLE 575 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 576 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 577 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"

TABLE 577 TTG session critical threshold event (continued)

Event	TTG session critical threshold
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 578 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 579 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 580 License sync failed event

Event	License sync failed
Event Type	licenseSyncFail
Event Code	1251
Severity	Warning
Attribute	"nodeName"="xxxxxxx", "licenseServerName"="ruckuswireless.flexeraoperation.com"

TABLE 580 License sync failed event (continued)

Event	License sync failed
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 581 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 582 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 583 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 584 License going to expire event

Event	License going to expire
Event Type	licenseGoingToExpire
Event Code	1255
Severity	Major
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 585 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.

NOTE

Refer to [Licensing Alarms](#) on page 118.

Data plane DHCP IP license insufficient

NOTE

This event is not applicable for SZ300/SZ100.

TABLE 586 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 587 Data plane NAT session license insufficient event

Event	Data plane NAT session license insufficient
Event Type	dpNatSessionLicenseNotEnough
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 588 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 589 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.

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 292
- [Incapable location info requested](#) on page 292
- [Unsupported location delivery request](#) on page 293

Unavailable location info requested

TABLE 590 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 591 Incapable location info requested event

Event	Incapable location info requested
Event Type	incapableLocInfoRequested
Event Code	1656
Severity	Debug
Attribute	"mvnold"=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"
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 592 Unsupported location delivery request event

Event	Unsupported location delivery request
Event Type	unSupportedLocDeliveryRequest
Event Code	1657
Severity	Debug
Attribute	"mvnold"=12, "wlanId"=1, "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radius" "realm"="operator realm", "radSrvIp"="1.1.1.1" "requestedMethod"="out of band initial request, etc" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	AAA [{radSrvIp}] 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 293
- [LMA ICMP reachable](#) on page 294
- [LMA server unreachable](#) on page 294
- [DHCP connected](#) on page 294
- [DHCP connection lost](#) on page 294

Config update failed

TABLE 593 Config update failed event

Event	Config update failed
Event Type	updateCfgFailed
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 594 LMA ICMP reachable event

Event	LMA ICMP reachable
Event Type	lmalcmpReachable
Event Code	5005
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2","lmalp"="1.1.1.1"
Displayed on the web interface	[[lmalp]] 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 595 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","lmalp"="1.1.1.1"
Displayed on the web interface	[[lmalp]] 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 596 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"
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 597 DHCP connection lost event

Event	DHCP connection lost
Event Type	lostCnxnToDHCP

TABLE 597 DHCP connection lost event (continued)

Event	DHCP connection lost
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.

NOTE

Refer to [PMIPv6 Alarms](#) on page 121.

SCI Events

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

- [Connect to SCI](#) on page 295
- [Disconnect to SCI](#) on page 295
- [Connect to SCI failure](#) on page 296
- [SCI has been disabled](#) on page 296
- [SCI and FTP have been disabled](#) on page 296

Connect to SCI

TABLE 598 Connect to SCI event

Event	Connect to SCI
Event Type	connectedToSci
Event Code	4001
Severity	Informational
Attribute	"id"="SCI Server","ip"="2.2.2.2","port"="8883","userName"="admin"
Displayed on the web interface	Connect to SCI with system id [{id}],address [{ip}:{port}] and login user [{userName}].
Description	This event occurs when the controller connects to SCI.

Disconnect to SCI

TABLE 599 Disconnect to SCI event

Event	Disconnect to SCI (Smart Cell Insight)
Event Type	disconnectedFromSci
Event Code	4002
Severity	Warning

TABLE 599 Disconnect to SCI event (continued)

Event	Disconnect to SCI (Smart Cell Insight)
Attribute	id="SCI Server", "ip"="2.2.2.2", "port"="8883", "userName"="admin"
Displayed on the web interface	Disconnect to SCI with system id [{id}], address [{ip}:{port}] and login user [{userName}]
Description	This event occurs when the controller disconnects from SCI.

Connect to SCI failure

TABLE 600 Connect to SCI failure event

Event	Connect to SCI failure (Smart Cell Insight)
Event Type	connectToSciFailure
Event Code	4003
Severity	Major
Displayed on the web interface	Try to connect to SCI with all SCI profiles but failure.
Description	This event occurs when the controller tries connecting to SCI with its profiles but fails.
Auto Clearance	This event triggers the alarm 4003, which is auto cleared by the event code 4002.

SCI has been disabled

TABLE 601 SCI has been disabled event

Event	SCI has been disabled
Event Type	disabledSciDueToUpgrade
Event Code	4004
Severity	Warning
Displayed on the web interface	SCI has been disabled due to SZ upgrade, please reconfigure SCI if need
Description	This event occurs when SCI is disabled due to the controller upgrade. This could require reconfiguration of SCI.

SCI and FTP have been disabled

TABLE 602 SCI and FTP have been disabled event

Event	SCI and FTP have been disabled
Event Type	disabledSciAndFtpDueToMutuallyExclusive
Event Code	4005
Severity	Warning
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.

NOTE

Refer to [SCI Alarms](#) on page 122.

Session Events

Following are the events related to session interface (UE TTG sessions)

- [Session timeout](#) on page 297
- [Delete all sessions](#) on page 297
- [Binding succeeded](#) on page 298
- [Binding failed](#) on page 298
- [Binding time expired](#) on page 299
- [Binding revoked](#) on page 299
- [Binding released](#) on page 299

Session timeout

NOTE

This event is not applicable for vSZ-H.

TABLE 603 Session timeout event

Event	Session timeout
Event Type	sessTimeout
Event Code	1235
Severity	Debug
Attribute	"mvsidn"=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" "ueImei"="12345","ueMsisdn"="98787"
Displayed on the web interface	Session for UE with IMSI [{{ueImei}}] 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 604 Delete all sessions event

Event	Delete all sessions
Event Type	delAllSess
Event Code	1237
Severity	Minor
Attribute	"mvsidn"="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}}]

TABLE 604 Delete all sessions event (continued)

Event	Delete all sessions
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 605 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 606 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" "lmaIp"="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 607 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" "lmaIp"="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 608 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" "lmaIp"="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 have been revoked on {produce.short.name}-D {{dataBladeIp}}
Description	This event occurs when the binding is revoked on the controller.

Binding released

NOTE

This event is not applicable for vSZ-H.

TABLE 609 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" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5"

TABLE 609 Binding released event (continued)

Event	Binding released
Displayed on the web interface	[[ueMacAddr]] UE Binding have been released on {produce.short.name}-D [[dataBladeIp]]
Description	This event occurs when some mobile node binding are released.

NOTE

Refer to [Session Alarms](#) on page 124.

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 300
- [STA session termination {produce.short.name} initiated success](#) on page 300
- [STA session termination AAA initiated success](#) on page 301
- [STA session termination AAA initiated failed](#) on page 301
- [STA re-authorization successful](#) on page 302

STA successful authentication

TABLE 610 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", "uelmsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvIp"="1.1.1.1"
Displayed on the web interface	[[srcProcess]] Auth of [[uelmsi]]/[[ueUsername]] on {produce.short.name} [[SCGMgmtIp]] with AAA server [[aaaSrvIp]] 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 611 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

TABLE 611 STA session termination {produce.short.name} initiated success event (continued)

Event	STA session termination {produce.short.name} initiated success
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]] 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 612 STA session termination AAA initiated success event

Event	STA session termination AAA initiated success
Event Type	staSessionTermAAAINitSucess
Event Code	1555
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]] Session Termination of [[ueImsi]]/[[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 613 STA session termination AAA initiated failed event

Event	STA session termination AAA initiated failed
Event Type	staSessionTermAAAINitFailed
Event Code	1556
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]] 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 614 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", "uelmsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvrIp"="1.1.1.1"
Displayed on the web interface	{{srcProcess}} Re-Auth of {{uelmsi}}/{{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 303	LS authentication failure on page 303	{{produce.short.name}} connected to LS on page 304
{{produce.short.name}} failed to connect to LS on page 304	{{produce.short.name}} received passive request on page 304	{{produce.short.name}} sent controller information report on page 305
{{produce.short.name}} received management request on page 305	{{produce.short.name}} sent AP info by venue report on page 305	{{produce.short.name}} sent associated client report on page 306
{{produce.short.name}} forwarded calibration request to AP on page 306	{{produce.short.name}} forwarded calibration request to AP on page 306	{{produce.short.name}} forwarded footfall request to AP on page 306
{{produce.short.name}} received unrecognized request on page 307	Syslog server reachable on page 307	Syslog server unreachable on page 307
Syslog server switched on page 308	Generate AP config for plane load rebalance succeeded on page 308	Generate AP config for plane load rebalance failed on page 308
FTP transfer on page 309	FTP transfer error on page 309	CSV export FTP transfer on page 309
CSV export FTP transfer error on page 310	CSV export FTP transfer maximum retry on page 310	CSV export disk threshold exceeded on page 310
CSV export disk max capacity reached on page 311	CSV export disk threshold back to normal on page 311	File upload on page 311
Email sent successfully on page 311	Email sent failed on page 312	SMS sent successfully on page 312
SMS sent failed on page 312	Process restart on page 313	Service unavailable on page 313
Keepalive failure on page 313	Resource unavailable on page 314	HIP started on page 314
HIP stopped on page 314	GUID-FD483EC2-6F84-4442-BBD5-CEEB00A3F8F5	Standby HIP restarted on page 315
HIP cache cleaned on page 315	All data planes in the zone affinity profile are disconnected on page 316	CALEA UE Matched on page 316

Event	Event	Event
GUID-7F110500-241B-4A2C-907A-1559CD91D063	GUID-F249E1C3-9782-4366-90D4-792453218093	Diameter peer transport failure on page 316
Diameter CER error on page 317	Diameter CER success on page 317	Diameter invalid version on page 318
GUID-07CBE4E9-25CE-4554-A2DA-B18820F9E1FD	Diameter peer add successful on page 318	GUID-DC66D841-B306-47D3-9B84-A7FFE083FBB7
GUID-4767803C-3AFA-4658-9172-1C815A188BBC	GUID-81DDFBA1-FCB3-45B6-8838-EC66E9F455F9	GUID-7C5FF652-5D78-4EA3-963C-E24594D26585
GUID-ED97681C-5A34-4738-9181-F9DE4754758F	GUID-8971DFE9-9D9B-4AF4-A657-5B9251348222	ZD AP migrating on page 318
ZD AP migrated on page 319	ZD AP rejected on page 319	ZD AP migration failed on page 319
Database error on page 320	Recover cassandra error on page 320	Process initiated on page 320
PMIPv6 unavailable on page 321	Memory allocation failed on page 321	Process stopped on page 321
Password expiration on page 322	Admin account lockout on page 322	Admin session expired on page 322
Disable inactive admins on page 323	Two factor auth failed on page 323	

No LS responses

TABLE 615 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 616 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}]
Description	This event occurs due to the authentication failure on connecting to the location based service.

{produce.short.name} connected to LS

TABLE 617 {produce.short.name} connected to LS event

Event	{produce.short.name} connected to LS
Event Type	scgLBSCConnectSuccess
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 618 {produce.short.name} failed to connect to LS event

Event	{produce.short.name} failed to connect to LS
Event Type	scgLBSCConnectFailed
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 619 {produce.short.name} received passive request event

Event	{produce.short.name} received passive request
Event Type	scgLBSSStartLocationService
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 620 {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 621 {produce.short.name} received management request event

Event	{produce.short.name} received management request
Event Type	scgLBSRcvdMgmtRequest
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 622 {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 623 {produce.short.name} sent query venues report event

Event	{produce.short.name} sent query venues report
Event Type	scgLBSSendVenuesReport

TABLE 623 {produce.short.name} sent query venues report event (continued)

Event	{produce.short.name} sent query venues report
Event Code	730
Severity	Informational
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 624 {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 625 {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 626 {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

TABLE 626 {produce.short.name} forwarded footfall request to AP event (continued)

Event	{produce.short.name} forwarded footfall request to AP
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "SCGMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"=""
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 627 {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 628 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 629 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"

TABLE 629 Syslog server unreachable event (continued)

Event	Syslog server unreachable
Displayed on the web interface	Syslog server {{syslogServerAddress}} is unreachable on {produce.short.name}.
Description	This event occurs when the syslog server is unreachable.
Auto Clearance	This event triggers the alarm 751, which is auto cleared by the event code 750.

Syslog server switched

TABLE 630 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.

Generate AP config for plane load rebalance succeeded

TABLE 631 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 632 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.

TABLE 632 Generate AP config for plane load rebalance failed event (continued)

Event	Generate AP config for plane load rebalance failed
Description	This event occurs when the user executes the load of data plane for rebalancing and generation of a new AP configuration fails.

FTP transfer

TABLE 633 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 634 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 635 CSV export FTP transfer event

Event	CSV export FTP transfer
Event Type	csvFtpTransfer
Event Code	972
Severity	Informational
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.xxxx.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 636 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:xx", "ip"="xx:xx:xx:xx:xx:xx", "portID"="xx: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 637 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:xx", "ip"="xx:xx:xx:xx:xx:xx", "portID"="xx: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 638 CSV export disk threshold exceeded event

Event	CSV export disk threshold exceeded
Event Type	csvDiskThreshholdExceeded
Event Code	975
Severity	Warning
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 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 639 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 640 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: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 641 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 642 Email sent successfully event

Event	Email sent successfully
Event Type	mailSendSuccess
Event Code	981

TABLE 642 Email sent successfully event (continued)

Event	Email sent successfully
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 643 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 644 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 645 SMS sent failed event

Event	SMS sent failed
Event Type	smsSendFailed
Event Code	984
Severity	Warning
Attribute	"srcProcess"="xxxxx","receiver"= "xxxxx",

TABLE 645 SMS sent failed event (continued)

Event	SMS sent failed
	"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 646 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 647 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 648 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"

TABLE 648 Keepalive failure event (continued)

Event	Keepalive failure
Displayed on the web interface	{{srcProcess}} on {produce.short.name} {{SCGMgmtIp}} restarted {{processName}} process.
Description	This event occurs when the mon/nc restarts the process due to a keep alive failure.

Resource unavailable

TABLE 649 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 650 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 651 HIP stopped event

Event	HIP stopped
Event Type	hipStopped
Event Code	1015

TABLE 651 HIP stopped event (continued)

Event	HIP stopped
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 652 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 653 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}}]
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 654 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 655 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", "dplP"="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 656 Diameter peer transport failure event

Event	Diameter peer transport failure
Event Type	diaPeerTransportFailure
Event Code	1403
Severity	Major
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"

TABLE 656 Diameter peer transport failure event (continued)

Event	Diameter peer transport failure
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 657 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 658 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"
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 659 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 660 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 661 ZD AP migrating event

Event	ZD AP migrating
Event Type	zdAPMigrating
Event Code	2001
Severity	Informational

TABLE 661 ZD AP migrating event (continued)

Event	ZD AP migrating
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 662 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 663 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 664 ZD AP migration failed event

Event	ZD AP migration failed
Event Type	zdAPMigrationFailed
Event Code	2004
Severity	Major

TABLE 664 ZD AP migration failed event (continued)

Event	ZD AP migration failed
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 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 665 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 666 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 667 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"

TABLE 667 Process initiated event (continued)

Event	Process initiated
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 668 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 669 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 670 Process stopped event

Event	Process stopped
Event Type	processStop

TABLE 670 Process stopped event (continued)

Event	Process stopped
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

NOTE

Refer to [System Alarms](#) on page 124.

Password expiration

TABLE 671 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 672 Admin account lockout event

Event	Admin account lockout
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	8011
Severity	Warning
Attribute	userId = "x"
Displayed on the web interface	Administrative account [{userId}] has been locked out because of repeat login failures.
Description	This event occurs when the account is locked.

Admin session expired

TABLE 673 Admin session expired event

Event	Admin session expired
Event Type	AdminSessionExpired
Event Code	8012
Severity	Informational
Attribute	userName = "x"

TABLE 673 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 account is idle for a period of time.

Disable inactive admins

TABLE 674 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 675 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 [Data Plane Alarms](#) on page 95.

Switch Events

Following are the events related to switch severity.

- [Switch critical message](#) on page 324
- [Switch alert message](#) on page 324
- [Switch warning message](#) on page 324

Switch critical message

TABLE 676 Switch critical message event

Event	Switch critical message
Event Type	SwitchCriticalMessage
Event Code	20000
Severity	Critical
Attribute	
Displayed on the web interface	
Description	This event occurs when the there is a switch critical message.

Switch alert message

TABLE 677 Switch alert message event

Event	Switch alert message
Event Type	SwitchAlertMessage
Event Code	20001
Severity	Major
Attribute	
Displayed on the web interface	
Description	This event occurs when there is a switch alert message.

Switch warning message

TABLE 678 Switch warning message event

Event	Switch warning message
Event Type	SwitchWarningMessage
Event Code	20003
Severity	Warning
Attribute	
Displayed on the web interface	
Description	This event occurs when there is a switch warning message.

Threshold Events

Following are the events related to threshold system set.

- [CPU threshold exceeded](#) on page 325
- [Memory threshold exceeded](#) on page 325
- [Disk usage threshold exceeded](#) on page 326
- [CPU threshold back to normal](#) on page 326

- [Memory threshold back to normal](#) on page 326
- [Disk threshold back to normal](#) on page 326
- [License threshold exceeded](#) on page 327
- [The drop of client count threshold exceeded](#) on page 327
- [Rate limit threshold surpassed](#) on page 327
- [Rate limit threshold restored](#) on page 328
- [Rate limit for TOR surpassed](#) on page 328
- [The number of users exceed its limit](#) on page 329
- [The number of devices exceeded its limit](#) on page 329

CPU threshold exceeded

TABLE 679 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 680 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 681 Disk usage threshold exceeded event

Event	Disk usage threshold exceeded
Event Type	diskUsageThresholdExceeded
Event Code	952
Severity	Critical
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 682 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 683 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 684 Disk threshold back to normal event

Event	Disk threshold back to normal
Event Type	diskUsageThresholdBackToNormal
Event Code	955

TABLE 684 Disk threshold back to normal event (continued)

Event	Disk threshold back to normal
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 685 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: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 686 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 687 Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major
Attribute	"mvnold"=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"

TABLE 687 Rate limit threshold surpassed event (continued)

Event	Rate limit threshold surpassed
	"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 [{aaaSrvrlp}] 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 688 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" "aaaSrvrlp"="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 [{aaaSrvrlp}] 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 689 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" "aaaSrvrlp"="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 [{aaaSrvrlp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.

TABLE 689 Rate limit for TOR surpassed event (continued)

Event	Rate limit for TOR surpassed
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 690 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.
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 691 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.

NOTE

Refer to [Threshold Alarms](#) on page 133.

Tunnel Events - Access Point (AP)

Following are the events related to tunnel events on access point.

- [Data plane accepted a tunnel request](#) on page 330
- [Data plane rejected a tunnel request](#) on page 330
- [Data plane terminated a tunnel](#) on page 331

Events Types

Tunnel Events - Access Point (AP)

- [AP created a tunnel](#) on page 331
- [AP tunnel disconnected](#) on page 331
- [AP softGRE tunnel fails over primary to secondary](#) on page 332
- [AP softGRE tunnel fails over secondary to primary](#) on page 332
- [AP softGRE gateway reachable](#) on page 332
- [AP softGRE gateway not reachable](#) on page 332
- [Data plane set up a tunnel](#) on page 333
- [AP secure gateway association success](#) on page 333
- [AP is disconnected from secure gateway](#) on page 333
- [AP secure gateway association failure](#) on page 334

NOTE

Event codes 601 to 610 are not applicable for vSZ-H.

Data plane accepted a tunnel request

TABLE 692 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 693 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 694 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 695 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 696 AP tunnel disconnected event

Event	AP tunnel disconnected
Event Type	apTunnelDisconnected
Event Code	610
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dpIP"="xxx.xxx.xxx.xxx", "reason"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] disconnected from data plane [{dpIP}]. 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 697 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 698 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 699 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"
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 700 AP softGRE gateway not reachable event

Event	AP softGRE gateway not reachable
Event Type	apSoftGREGatewayNotReachable

TABLE 700 AP softGRE gateway not reachable event (continued)

Event	AP softGRE gateway not reachable
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 701 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 702 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.
Description	This event occurs when the AP is able to reach the secure gateway successfully.

AP is disconnected from secure gateway

TABLE 703 AP is disconnected from secure gateway event

Event	AP is disconnected from secure gateway
Event Type	ipsecTunnelDisassociated

TABLE 703 AP is disconnected from secure gateway event (continued)

Event	AP is disconnected from secure gateway
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 704 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.

NOTE

Refer to [Tunnel Alarms - Access Point](#) on page 136.

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 335
- [DP sGRE keep alive timeout](#) on page 335
- [DP sGRE GW inactive](#) on page 335
- [DP DHCPRelay no response](#) on page 336
- [DP DHCPRelay failover](#) on page 336
- [DP sGRE new tunnel](#) on page 336
- [DP sGRE del tunnel](#) on page 336
- [DP sGRE keepalive recovery](#) on page 337
- [DP DHCPRelay response recovery](#) on page 337
- [DP sGRE GW reachable](#) on page 337
- [DP sGRE GW active](#) on page 338

- [DP sGRE GW failover](#) on page 338

DP sGRE GW unreachable

TABLE 705 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 706 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 707 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
Description	This event occurs when the data plane detects that a core network gateway is inactive.

DP DHCPRelay no response

TABLE 708 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 709 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 710 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 711 DP sGRE del tunnel event

Event	DP sGRE del tunnel
Event Type	dpSgreDelTunnel
Event Code	621

TABLE 711 DP sGRE del tunnel event (continued)

Event	DP sGRE del tunnel
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 712 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 713 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 714 DP sGRE GW reachable event

Event	DP sGRE GW reachable
Event Type	dpSgreGWReachable
Event Code	624
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 now reachable

TABLE 714 DP sGRE GW reachable event (continued)

Event	DP sGRE GW reachable
Description	This event occurs when the core gateway is reachable.

DP sGRE GW active

TABLE 715 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 716 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.

NOTE

Refer to [Tunnel Alarms - Access Point](#) on page 136.



© 2018 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com