



RUCKUS SmartZone (LT-GD) Alarm and Event Reference Guide, 6.1.2

Published from  
CommScope Technical Content Portal by  
29 January 2025

# CommScope Legal Statements

© 2025 CommScope, Inc. All rights reserved

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

All trademarks identified by ™ or ® are trademarks or registered trademarks in the US and may be registered in other countries. All product names, trademarks, and registered trademarks are property of their respective owners.

## Patent marking notice

For applicable patents, see [www.cs-pat.com](http://www.cs-pat.com). That website is intended to give notice under 35 U.S.C. § 287(a) of articles that are patented or for use under the identified patents. That website identifies the patents associated with each of the patented articles.

# Table of Contents

[Ruckus Back Cover](#)

[Contact Information, Resources, and Conventions](#)

[About This Guide](#)

New in This Document. . . . . 57

Introduction. . . . . 57

Terminology. . . . . 57

[Alarm and Event Management](#)

Overview. . . . . 65

Alarm and Event Management. . . . . 65

    Event Categories. . . . . 65

    Event Attributes. . . . . 66

    Generation of Alarm and Event. . . . . 66

    Smart Monitor Feature. . . . . 71

[Alarm Types](#)

Introduction. . . . . 73

Accounting Alarms. . . . . 73

    Accounting server not reachable. . . . . 73

    Accounting Failed Over to Secondary. . . . . 74

    Accounting Fallback to Primary. . . . . 75

AP Accounting Message Mandatory Parameter Missing. ....	76
AP Accounting Message Decode Failed. ....	77
AP Account Message Drop While No Accounting Start Message. ....	78
Unauthorized CoA/DM message dropped. ....	79
AP Authentication Alarms. ....	80
RADIUS server unreachable. ....	81
LDAP server unreachable. ....	82
AD server unreachable. ....	83
WeChat ESP authentication server unreachable. ....	83
WeChat ESP authentication server unresolvable. ....	84
WeChat ESP DNAT server unreachable. ....	85
WeChat ESP DNAT server unresolvable. ....	86
AP Communication Alarms. ....	87
AP rejected. ....	88
AP configuration update failed. ....	88
AP swap model mismatched. ....	89
AP pre-provision model mismatched. ....	90
AP firmware update failed. ....	91
AP WLAN oversubscribed. ....	92
AP join zone failed. ....	93
AP image signing failed. ....	94

AP LBS Alarms. ....	96
No LS responses. ....	96
LS authentication failure. ....	97
AP failed to connect to LS. ....	98
AP State Change Alarms. ....	99
AP rebooted by system. ....	99
AP disconnected. ....	100
AP deleted. ....	101
AP cable modem interface down. ....	102
AP DHCP service failure. ....	102
AP NAT failure. ....	103
AP DHCP/NAT DWPDP Ethernet port configuration override. ....	104
SZ DHCP/NAT DWPDP Ethernet port configuration override. ....	105
SIM removal. ....	106
AP System Anomaly. ....	106
AP 3rd Radio. ....	107
apIllegalToChange3rdRadioBand. ....	107
apIllegal6gVAPCreation. ....	108
Authentication Alarms. ....	108
Authentication server not reachable. ....	109
Authentication failed over to secondary. ....	110

Authentication fallback to primary. . . . .	110
AD/LDAP connectivity failure. . . . .	111
Bind fails with AD/LDAP. . . . .	113
Bind success with LDAP, but unable to find clear text password for the user. . . . .	114
RADIUS fails to connect to AD NPS server. . . . .	115
RADIUS fails to authenticate with AD NPS server. . . . .	116
Fails to establish TLS tunnel with AD/LDAP. . . . .	117
RAC DNS Resolve Failed. . . . .	118
Control and Data Plane Interface Alarms. . . . .	118
GtpManager (DP) disconnected. . . . .	119
Cloud Alarms. . . . .	119
Cloud Analytics Service has been Enabled. . . . .	120
Cloud Analytics Service has been Disabled. . . . .	120
Cloud Analytics Disconnected. . . . .	121
Cluster Alarms. . . . .	121
New node failed to join. . . . .	123
Node removal failed. . . . .	124
Node out of service. . . . .	125
Cluster in maintenance state. . . . .	126
Cluster backup failed. . . . .	127
Cluster restore failed. . . . .	128

Cluster upgrade failed. ....	129
Cluster application stopped. ....	130
Node bond interface down. ....	131
Node physical interface down. ....	132
Cluster node rebooted. ....	133
Cluster node shut down. ....	134
Node IP Changed. ....	134
Disk usage exceed threshold. ....	135
Cluster out of service. ....	136
Cluster upload AP firmware failed. ....	137
Cluster add AP firmware failed. ....	137
Unsync NTP time. ....	138
Cluster upload KSP file failed. ....	139
Configuration backup failed. ....	140
Configuration restore failed. ....	140
AP certificate updated. ....	141
Upgrade SS table failed. ....	142
Cluster redundancy sync configuration failed. ....	143
Cluster redundancy restoring configuration failed. ....	143
Not all APs rehome after timeout. ....	144
Over switch max capacity. ....	145

AP is connected to Standby Cluster Over The Expiration Date. . . . .	145
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy. . . . .	146
External DP Connected to Standby Cluster after Rehome Timeout. . . . .	147
Certificate is about to Expire. . . . .	147
Certificate is already Expired. . . . .	148
Configuration Alarms. . . . .	149
Zone configuration preparation failed. . . . .	149
AP configuration generation failed. . . . .	150
End-of-life AP model detected. . . . .	151
VLAN configuration mismatch on non DHCP/NAT WLAN. . . . .	152
VLAN configuration mismatch on DHCP/NAT WLAN. . . . .	153
Data Plane Alarms. . . . .	154
Data plane configuration update failed. . . . .	155
Data plane disconnected. . . . .	156
Data plane physical interface down. . . . .	156
Data plane rebooted. . . . .	157
Data plane packet pool is under low water mark. . . . .	158
Data plane packet pool is under critical low water mark. . . . .	159
Data plane core dead. . . . .	160
Data plane process restarted. . . . .	161
Data plane license is not enough. . . . .	161

Data plane upgrade failed. ....	162
Data plane of data center side fails to connect to the CALEA server. ....	164
Data plane fails to connects to the other data plane. ....	164
Data plane DHCP IP pool usage rate is 100 percent. ....	165
Data Streaming Alarms. ....	166
Connecting Failure to a Data Streaming Profile. ....	166
Gn/S2a Interface Alarms. ....	167
GGSN restarted. ....	167
GGSN not reachable. ....	168
GGSN not resolved. ....	169
PDNGW could not be resolved. ....	170
PDNGW version not supported. ....	171
Associated PDNGW down. ....	172
Create session response failed. ....	173
Decode failed. ....	174
Modify bearer response failed. ....	175
Delete session response failed. ....	176
Delete bearer request failed. ....	177
Update bearer request failed. ....	178
CGF server not configured. ....	179
GR Interface Alarms. ....	179

Destination not reachable. ....	180
App server down. ....	181
App server inactive. ....	182
Association establishment failed. ....	183
Association down. ....	184
Outbound routing failure. ....	185
Did allocation failure. ....	186
IPMI Alarms. ....	186
ipmiVoltage. ....	188
ipmiThempBB. ....	189
ipmiThempFP. ....	190
ipmiThempIOH. ....	191
ipmiThempMemP. ....	192
ipmiThempPS. ....	193
ipmiThempP. ....	194
ipmiThempHSBP. ....	195
ipmiFan. ....	196
ipmiPower. ....	197
ipmiCurrent. ....	197
ipmiFanStatus. ....	198
ipmiPsStatus. ....	199

ipmiDrvStatus. . . . .	200
Licensing Alarms. . . . .	201
TTG session critical threshold. . . . .	201
TTG session license exhausted. . . . .	202
License going to expire. . . . .	203
Insufficient license capacity. . . . .	204
Data plane DHCP IP license insufficient. . . . .	204
Data plane NAT session license insufficient. . . . .	205
Insufficient license capacity. . . . .	206
PMIPv6 Alarms. . . . .	207
Config update failed. . . . .	207
DHCP connection lost. . . . .	208
SCI Alarms. . . . .	209
Connect to SCI failure. . . . .	209
SCI has been disabled. . . . .	210
SCI and FTP have been disabled. . . . .	210
Session Alarms. . . . .	211
Binding failed. . . . .	211
System Alarms. . . . .	212
No LS responses. . . . .	213
LS authentication failure. . . . .	214

{produce.short.name} failed to connect to LS. ....	215
Syslog server unreachable. ....	215
CSV export FTP maximum retry. ....	216
CSV export disk threshold exceeded. ....	217
CSV export disk max capacity reached. ....	218
Process restart. ....	218
Service unavailable. ....	219
Keepalive failure. ....	220
Resource unavailable. ....	221
HIP failed over. ....	221
Unconfirmed program detection. ....	222
Diameter initialization error. ....	223
Diameter peer transport failure. ....	224
Diameter CER error. ....	225
Diameter peer add error. ....	226
Diameter peer remove successful. ....	227
Diameter realm entry error. ....	228
Diameter failover to alternate peer. ....	229
Diameter fail back to peer. ....	230
Diameter CEA unknown peer. ....	231
Diameter no common application. ....	232

Process initiated. ....	233
PMIPv6 unavailable. ....	234
Memory allocation failed. ....	235
The last one data plane is disconnected zone affinity profile alarm. ....	236
scheduleZoneFirmwareUpgrade. ....	236
Switch. ....	237
Power supply failure. ....	238
Fan failure. ....	239
Module insertion. ....	240
Module removal. ....	240
Temperature above threshold warning. ....	241
Stack member unit failure. ....	242
PoE power allocation failure. ....	243
DHCP_Snooping: DHCP offer dropped message. ....	243
Port put into error disable state. ....	244
Switch offline. ....	245
Switch duplicated. ....	245
Reject certificate signing request. ....	246
Pending certificate signing request. ....	247
Switch CPU major threshold exceed. ....	248
Switch CPU critical threshold exceed. ....	248

Switch memory major threshold exceed. ....	249
Switch memory critical threshold exceed. ....	250
Switch custom major threshold exceed. ....	251
Switch custom critical threshold exceed. ....	251
Switch Firmware Upgrade Failed. ....	252
Switch Configuration Update Failed. ....	252
Threshold Alarms. ....	253
CPU threshold exceeded. ....	254
Memory threshold exceeded. ....	255
Disk usage threshold exceeded. ....	256
The drop of client count threshold exceeded. ....	257
License threshold exceeded. ....	257
HDD Health Degradation. ....	258
Rate limit for TOR surpassed. ....	259
The number of users exceeded its limit. ....	260
The number of devices exceeded its limit. ....	261
Over AP maximum capacity. ....	261
Over Device maximum capacity. ....	262
Tunnel Alarms - Access Point. ....	262
AP softGRE gateway not reachable. ....	263
AP is disconnected from secure gateway. ....	263

AP secure gateway association failure. ....	264
---	-----

## Events Types

3rd Party Access Point Events. ....	267
3rd party AP connected. ....	267
Accounting Events. ....	268
Accounting session disabled. ....	269
Accounting server not reachable. ....	269
Accounting failed over to secondary. ....	270
Accounting fallback to primary. ....	271
AP accounting message mandatory parameter missing. ....	272
Unknown realm. ....	273
AP accounting message decode failed. ....	274
AP accounting retransmission message dropped. ....	274
AP accounting response while invalid config. ....	275
AP account message drop while no accounting start message. ....	276
Unauthorized COA/DM message dropped. ....	277
AP Authentication Events. ....	278
Radius server reachable. ....	279
Radius server unreachable. ....	280
LDAP server reachable. ....	280
LDAP server unreachable. ....	281

AD server reachable. ....	282
AD server unreachable. ....	282
Wechat ESP authentication server reachable. ....	283
WeChat ESP authentication server unreachable. ....	284
WeChat ESP authentication server resolvable. ....	285
WeChat ESP authentication server unresolvable. ....	285
WeChat ESP DNAT server reachable. ....	286
WeChat ESP DNAT server unreachable. ....	287
WeChat ESP DNAT server resolvable. ....	287
WeChat ESP DNAT server unresolvable. ....	288
Authentication Attempts. ....	289
Authentication Unsuccessful. ....	289
Authentication Re-attempt. ....	290
Authentication 8021. ....	291
AP Local Session Timeout. ....	291
AP Remote Session Timeout. ....	292
AP Interactive Session Termination. ....	292
AP Communication Events. ....	293
AP discovery succeeded. ....	295
AP managed. ....	295
AP rejected. ....	296

AP firmware updated. ....	297
AP firmware update failed. ....	297
Updating AP firmware. ....	298
Updating AP configuration. ....	299
AP configuration updated. ....	299
AP configuration update failed. ....	300
AP pre-provision model mismatched. ....	301
AP swap model mismatched. ....	301
AP WLAN oversubscribed. ....	302
AP join zone failed. ....	303
AP illegal to change country code. ....	303
AP configuration get failed. ....	304
Rogue AP. ....	304
Rogue AP disappeared. ....	305
Classified Rogue AP. ....	306
AP image signing failed. ....	306
Jamming attack. ....	307
Rogue client. ....	308
Key gen fail. ....	308
Key dis fail. ....	309
Key dis fail GTK. ....	309

wpaendec fail. . . . .	310
IPsecsec fail. . . . .	311
Fw manual initiation. . . . .	311
AP Management TSF data. . . . .	312
AP TSF failure. . . . .	313
AP Self tests. . . . .	313
Firmware initiation update. . . . .	314
SSH initiation. . . . .	315
SSH termination. . . . .	315
SSH failure. . . . .	316
TLS initiation. . . . .	316
TLS termination. . . . .	317
TLS failure. . . . .	318
IP sec initiation. . . . .	318
IP sec termination. . . . .	319
IP sec failure. . . . .	319
AP LBS Events. . . . .	320
No LS responses. . . . .	321
LS authentication failure. . . . .	321
AP connected to LS. . . . .	322
AP failed to connect to LS. . . . .	322

AP started location service. . . . .	323
AP stopped location service. . . . .	324
AP received passive calibration request. . . . .	324
AP received passive footfall request. . . . .	325
AP received unrecognized request. . . . .	325
AP Mesh Events. . . . .	326
EMAP downlink connected to MAP. . . . .	327
EMAP downlink disconnected from MAP. . . . .	328
EMAP uplink connected to MAP. . . . .	328
EMAP uplink disconnected from MAP. . . . .	329
MAP disconnected. . . . .	329
MAP downlink connected. . . . .	330
MAP downlink connected to EMAP. . . . .	331
MAP downlink disconnected from EMAP. . . . .	331
RAP downlink connected to MAP. . . . .	332
MAP uplink connected to EMAP. . . . .	332
MAP uplink disconnected from EMAP. . . . .	333
MAP uplink connected to RAP. . . . .	334
MAP uplink connected to MAP. . . . .	334
Mesh state updated to MAP. . . . .	335
Mesh state updated to MAP no channel. . . . .	336

Mesh state updated to RAP. ....	336
Mesh state update to RAP no channel. ....	337
MAP downlink connected to MAP. ....	338
MAP downlink disconnected from MAP. ....	338
RAP downlink disconnected from MAP. ....	339
AP State Change Events. ....	339
AP rebooted by user. ....	341
AP rebooted by system. ....	342
AP disconnected. ....	343
AP IP address updated. ....	343
AP reset to factory default. ....	344
AP channel updated. ....	344
AP country code updated. ....	345
AP channel updated because dynamic frequency selection (DFS) detected a radar. ....	346
AP change control plane. ....	346
AP connected. ....	347
AP deleted. ....	348
AP heartbeat lost. ....	348
AP tagged as critical. ....	349
AP cable modem interface down. ....	349
AP brownout. ....	350

AP cable modem power-cycled by user. ....	350
AP smart monitor turn off WLAN. ....	351
AP client load balancing limit reached. ....	352
AP client load balancing limit recovered. ....	352
AP WLAN state changed. ....	353
AP capacity reached. ....	354
AP capacity recovered. ....	354
AP cable modem interface up. ....	355
AP cable modem soft-rebooted by user. ....	355
AP cable modem set to factory default by user. ....	356
AP health high latency flag. ....	357
AP health low capacity flag. ....	357
AP health high connection failure flag. ....	358
AP health high client count flag. ....	358
AP health high latency clear. ....	359
AP health low capacity clear. ....	359
AP health high connection failure clear. ....	360
AP health high client count clear. ....	360
Primary DHCP AP is down. ....	361
Primary DHCP AP is up. ....	361
Secondary DHCP AP is down. ....	362

Secondary DHCP AP is up. ....	362
Primary or secondary DHCP AP detects 90% of the configured total IPs. ....	363
Both primary and secondary DHCP server APs are down. ....	363
AP NAT gateway IP failover detected for particular VLAN pool. ....	364
AP NAT gateway IP fall back detected for particular VLAN pool. ....	364
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. ....	365
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. ....	366
AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down. ....	367
AP health high airtime utilization flag. ....	367
AP health high airtime utilization clear. ....	368
AP cluster failover. ....	368
AP cluster rehome. ....	369
AP switchover cluster failed. ....	370
AP MAC OUI violation. ....	370
Backhaul switched to primary. ....	371
Backhaul switched to secondary. ....	371
LTE network connectivity lost. ....	372
Ethernet network connectivity lost. ....	373
LTE DHCP timeout. ....	373
Ethernet link down. ....	374

Ethernet link up. ....	374
SIM switch. ....	375
Remote host blacklisted. ....	375
SIM removal. ....	376
LTE network registration status. ....	377
LTE connection status. ....	377
LTE good rssi status. ....	378
LTE weak rssi status. ....	378
AP client load balancing limit reached. ....	379
AP client load balancing limit recovered. ....	380
AP System Anomaly. ....	381
AP Temp AF Threshold Exceeded. ....	381
AP Writable File Threshold Exceeded. ....	382
AP Operate in BT. ....	382
AP MDU Port Status Down. ....	383
AP USB Events. ....	383
AP USB software package downloaded. ....	384
AP USB software package download failed. ....	384
Authentication Events. ....	385
Authentication server not reachable. ....	386
Unknown realm. ....	386

Authentication succeeded. ....	387
Authentication failed. ....	388
Pseudonym authentication succeeded. ....	389
Pseudonym authentication failed. ....	390
Fast re-authentication succeeded. ....	391
Fast re-authentication failed. ....	391
Authentication failed over to secondary. ....	392
Authentication fallback to primary. ....	393
AD/LDAP connected successfully. ....	394
AD/LDAP connectivity failure. ....	395
Bind fails with AD/LDAP. ....	395
Bind success with LDAP, but unable to find clear text password for the user. ....	396
RADIUS fails to connect to AD NPS server. ....	397
RADIUS fails to authenticate with AD NPS server. ....	398
Successfully established the TLS tunnel with AD/LDAP. ....	398
Fails to establish TLS tunnel with AD/LDAP. ....	399
TLS Establishment Failed between SZ and external AAA Server. ....	399
RAC DNS Resolve Failed. ....	400
Authorization Events. ....	401
DM received from AAA. ....	401
DM NACK sent to AAA. ....	402

DM sent to NAS. ....	403
DM NACK received from NAS. ....	403
CoA received from AAA. ....	404
CoA NACK sent to AAA. ....	405
CoA sent NAS. ....	405
CoA NAK received NAS. ....	406
CoA authorize only access reject. ....	407
CoA RWSG MWSG notification failure. ....	407
Control and Data Plane Interface. ....	408
DP connected. ....	409
GtpManager (DP) disconnected. ....	409
Session updated at DP. ....	410
Session update at DP failed. ....	411
Session deleted at DP. ....	412
Session delete at DP failed. ....	413
C2d configuration failed. ....	413
Client Events. ....	414
Client authentication failed. ....	416
Client joined. ....	417
Client failed to join. ....	418
Client disconnected. ....	418

Client connection timed out. ....	419
Client authorization successfully. ....	420
Client authorization failed. ....	421
Client session expired. ....	422
Client roaming. ....	422
Client logged out. ....	423
3rd party client join. ....	424
3rd party client inactivity timeout. ....	424
3rd party client authorization. ....	425
3rd party client authorization failure. ....	426
3rd party client session expiration. ....	427
3rd party client roaming. ....	428
3rd party client session logout. ....	428
Client roaming disconnected. ....	429
Client blocked. ....	430
Client grace period. ....	431
Onboarding registration succeeded. ....	431
Onboarding registration failed. ....	432
Remediation succeeded. ....	433
Remediation failed. ....	433
Force DHCP disconnected. ....	434

WDS device joined. ....	435
WDS device left. ....	435
Client is blocked because of barring UE rule. ....	436
Client is unblocked by barring UE rule. ....	436
Start CALEA mirroring client. ....	437
Stop CALEA mirroring client. ....	437
Client information updated. ....	438
Wired client joined. ....	438
Wired client failed to join. ....	439
Wired client disconnected. ....	440
Wired client authorization successfully. ....	440
Wired client session expired. ....	441
Application identified. ....	442
Application denied. ....	442
URL filtering server unreachable. ....	443
URL filtering server reachable. ....	443
Packet spoofing detected. ....	444
Packet spoofing detected. ....	444
Packet spoofing detected. ....	445
Packet spoofing detected. ....	446
Cloud Events. ....	446

Cloud Services Enabled. . . . .	447
Cloud Services Disabled. . . . .	447
Cloud Analytics Enabled. . . . .	448
Cloud Analytics Disabled. . . . .	448
Cloud Services Token Refreshed. . . . .	449
Cloud Analytics Token Renewed. . . . .	449
Cloud Analytics Service has been Enabled. . . . .	450
Cloud Analytics service has been disabled. . . . .	451
Cloud Analytics Disconnected. . . . .	451
cloudAPRegistrarSyncEnabled. . . . .	452
cloudAPRegistrarSyncDisabled. . . . .	452
cloudAPRegistrarSyncSZInfo. . . . .	453
cloudAPRegistrarSyncAPIInfo. . . . .	453
Cluster Events. . . . .	454
Cluster created successfully. . . . .	456
New node joined successfully. . . . .	456
New node failed to join. . . . .	457
Node removal completed. . . . .	458
Node removal failed. . . . .	458
Node out of service. . . . .	459
Cluster in maintenance state. . . . .	460

Cluster back in service. . . . .	460
Cluster backup completed. . . . .	461
Cluster backup failed. . . . .	461
Cluster restore completed. . . . .	462
Cluster restore failed. . . . .	463
Cluster node upgrade completed. . . . .	463
Entire cluster upgraded successfully. . . . .	464
Cluster upgrade failed. . . . .	465
Cluster application stopped. . . . .	465
Cluster application started. . . . .	466
Cluster backup started. . . . .	467
Cluster upgrade started. . . . .	467
Cluster leader changed. . . . .	468
Node bond interface down. . . . .	468
Node bond interface up. . . . .	469
Node IP address changed. . . . .	470
Node physical interface down. . . . .	470
Node physical interface up. . . . .	471
Cluster node rebooted. . . . .	471
NTP time synchronized. . . . .	472
Cluster node shutdown. . . . .	473

Cluster upload started. . . . .	473
Cluster upload completed. . . . .	474
Cluster upload failed. . . . .	474
SSH tunnel switched. . . . .	475
Cluster remove node started. . . . .	476
Node back in service. . . . .	476
Disk usage exceed threshold. . . . .	477
Cluster out of service. . . . .	477
Initiated moving APs in node to a new cluster. . . . .	478
Cluster upload vSZ-D firmware started. . . . .	479
Cluster upload vSZ-D firmware completed. . . . .	479
Cluster upload vSZ-D firmware failed. . . . .	480
Cluster upload AP firmware started. . . . .	480
Cluster upload AP firmware completed. . . . .	481
Cluster upload AP firmware failed. . . . .	482
Cluster add AP firmware started. . . . .	482
Cluster add AP firmware completed. . . . .	483
Cluster add AP firmware failed. . . . .	483
Cluster name is changed. . . . .	484
Unsync NTP Time. . . . .	485
Cluster upload KSP file started. . . . .	485

Cluster upload KSP file completed. ....	486
Cluster upload KSP file failed. ....	486
NTP unreachable server. ....	487
Configuration backup started. ....	487
Configuration backup succeeded. ....	488
Configuration backup failed. ....	488
Configuration restore succeeded. ....	489
Configuration restore failed. ....	489
AP Certificate Expired. ....	490
AP Certificate Updated. ....	491
Configuration restore started. ....	491
Upgrade SSTable failed. ....	491
Reindex elastic search finished. ....	492
Initiated APs contact APR. ....	492
All nodes back in service. ....	493
Not management service ready. ....	493
Management service ready. ....	493
Configuration sync failed. ....	494
Node IPv6 address added. ....	494
AP is connected to standby cluster over the expiration date. ....	495
Node IPv6 address deleted. ....	496

Sync Configuration started for Cluster Redundancy. . . . .	496
Sync Configuration Success for Cluster Redundancy. . . . .	497
Standby Cluster Failed to Restore a Configuration for Cluster Redundancy. . . . .	497
Standby Cluster Restores a Configuration for Cluster Redundancy. . . . .	498
Standby Cluster Restored a Configuration Success for Cluster Redundancy. . . . .	498
Standby Cluster Back to Monitoring Mode for Cluster Redundancy. . . . .	499
AP Connected to Standby Cluster after Rehome Timeout. . . . .	500
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy. . . . .	500
External DP Connected to Standby Cluster after Rehome Timeout. . . . .	501
Certificate is about to Expire. . . . .	502
Certificate is already Expired. . . . .	502
Result of Renew Certificate. . . . .	503
Cluster node Resource Invalid. . . . .	503
Configuration Events. . . . .	504
Configuration updated. . . . .	505
Configuration update failed. . . . .	505
Configuration receive failed. . . . .	506
Incorrect flat file configuration. . . . .	507
Zone configuration preparation failed. . . . .	507
AP configuration generation failed. . . . .	508
End-of-life AP model detected. . . . .	509

VLAN configuration mismatch on non-DHCP/NAT WLAN. ....	509
VLAN configuration mismatch on DHCP/NAT WLAN. ....	510
Generation failed during CCM GPB generation. ....	510
Preparation failed during AP knowledge generation. ....	511
Generation failed during AP knowledge generation. ....	512
End-of-life AP model detected during AP knowledge generation. ....	512
Notification failed during AP knowledge generation. ....	513
Datablade Events. ....	514
DP integrity test failed. ....	515
DP CLI enable failed. ....	515
DP re-authentication. ....	516
DP password min length updated. ....	517
DP password changed. ....	517
DP enable password changed. ....	518
DP https authentication failed. ....	518
DP certificate uploaded. ....	519
DP Scg FQDN updated. ....	519
DP initial upgrade. ....	520
DP discontinuous time change NTP server DP Ntp time sync. ....	521
DP user login. ....	521
DP user login failed. ....	522

DP user logout. . . . .	522
DP account locked. . . . .	523
DP session idle updated. . . . .	523
DP session idle terminated. . . . .	524
DP SSH tunnel failed. . . . .	525
DP https connection failed. . . . .	525
DP IPsec tunnel create failed. . . . .	526
Data Plane Events. . . . .	526
Data plane discovered. . . . .	528
Data plane discovery failed. . . . .	528
Data plane configuration updated. . . . .	529
Data plane configuration update failed. . . . .	530
Data plane rebooted. . . . .	530
Data plane heartbeat lost. . . . .	531
Data plane IP address updated. . . . .	531
Data plane updated to a new control plane. . . . .	532
Data plane status update failed. . . . .	533
Data plane statistics update failed. . . . .	533
Data plane connected. . . . .	534
Data plane disconnected. . . . .	534
Data plane physical interface down. . . . .	535

Data plane physical interface up. ....	536
Data plane packet pool is under low water mark. ....	536
Data plane packet pool is under critical low water mark. ....	537
Data plane packet pool is above high water mark. ....	538
Data plane core dead. ....	538
Data plane process restarted. ....	539
Data plane discovery succeeded. ....	539
Data plane managed. ....	540
Data plane deleted. ....	541
Data plane license is not enough. ....	541
Data plane upgrade started. ....	542
Data plane upgrading. ....	543
Data plane upgrade succeeded. ....	543
Data plane upgrade failed. ....	544
Data Plane Upgrade Failed Due to Corrupted RPM. ....	544
Data plane of data center side successfully connects to the CALEA server. ....	545
Data plane of data center side fails to connect to the CALEA server. ....	546
Data Plane of data center side disconnects to CALEA server. ....	546
Data plane successfully connects to the other data plane. ....	547
Data plane fails to connect to the other data plane. ....	548
Data plane disconnects to the other data plane. ....	548

Start CALEA mirroring client in data plane. ....	549
Data plane DHCP IP pool usage rate is 100 percent. ....	549
Data plane DHCP IP pool usage rate is 80 percent. ....	550
Data plane NAT session capacity usage rate is 80 percent. ....	551
Data plane NAT session capacity usage rate is 100 percent. ....	551
Data plane DHCP IP capacity usage rate is 80 percent. ....	552
Data plane DHCP IP capacity usage rate is 100 percent. ....	553
Data plane backup success. ....	553
Data plane backup failed. ....	554
Data plane restore success. ....	554
Data plane restore failed. ....	555
dplpmiPsStatus. ....	556
dplpmiThempIOH. ....	556
dplpmiThempMemP. ....	557
dplpmiPsStatus. ....	557
dplpmiREVoltage. ....	558
dplpmiREThempIOH. ....	559
dplpmiREThempMemP. ....	559
dplpmiRePsStatus. ....	560
dpSSDHealthDegrade. ....	560
Remote Administration Start. ....	561

Remote Administration Stop. ....	562
Data plane Switchover Failed. ....	562
Data Streaming Event. ....	563
Connected to Data a Streaming Endpoint. ....	563
Disconnected to Data a Streaming Endpoint. ....	563
Connected to Data a Streaming Endpoint Failure. ....	564
DHCP Events. ....	564
DHCP inform received. ....	565
DHCP dcln received. ....	565
GA Interface Events. ....	566
Connection to CGF failed. ....	566
CGF keepalive not responded. ....	567
CDR transfer succeeded. ....	568
CDR generation failed. ....	569
CDR transfer failed. ....	569
Gn/S2a Interface Events. ....	570
GGSN restarted. ....	571
GGSN not reachable. ....	572
Echo response not received. ....	572
GGSN not resolved. ....	573
PDP context established. ....	574

PDP create failed. . . . .	574
PDP update by HLR succeeded. . . . .	575
PDP update by HLR failed. . . . .	576
PDP update by roaming succeeded. . . . .	577
PDP update by roaming failed. . . . .	578
PDP update by GGSN succeeded. . . . .	578
PDP update by GGSN failed. . . . .	579
PDP delete by TTG succeeded. . . . .	580
PDP delete by TTG failed. . . . .	581
PDP delete by GGSN succeeded. . . . .	581
PDP delete by GGSN failed. . . . .	582
IP assigned. . . . .	583
IP not assigned. . . . .	584
Unknown UE. . . . .	584
PDP update success COA. . . . .	585
PDP update fail COA. . . . .	586
PDNGW could not be resolved. . . . .	587
PDNGW version not supported. . . . .	588
Associated PDNGW down. . . . .	588
Create session response failed. . . . .	589
Decode failed. . . . .	590

Modify bearer response failed. . . . .	591
Delete session response failed. . . . .	591
Delete bearer request failed. . . . .	592
Update bearer request failed. . . . .	593
CGF server not configured. . . . .	594
Gr Interface Event. . . . .	594
Destination not reachable. . . . .	595
Destination available. . . . .	596
App server down. . . . .	597
App server inactive. . . . .	597
App server active. . . . .	598
Association establishment failed. . . . .	599
Association down. . . . .	600
Association up. . . . .	600
Send auth info success. . . . .	601
Auth info sending failed. . . . .	602
GPRS location update succeeded. . . . .	602
GPRS location update failed. . . . .	603
Insert sub data success. . . . .	604
Insert sub data failed. . . . .	604
Outbound routing failure. . . . .	605

Did allocation failure. . . . .	606
Restore data success. . . . .	606
Restore data failed. . . . .	607
IPMI Events. . . . .	607
ipmiVoltage. . . . .	608
ipmiThempBB. . . . .	609
ipmiThempFP. . . . .	610
ipmiThempIOH. . . . .	611
ipmiThempMemP. . . . .	611
ipmiThempPS. . . . .	612
ipmiThempP. . . . .	613
ipmiThempHSBP. . . . .	614
ipmiFan. . . . .	615
ipmiPower. . . . .	615
ipmiCurrent. . . . .	616
ipmiFanStatus. . . . .	617
ipmiPsStatus. . . . .	617
ipmiDrvStatus. . . . .	618
ipmiREVotage. . . . .	619
ipmiREThempBB. . . . .	620
ipmiREThempFP. . . . .	620

ipmiREThempIOH. ....	621
ipmiREThempMemP. ....	621
ipmiREThempPS. ....	622
ipmiREThempP. ....	623
ipmiREThempHSBP. ....	623
ipmiREFan. ....	624
ipmiREPower. ....	625
ipmiRECurrent. ....	625
ipmiREFanStatus. ....	626
ipmiREPsStatus. ....	627
ipmiREDrvStatus. ....	627
Licensing Interface Events. ....	628
TTG session warning threshold. ....	629
TTG session major threshold. ....	630
TTG session critical threshold. ....	630
TTG session license exhausted. ....	631
License sync succeeded. ....	632
License sync failed. ....	632
License import succeeded. ....	633
License import failed. ....	634
License data changed. ....	634

License going to expire. . . . .	635
Insufficient license capacity. . . . .	635
Data plane DHCP IP license insufficient. . . . .	636
Data plane NAT session license insufficient. . . . .	637
AP number limit exceeded. . . . .	637
Insufficient license capacity. . . . .	638
Insufficient license capacity. . . . .	639
Location Delivery Events. . . . .	639
Unavailable location info requested. . . . .	640
Incapable location info requested. . . . .	640
Unsupported location delivery request. . . . .	641
PMIPv6 Events. . . . .	642
Config update failed. . . . .	642
LMA ICMP reachable. . . . .	643
LMA server unreachable. . . . .	644
DHCP connected. . . . .	644
DHCP connection lost. . . . .	645
Session Events. . . . .	645
Session timeout. . . . .	646
Delete all sessions. . . . .	647
Binding succeeded. . . . .	647

Binding failed. ....	648
Binding time expired. ....	649
Binding revoked. ....	649
Binding released. ....	650
STA Interface Events. ....	651
STA successful authentication. ....	651
STA session termination {produce.short.name} initiated success. ....	652
STA session termination AAA initiated success. ....	653
STA session termination AAA initiated failed. ....	654
STA re-authorization successful. ....	654
System Events. ....	655
No LS responses. ....	657
LS authentication failure. ....	658
{produce.short.name} connected to LS. ....	658
{produce.short.name} failed to connect to LS. ....	659
{produce.short.name} received passive request. ....	660
{produce.short.name} sent controller information report. ....	660
{produce.short.name} received management request. ....	661
{produce.short.name} sent AP info by venue report. ....	662
{produce.short.name} sent query venues report. ....	662
{produce.short.name} sent associated client report. ....	663

{produce.short.name} forwarded calibration request to AP. ....	663
{produce.short.name} forwarded footfall request to AP. ....	664
{produce.short.name} received unrecognized request. ....	665
Syslog server reachable. ....	666
Syslog server unreachable. ....	666
Syslog server switched. ....	667
System service failure. ....	668
Generate AP config for plane load rebalance succeeded. ....	668
Generate AP config for plane load rebalance failed. ....	669
FTP transfer. ....	669
FTP transfer error. ....	670
CSV export FTP transfer. ....	671
CSV export FTP transfer error. ....	671
CSV export FTP transfer maximum retry. ....	672
CSV export disk threshold exceeded. ....	672
CSV export disk max capacity reached. ....	673
CSV export disk threshold back to normal. ....	673
File upload. ....	674
Email sent successfully. ....	675
Email sent failed. ....	675
SMS sent successfully. ....	676

SMS sent failed. ....	676
Process restart. ....	677
Service unavailable. ....	678
Keepalive failure. ....	678
Resource unavailable. ....	679
HIP started. ....	680
HIP stopped. ....	680
Standby HIP restarted. ....	681
HIP cache cleaned. ....	682
All data planes in the zone affinity profile are disconnected. ....	683
CALEA UE Matched. ....	683
Diameter peer transport failure. ....	684
Diameter CER error. ....	684
Diameter CER success. ....	685
Diameter invalid version. ....	686
Diameter peer add successful. ....	687
ZD AP migrating. ....	688
ZD AP migrated. ....	689
ZD AP rejected. ....	689
ZD AP migration failed. ....	690
Database error. ....	691

Recover cassandra error. ....	691
Process initiated. ....	692
PMIPv6 unavailable. ....	692
Memory allocation failed. ....	693
Process stopped. ....	694
SZ Login Fail. ....	695
SZ Login. ....	695
SZ Logout. ....	696
Password expiration. ....	696
Admin account logout. ....	697
Admin session expired. ....	697
Disable inactive admins. ....	698
Two factor auth failed. ....	698
Unconfirmed program detection. ....	699
Admin account logout after failed attempts. ....	700
Discontinuous time change. ....	700
Mesh network connectivity lost. ....	701
Failure of Key Generation. ....	701
Failure of IPsec. ....	702
Failure Certificate. ....	703
IPsec KE is Up. ....	703

IPsec IKE is Down. . . . .	704
Discontinuous Time Change. . . . .	704
szAuthAction. . . . .	705
Switch Events. . . . .	705
Switch critical message. . . . .	707
Switch alert message. . . . .	707
Switch warning message. . . . .	708
Switch CPU warning threshold exceed. . . . .	708
Switch CPU major threshold exceed. . . . .	709
Switch CPU critical threshold exceed. . . . .	709
Switch memory warning threshold exceed. . . . .	710
Switch memory major threshold exceed. . . . .	711
Switch memory critical threshold exceed. . . . .	711
Switch custom warning threshold exceed. . . . .	712
Switch custom major threshold exceed. . . . .	712
Switch custom critical threshold exceed. . . . .	713
GetCACert Request. . . . .	714
Certificate signing request. . . . .	714
Accept certificate signing request. . . . .	715
Reject certificate signing request. . . . .	715
Pending certificate signing request. . . . .	716

Switch is Offline for 15 Minutes. ....	716
Over Switch Max Capacity. ....	717
Switch Duplicated. ....	718
Switch Firmware Upgrade. ....	718
Switch Firmware Upgrade Failed. ....	719
Switch Configuration Update. ....	719
Switch Configuration Update Failed. ....	720
Switch Reboot. ....	721
Switch Delete. ....	721
Switch Disconnected from the Controller. ....	722
Switch is Connected to the Controller. ....	722
Switch Discovered by the Controller. ....	723
scheduleZoneFirmwareUpgrade. ....	723
Threshold Events. ....	724
CPU threshold exceeded. ....	725
Memory threshold exceeded. ....	726
Disk usage threshold exceeded. ....	726
CPU threshold back to normal. ....	727
Memory threshold back to normal. ....	728
Disk threshold back to normal. ....	728
License threshold exceeded. ....	729

The drop of client count threshold exceeded. . . . .	729
Rate limit threshold surpassed. . . . .	730
Rate limit threshold restored. . . . .	731
Rate limit for TOR surpassed. . . . .	732
The number of users exceed its limit. . . . .	733
The number of devices exceeded its limit. . . . .	733
Over AP maximum capacity. . . . .	734
Over Device Maximum Capacity. . . . .	735
Device Capacity Threshold Back to Normal. . . . .	735
Tunnel Events - Access Point (AP). . . . .	736
Data plane accepted a tunnel request. . . . .	736
Data plane rejected a tunnel request. . . . .	737
Data plane terminated a tunnel. . . . .	738
AP created a tunnel. . . . .	738
AP tunnel disconnected. . . . .	739
AP softGRE tunnel fails over primary to secondary. . . . .	740
AP softGRE tunnel fails over secondary to primary. . . . .	740
AP softGRE gateway reachable. . . . .	741
AP softGRE gateway not reachable. . . . .	742
Data plane set up a tunnel. . . . .	742
AP secure gateway association success. . . . .	743

AP is disconnected from secure gateway. ....	744
AP secure gateway association failure. ....	744
Tunnel Events - Data Plane. ....	745
DP sGRE GW unreachable. ....	746
DP sGRE keep alive timeout. ....	746
DP sGRE GW inactive. ....	747
DP DHCPRelay no response. ....	747
DP DHCPRelay failover. ....	748
DP sGRE new tunnel. ....	749
DP sGRE del tunnel. ....	749
DP sGRE keepalive recovery. ....	750
DP DHCPRelay response recovery. ....	750
DP sGRE GW reachable. ....	751
DP sGRE GW active. ....	752
DP sGRE GW failover. ....	752
DP switchover. ....	753
AP Ethernet Phy Error Count. ....	753
AP Ethernet PHY Down Shift. ....	754
AP BAND Change. ....	755
apIllegalToChange3rdRadioBand. ....	755
apIllegal6gVAPCreation. ....	755

ap6gWLANCfgDone..... 756

# Ruckus Back Cover

---

© 2023 CommScope, Inc. All rights reserved.

350 West Java Dr., Sunnyvale, CA 94089 USA

<https://www.commscope.com>

# Contact Information, Resources, and Conventions

---

## Contacting RUCKUS Customer Services and Support

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

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

### What Support Do I Need?

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

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

### Open a Case

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

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

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

## Self-Service Resources

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

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

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

## Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

## RUCKUS Product Documentation Resources

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

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

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

## Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

## Document Conventions

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




**Table 1.** Text Conventions

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

## Notes, Cautions, and Safety Warnings

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

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

-  **Attention:** An ATTENTION statement indicates some information that you must read before continuing with the current action or task.
-  **CAUTION:** A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.
-  **DANGER:** A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## Command Syntax Conventions

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

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.  Default responses to system prompts are enclosed in square brackets.
{x  y  z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	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.

# About This Guide

## New in This Document

### Introduction

### Terminology

## New in This Document

**Table 1.** Summary of Enhancements in SmartZone Release 6.1.2 (December, 2023)

Description	Location	Publication Date
Alarm Code 302	Refer to <a href="#">AP rebooted by system</a>	December 2023

Parent topic: [About This Guide](#)

## Introduction

This *SmartZone Alarm and Event Guide* describes the various types of alarms and events that SmartZone 300 (SZ300), SmartZone 100 (SZ100), Virtual SmartZone-Essentials (vSZ-E) 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 Networks. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

Parent topic: [About This Guide](#)

## Terminology

The following table lists the terms used in this guide.

**Table 1.** Terms used

Term	Description
3GPP	3rd Generation Partnership Project

Term	Description
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
CDR	<p>Call Detail Record.</p> <p>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.</p>

Term	Description
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

Term	Description
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

Term	Description
GTP-U	GTP user plane
GTP'	GPRS protocol, used for CDR transport. It is derived from GTP with enhancements to improve transport reliability necessary for CDRs
GTPP	GPRS Tunneling Protocol Prime
GTPv1-U	GTP version 1, user plane
GTPv2-C	GTP version 2, control plane
HIP	Host Identity Protocol
HLR	Home Location Register
ICMP	Internet Control Message Protocol
IE	Information Element
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IPSP	IP Signalling Protocol
LBS	Location Based Service
LCS	Location Services
LDAP	Lightweight Directory Access Protocol
LMA	Local Mobility Anchor

Term	Description
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MOR	Maximum Outstanding Requests
MS-ISDN	Mobile Subscriber Integrated Services Digital Network Number
MTU	Maximum Transmission Unit
MWSG	Metro Wireless Security Gateway
NAS	Network Access Server
NTP	Network Time Protocol)
OUI	Organization Unique ID
P-GW	Packet Data Network Gateway
PAA	PDN Address Allocation
PCN	Packet switched Core network Node (SGSN, GGSN, S-GW, P-GW)
PCO	Protocol Configuration Options
PDN	Packet Data Network
PDP	Packet Data Protocol
PGW	PDN Gateway

Term	Description
produce.short.name	Refers to either SZ300 or vSZ-H
R-WSG/WSG	RUCKUS Security Gateway
RAC	Radio Access Controller
RAP	Root Access Point
RAR	Re-Auth Request
RSSI	Received Signal Strength Indicator
S-CDR	SGSN Call Detail Record
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
SG	Signalling Gateway
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SSID	Service Set Identifier (SSID)
STR	STR (Session Termination-Request)
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TEID	Tunnel End Point Identifier
UDP	User Datagram Protocol

Term	Description
UE	User Equipment
UI	Web User Interface
USB	Universal Serial Bus
WDS	Wireless Distribution System

Parent topic: [About This Guide](#)

# Alarm and Event Management

---

## Overview

### Alarm and Event Management

## 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](#) for the terminology used in this guide. Refer to the Preface section for the conventions used in this guide.

Parent topic: [Alarm and Event Management](#)

## 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](#)
- [Event Attributes](#)
- [Generation of Alarm and Event](#)

Parent topic: [Alarm and Event Management](#)

## 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.

Parent topic: [Alarm and Event Management](#)

## 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

Parent topic: [Alarm and Event Management](#)

## Generation of Alarm and Event

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

1. Alarm
  - a. An alarm is a persistent indication of a fault that clears only when the triggering condition had been resolved.

b. An alarm can be filtered in the controller web interface based on:

- Alarm Category - Alarm classifications
- Alarm Source: Source of the alarm
- Alarm Status: Could either be outstanding or cleared
- Acknowledge Time: The time when the alarm is acknowledged
- Date and Time - Date and time when the alarm is acknowledged
- Severity: Severity is classified as critical, major or minor
- Status - Could either be cleared or outstanding
- Type - Alarm type

c. To view the below alarm information in the controller web interface navigate to **Events & Alarms > Alarms**

- Date and Time
- Code
- Alarm Type
- Severity
- Status
- Acknowledged on
- Cleared By
- Cleared On
- Comments
- Activity
- Actions

d. On an alarm generation, the controller web interface provides the following information as seen in the figure below.

- Alarm console, which displays the cleared and outstanding alarms visible to the user who is currently logged on.
- Alarm summary, which lists various information such as outstanding alarm counts, unacknowledged alarm counts, etc.
- You may clear an alarm or a set of alarms to let other administrators know that you have already resolved the issue. When you select a group of alarms, the **Clear Alarm** button is activated. Click this button. A text box appears where you can enter comments or notes about the resolved issue. Click **Apply** when done. To view the cleared alarms, select the cleared option.
- You may acknowledge an alarm or a set of alarms to let other administrators know that you have acknowledged it. When you select an alarm or group of alarms, the **Acknowledge Alarm** button is activated. Click this button. A text box appears where you need to confirm the acknowledgment. Click **Yes** when done. The **Acknowledged on** column in the Alarms table gets updated.
- Filtering features based on the alarm attributes.

The **Filter** button is deactivated by default. Click this button if you want to turn on the filter. Click the gear icon to set the filter. A text box appears where you can enter the severity, status and start and end date and time. Click **OK** when done.

- You may also export the data as a CSV file.

**Figure 1. Alarms**

Date and Time	Code	Alarm Type	Severity	Status	Activity	Acknowledged On	Cleared By	Cleared On
2017/01/24 16:...	302	AP rebooted by system	Major	Outstanding	AP [INDIA-AP-H510@1C:B9:C4:23:03...	N/A	N/A	N/A
2017/01/26 15:...	302	AP rebooted by system	Major	Outstanding	AP [R710-215@D4:68:4D:1A:68:20] r...	N/A	N/A	N/A
2017/01/25 16:...	303	AP disconnected	Major	Outstanding	AP [INDIA-AP-H510@1C:B9:C4:23:03...	N/A	N/A	N/A
2017/01/25 16:...	303	AP disconnected	Major	Outstanding	AP [C110@F0:3E:9D: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

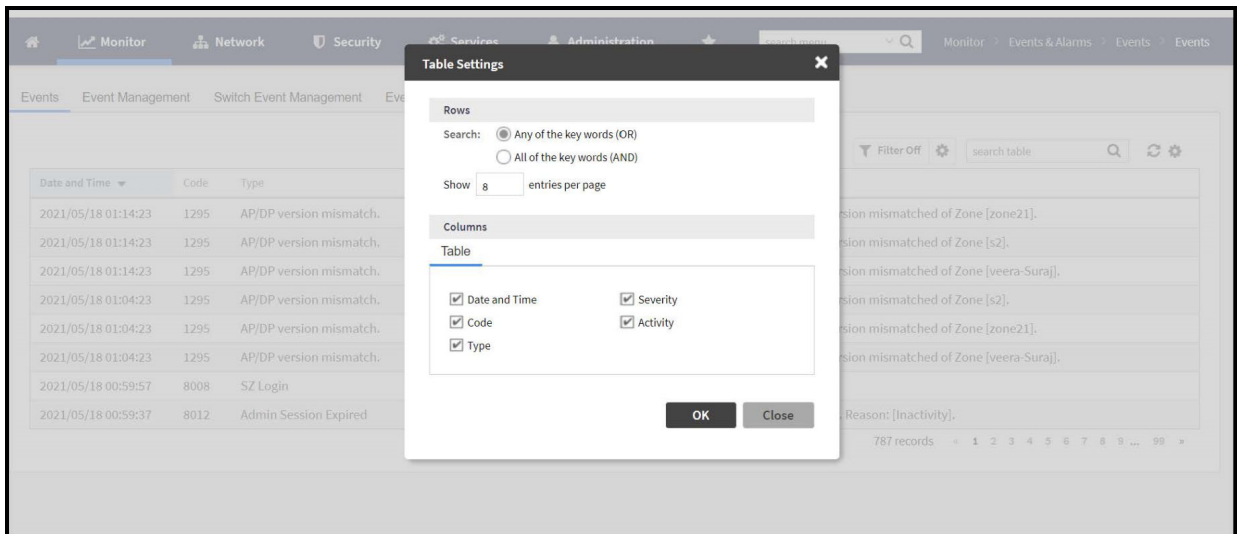
## 2. Event - On an event generation the following:

- 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.

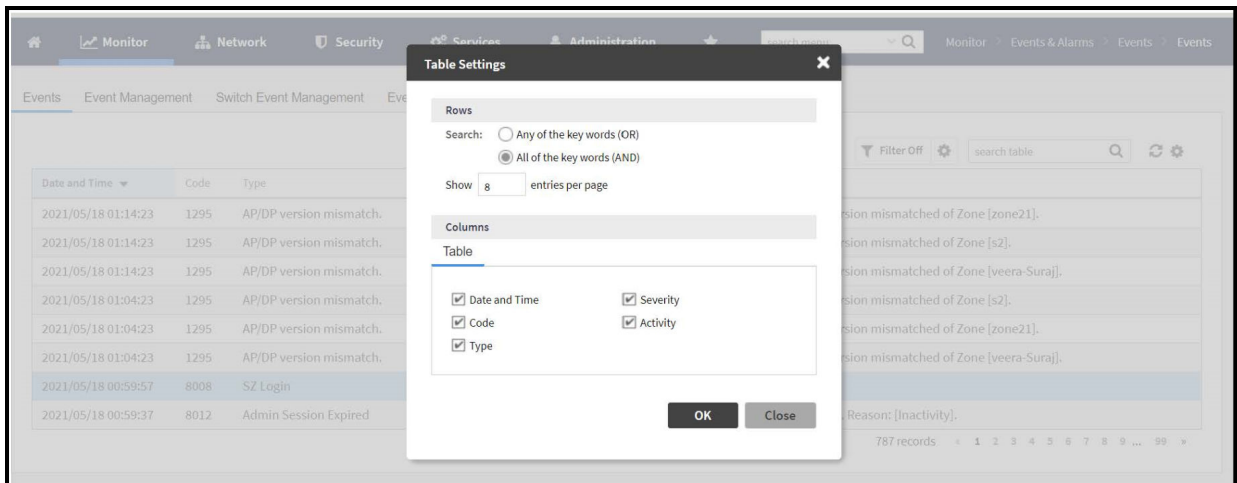
**Events** - The web interface provides event log window as seen in the figure below, for users to visualize and analyze the events. To view the event information in the controller web interface navigate to **Events & Alarms > Events**.

Events can be searched with "OR" or "AND" options as displayed in the below images.

#### Search Events with OR Option



#### Search Events with AND Option



- **Date and Time:** Displays the date and time when the event occurred.
- **Code:** Displays the event code.
- **Type:** Displays the type of event that occurred (for example, AP configuration updated).

- **Severity:** Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc.
- **Activity:** Displays additional details about the event, including (if available) the specific access point, control plane, or data plane that triggered.

**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**

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](#) and [Events Types](#) 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.

**Parent topic:** [Alarm and Event Management](#)

## Smart Monitor Feature

Smart Monitor feature is going to check AP's uplink connectivity periodically and turn off the WLANs according to the connection status. Note that Smart Monitor feature can be enabled / disabled perZone and AP.

Smart Monitor will use **arping** as checking method. AP will check the connectivity with **default gateway** which is fetched from routing table automatically. According to the result, Smart Monitor will make the decision to turn on/off the WLANs.

AP will send an event to notify SCG that smart monitor has turned off WLANs when AP lost its gateway. But there is an issue occurred that AP has already lost its gateway, it also could not reach the SCG. Thus, the event cannot be sent until the connection is recovered.

- When smart monitor turned off WLANs, AP sends a log to syslog. Thus the related log is got locally from AP's syslog.
- AP should send this event to SCG once Smart Monitor recovered the WLAN. The event should carry the timestamp to record when WLANs has been turned off and on by smart monitor.

🔗 **Note:** Refer to [Alarm Types](#) and [Events Types](#) 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.

**Parent topic:** [Alarm and Event Management](#)

# Alarm Types

---

[Introduction](#)

[Accounting Alarms](#)

[AP Authentication Alarms](#)

[AP Communication Alarms](#)

[AP LBS Alarms](#)

[AP State Change Alarms](#)

[AP 3rd Radio](#)

[Authentication Alarms](#)

[Control and Data Plane Interface Alarms](#)

[Cloud Alarms](#)

[Cluster Alarms](#)

[Configuration Alarms](#)

[Data Plane Alarms](#)

[Data Streaming Alarms](#)

[Gn/S2a Interface Alarms](#)

[GR Interface Alarms](#)

[IPMI Alarms](#)

[Licensing Alarms](#)

[PMIPv6 Alarms](#)

[SCI Alarms](#)

[Session Alarms](#)

[System Alarms](#)

[Switch](#)

## Threshold Alarms

### Tunnel Alarms - Access Point

# 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.

Parent topic: [Alarm Types](#)

## Accounting Alarms

The following alarms are related to accounting.

- [Accounting server not reachable](#)
- [Accounting Failed Over to Secondary](#)
- [Accounting Fallback to Primary](#)
- [AP Accounting Message Mandatory Parameter Missing](#)
- [AP Accounting Message Decode Failed](#)
- [AP Account Message Drop While No Accounting Start Message](#)
- [Unauthorized CoA/DM message dropped](#)

Parent topic: [Alarm Types](#)

## Accounting server not reachable


**Table 1.** Accounting server not reachable alarm

Alarm	Accounting server not reachable
Alarm Type	accSrvrNotReachable
Alarm Code	1602
Severity	Major

Alarm	Accounting server not reachable
Aggregation Policy	An alarm is raised for every event from the event code 1602. A single event triggers a single alarm.
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 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.

Parent topic: [Accounting Alarms](#)

## Accounting Failed Over to Secondary

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** Accounting Failed Over to Secondary Alarm

Alarm	Accounting failed over to secondary
Alarm Type	accFailedOverToSecondary
Alarm Code	1653
Severity	Major

Alarm	Accounting failed over to secondary
Aggregation Policy	An alarm is raised for every event from the event code 1653. A single event triggers a single alarm.
Attribute	<pre> "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" </pre>
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.

Parent topic: [Accounting Alarms](#)

## Accounting Fallback to Primary

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** Accounting Fallback to Primary Alarm

Alarm	Accounting fallback to primary
Alarm Type	accFallbackToPrimary
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.

Alarm	Accounting fallback to primary
Attribute	<pre> "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" </pre>
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.

Parent topic: [Accounting Alarms](#)

## AP Accounting Message Mandatory Parameter Missing

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** AP Accounting Message Mandatory Parameter Missing Alarm

Alarm	AP accounting message mandatory parameter missing
Alarm Type	apAcctMsgMandatoryPrmMissing
Alarm Code	1901
Severity	Critical

Alarm	AP accounting message mandatory parameter missing
Aggregation Policy	From the event code 1901 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	<pre> “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” </pre>
Displayed on the web interface	[[srcProcess]] Mandatory attribute missing in Accounting Packet received from AP [[apIpAddress]] on {produce.short.name} [[SCGMgmtIp]], with username [[ueImsi]]@{realm}}
Description	This alarm is triggered when the controller fails to find the mandatory parameter in the RADIUS accounting message received from the AP. This mandatory parameter is required for generating the WAN-CDR.
Recommended Action	Download the RADIUS log file from the web interface to check the error cause.

Parent topic: [Accounting Alarms](#)

## AP Accounting Message Decode Failed


 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** AP Accounting Message Decode Failed Alarm

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

Parent topic: [Accounting Alarms](#)

## AP Account Message Drop While No Accounting Start Message


 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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 <b>Acct Interim/Stop</b> message as account start is not received from the AP.
Recommended Action	Check the accounting retransmit timer and retransmit count in the Access Point (AP) configuration. Also check if the interface from the AP to the controller is congested.

Parent topic: [Accounting Alarms](#)

## Unauthorized CoA/DM message dropped

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Accounting Alarms](#)

## AP Authentication Alarms

The following alarms are related to AP authentication.

- [RADIUS server unreachable](#)
- [LDAP server unreachable](#)

- [AD server unreachable](#)
- [WeChat ESP authentication server unreachable](#)
- [WeChat ESP authentication server unresolvable](#)
- [WeChat ESP DNAT server unreachable](#)
- [WeChat ESP DNAT server unresolvable](#)

Parent topic: [Alarm Types](#)

## RADIUS server unreachable

**Table 1.** 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.

Parent topic: [AP Authentication Alarms](#)

## LDAP server unreachable

**Table 1.** 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.

Parent topic: [AP Authentication Alarms](#)

## AD server unreachable

**Table 1.** AD server unreachable alarm

Alarm	AD server unreachable
Alarm Type	adServerUnreachable
Alarm Code	2142
Severity	Major
Aggregation Policy	From the event code 2142 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="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.

Parent topic: [AP Authentication Alarms](#)

## WeChat ESP authentication server unreachable

**Table 1.** WeChat ESP authentication server unreachable alarm

Alarm	WeChat ESP authentication server unreachable
Alarm Type	espAuthServerUnreachable

Alarm	WeChat ESP authentication server unreachable
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.

Parent topic: [AP Authentication Alarms](#)

## WeChat ESP authentication server unresolvable

**Table 1.** WeChat ESP authentication server unresolvable alarm

Alarm	WeChat ESP authentication server unresolvable
Alarm Type	espAuthServerUnResolvable
Alarm Code	2154
Severity	Major

Alarm	WeChat ESP authentication server unresolvable
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-8484-82919275dc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2153.
Displayed on the web interface	AP [{apName}&apMac]} is unable to resolve WeChat ESP authentication server domain name [{dn}] to IP
Description	This alarm is triggered when AP is unable to resolve WeChat ESP authentication server domain name.
Recommended Actions	Check the DNS server configuration settings in the controller web interface.

Parent topic: [AP Authentication Alarms](#)

## WeChat ESP DNAT server unreachable

**Table 1.** 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","zo

Alarm	WeChat ESP DNAT server unreachable
	neUUID="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.

Parent topic: [AP Authentication Alarms](#)

## WeChat ESP DNAT server unresolvable

**Table 1.** 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.

Alarm	WeChat ESP DNAT server unresolvable
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.

Parent topic: [AP Authentication Alarms](#)

## AP Communication Alarms

Following are the alarms related to access point communications.

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

Parent topic: [Alarm Types](#)

## AP rejected

**Table 1.** 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.

Parent topic: [AP Communication Alarms](#)

## AP configuration update failed

**Table 1.** AP configuration update failed alarm

Alarm	AP configuration update failed
Alarm Type	apConfUpdateFailed
Alarm Code	102

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

Parent topic: [AP Communication Alarms](#)

## AP swap model mismatched

**Table 1.** AP swap model mismatched alarm

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

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

Parent topic: [AP Communication Alarms](#)

## AP pre-provision model mismatched

**Table 1.** 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"

Alarm	AP pre-provision model mismatched
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.

Parent topic: [AP Communication Alarms](#)

## AP firmware update failed

**Table 1.** 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.

Alarm	AP firmware 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.

Parent topic: [AP Communication Alarms](#)

## AP WLAN oversubscribed


**Table 1.** 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"> <li>• Create a new WLAN group with WLANs. Ensure that it is not more than the AP's WLAN capacity. Apply the new WLAN group to either the AP or the AP's AP Group.</li> </ul>

Alarm	AP WLAN oversubscribed
	<ul style="list-style-type: none"> <li>Find the WLAN group used by the AP and reduce the number of WLAN.</li> </ul>

Parent topic: [AP Communication Alarms](#)

## AP join zone failed

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** AP join zone failed alarm

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

Alarm	AP join zone failed
	need to purchase additional licenses, in case of insufficient licenses.

Parent topic: [AP Communication Alarms](#)

## 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

**Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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"

Alarm	AP Image signing failed
Displayed on the web interface	AP Image Signing: The AP[{{apMac}}] with firmware version [{{fwVersion}}] is USI. USI to FSI upgrade is not allowed due to difference in Image formats.
Description	This alarm is triggered when the upgrade fails due to AP image mismatch.
Recommended Actions	<p>This issue of not able to upgrade from releases prior to or from 3.2.x to R3.6+ occurs as per the following category.</p> <ul style="list-style-type: none"> <li>• <b>Category 1:</b> AP firmware images for releases prior to 3.4.x is in the format USI (Un Signed Image)</li> <li>• <b>Category 2:</b> AP firmware images for releases 3.4.x and 3.5.x is in the format ISI (Intermediate Signed Image)</li> <li>• <b>Category 3:</b> AP firmware images for releases 3.6 and above is in the format FSI (Fully Signed Image)</li> </ul> <p>When upgrading from releases prior to 3.4 to 3.6.x and above, the AP image in category1 (USI) should be first upgraded to category 2 (ISI) and only then upgraded to category 3 (FSA). For example, move the AP image first to 3.4 or 3.5 zone and then to 3.6.x zone. If you attempt to do a direct upgrade (from USI to FSI) alarm 187 is triggered.</p> <p>If you are unable to upgrade the AP image using the controller web user interface, you can alternatively upgrade through TFTP or FTP using CLI mode as per the below steps.</p> <ul style="list-style-type: none"> <li>• <b>Step 1:</b> Configure FTP or TFTP server in the network with any image (even FSI for 3.6.x is allowed)</li> <li>• <b>Step 2:</b> Login to AP CLI and configure TFTP or FTP server IP address and image file name by</li> </ul>

Alarm	AP Image signing failed
	<p>using the command <code>fw set</code> and its related sub options.</p> <ul style="list-style-type: none"> <li>• <b>Step 3</b> Execute the command <code>fw update</code></li> <li>• <b>Step 4:</b> On completion of step 3 you can now upgrade the API image to <b>ISI &gt; FSI</b> using the controller web user interface.</li> </ul>

Parent topic: [AP Communication Alarms](#)

## AP LBS Alarms

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

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

Parent topic: [Alarm Types](#)

## No LS responses

**Table 1.** 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.

Alarm	No LS responses
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.

Parent topic: [AP LBS Alarms](#)

## LS authentication failure

**Table 1.** 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.

Alarm	LS authentication failure
Recommended Actions	The password needs to be corrected in the LBS service page.

Parent topic: [AP LBS Alarms](#)

## AP failed to connect to LS

**Table 1.** 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.

Parent topic: [AP LBS Alarms](#)

# AP State Change Alarms

Following are the alarms related to access point state changes:

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

Parent topic: [Alarm Types](#)

## AP rebooted by system

**Table 1.** 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"

Alarm	AP rebooted by system
Displayed on the web interface	AP [{apName}&apMac}] rebooted by the system because of [{reason}]
Description	<p>This alarm is triggered when any of the following occurs:</p> <ul style="list-style-type: none"> <li>• The system reboots the AP.</li> <li>• The SSH tunnel cipher is updated.</li> <li>• SSH/TLS key enhance mode is enabled.</li> <li>• SSH/TLS key enhance mode is disabled.</li> </ul>
Recommended Actions	Check the reasons for the reboot. If the reason is unknown, retrieve the AP support text and send it to RUCKUS support.

Parent topic: [AP State Change Alarms](#)

## AP disconnected

**Table 1.** 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"

Alarm	AP disconnected
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.

Parent topic: [AP State Change Alarms](#)

## AP deleted

**Table 1.** AP deleted alarm

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

Parent topic: [AP State Change Alarms](#)

## AP cable modem interface down

**Table 1.** 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.

Parent topic: [AP State Change Alarms](#)

## AP DHCP service failure

**Table 1.** AP DHCP service failure alarm

Alarm	Both primary and secondary DHCP server APs are down
Alarm Type	apDHCPServiceFailure
Alarm Code	341

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

Parent topic: [AP State Change Alarms](#)

## AP NAT failure

**Table 1.** 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.

Alarm	AP cable modem interface down NAT failure detected by controller due to three (3) consecutive NAT gateway APs are down
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.

Parent topic: [AP State Change Alarms](#)

## AP DHCP/NAT DWPD Ethernet port configuration override

**Table 1.** 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

Alarm	AP DHCP/NAT DWPD Ethernet port configuration override
	as <code>{{forwardingType}}</code> , 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.

Parent topic: [AP State Change Alarms](#)

## SZ DHCP/NAT DWPD Ethernet port configuration override

**Table 1.** 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	<code>{{ethPort}}</code> already configured as <code>{{forwardingType}}</code> for AP <code>[{apMac}]</code> . Overriding to LAN/Local Subnet by DHCP/NAT configuration.
Description	This alarm is triggered when the Ethernet port is already configured for the AP.

Parent topic: [AP State Change Alarms](#)

## SIM removal

**Table 1.** SIM removal alarm

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

Parent topic: [AP State Change Alarms](#)

## AP System Anomaly

**Table 1.** AP System Anomaly alarm

Alarm	AP System Anomaly
Alarm Type	apWritableRO
Alarm Code	285
Severity	Critical

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

Parent topic: [AP State Change Alarms](#)

## AP 3rd Radio

[apIllegalToChange3rdRadioBand](#)

[apIllegal6gVAPCreation](#)

Parent topic: [Alarm Types](#)

## apIllegalToChange3rdRadioBand

**Table 1.** apIllegalToChange3rdRadioBand event

Alarm	apIllegalToChange3rdRadioBand
Alarm Type	apIllegalToChange3rdRadioBand
Alarm Code	356
Severity	Major
Attribute	"apName"="xxxxx", 'apMac'='xx:xx:xx:xx:xx:xx',"curBand"="xxxxx", "newBand"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] failed to change the 3rd Radio BAND from [{curBand}] to [{newBand}].
Description	This alarm triggers when the BAND change for 3rd radio is not allowed due to Country Configuration

Parent topic: [AP 3rd Radio](#)

## apIllegal6gVAPCreation

**Table 1.** apIllegal6gVAPCreation event

Alarm	apIllegal6gVAPCreation
Alarm Type	apIllegal6gVAPCreation
Alarm Code	357
Severity	Major
Attribute	"apName"="xxxxx","apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] failed to create 3rd Radio VAP for some WLANs, please look for event 357 in the event page for more detail.
Description	This alarm triggers when 6G Radio received the WLAN's with security is other than WPA3 and OWE

Parent topic: [AP 3rd Radio](#)

## Authentication Alarms

The following are the alarms related to authentication.

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

Parent topic: [Alarm Types](#)

## Authentication server not reachable

**Table 1.** Authentication server not reachable alarm

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

Parent topic: [Authentication Alarms](#)

## Authentication failed over to secondary

**Table 1.** 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	"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]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.

Parent topic: [Authentication Alarms](#)

## Authentication fallback to primary

**Table 1.** Authentication fallback to primary alarm

Alarm	Authentication fallback to primary
Alarm Type	authFallbackToPrimary

Alarm	Authentication fallback to primary
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	"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 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.

Parent topic: [Authentication Alarms](#)

## AD/LDAP connectivity failure

**Table 1.** AD/LDAP connectivity failure alarm

Alarm	AD/LDAP connectivity failure
Alarm Type	racADLDAPFail
Alarm Code	1752

Alarm	AD/LDAP connectivity failure
Severity	Major
Aggregation Policy	From the event code 1752 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	<code>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12,</code> <code>"srcProcess"="RAC", "authSrvrIp"="1.1.1.1",</code> <code>"SCGMgmtIp"="2.2.2.2"</code>  <code>"desc"= "Connection to AD/LDAP fails"</code>
Displayed on the web interface	[[srcProcess]] Connect to AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]]
Description	This alarm is triggered when RADIUS server fails to connect with AD/LDAP server.
Recommended Actions	<ul style="list-style-type: none"> <li>• Check whether AD/LDAP server instance is running on the target machine</li> <li>• Check whether the AD/LDAP server can be reached from the controller</li> <li>• Verify if AD/LDAP server instances are listening on ports 3268 and 389</li> <li>• Verify if the requests are reaching AD/LDAP servers by any packet capture tool (tcpdump, wireshark)</li> </ul>

Parent topic: [Authentication Alarms](#)

## Bind fails with AD/LDAP

**Table 1.** 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	<p>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12,  "srcProcess"="RAC", "authSrvrIp"= "1.1.1.1",  "username"="testuser"</p> <p>"SCGMgmtIp"="2.2.2.2", "desc"="Bind to AD/LDAP fails"</p>
Displayed on the web interface	[[srcProcess]] Bind to AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]] for User[[userName]]
Description	This alarm is triggered when RADIUS server binding fails to AD/LDAP server.
Recommended Actions	<ul style="list-style-type: none"> <li>• Verify the base and administrator domain names as configured in the controller web interface</li> <li>• Verify the administrator user name and password as configured in the controller web interface</li> <li>• Verify whether the configured administrator user name and password is authenticated by the AD/LDAP servers</li> </ul>

Parent topic: [Authentication Alarms](#)

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

**Table 1.** 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	<p>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"= "testuser"</p> <p>"SCGMgmtIp"="2.2.2.2", "desc"="Fail to find password"</p>
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.

Parent topic: [Authentication Alarms](#)

## RADIUS fails to connect to AD NPS server

**Table 1.** 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"> <li>• Verify if the configured NPS server instance is up and running (Network Policy Server)</li> <li>• Verify if the NPS server instance is communicating on the standard RADIUS port 1812</li> <li>• Ensure that Windows server where AD/NPS server is provisioned can be reached from the controller web interface</li> </ul>

Parent topic: [Authentication Alarms](#)

## RADIUS fails to authenticate with AD NPS server

**Table 1.** 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	<p>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12,  "srcProcess"="RAC", "authSrvrIp"="1.1.1.1",  "username"="testuser"</p> <p>"SCGMgmtIp"="2.2.2.2", "desc"="Fails to authenticate with AD NPS"</p>
Displayed on the web interface	[[srcProcess]] Fails to authenticate AD NPS[[authSrvrIp]] on SCG[[SCGMgmtIp]] for User[[userName]]
Description	This alarm is triggered when the RADIUS server fails to authenticate with the AD NPS server.
Recommended Actions	<ul style="list-style-type: none"> <li>• The shared secret for NPS server should be same as that of administrator password provisioned in the controller web interface for AD server</li> <li>• NPS should be configured to accept request (CHAP and MSCHAPv2) from the controller</li> <li>• For CHAP authentication to work the AD server should store the password in reversible encryption format</li> <li>• Ensure that NPS is registered with AD server</li> </ul>

**Note:**

Refer to [Authentication Events](#).

Parent topic: [Authentication Alarms](#)

## Fails to establish TLS tunnel with AD/LDAP

**Table 1.** 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.

Parent topic: [Authentication Alarms](#)

## RAC DNS Resolve Failed

**Table 1.** racDNSResolveFailed

Alarm	RAC DNS fails to resolve the FQDN for AAA
Alarm Type	racDNSResolveFailed
Alarm Code	1771
Severity	Major
Attribute	"mvnold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd"  "SCGMgmtIp"="10.174.75.68"  "FQDNName"="ruckus.test.com"
Displayed on the web interface	[[srcProcess]] Fails to connect to resolve the FQDN [[FQDNName]] from SCG[[SCGMgmtIp]]
Description	This alarm occurs when RADIUS fails to resolve the FQDN of AAA.

Parent topic: [Authentication Alarms](#)

## 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](#)

Parent topic: [Alarm Types](#)

## GtpManager (DP) disconnected

**Table 1.** GtpManager (DP) disconnected alarm

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

Parent topic: [Control and Data Plane Interface Alarms](#)

## Cloud Alarms

[Cloud Analytics Service has been Enabled](#)

## Cloud Analytics Service has been Disabled

### Cloud Analytics Disconnected

Parent topic: [Alarm Types](#)

## Cloud Analytics Service has been Enabled

**Table 1.** Cloud Analytics Service has been Enabled Alarm

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

Parent topic: [Cloud Alarms](#)

## Cloud Analytics Service has been Disabled

**Table 1.** Cloud Analytics Service has been Disabled Alarm

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

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

Parent topic: [Cloud Alarms](#)

## Cloud Analytics Disconnected

**Table 1.** Cloud Analytics Disconnected Alarm

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

Parent topic: [Cloud Alarms](#)

## Cluster Alarms

Following are the alarms related to cluster:

- [New node failed to join](#)
- [Node removal failed](#)
- [Node out of service](#)

- Cluster in maintenance state
- Cluster backup failed
- Cluster restore failed
- Cluster upgrade failed
- Cluster application stopped
- Node bond interface down
- Node physical interface down
- Cluster node rebooted
- Cluster node shut down
- Disk usage exceed threshold
- Cluster out of service
- Cluster upload AP firmware failed
- Cluster add AP firmware failed
- Unsync NTP time
- Cluster upload KSP file failed
- Configuration backup failed
- Configuration restore failed
- AP certificate updated
- Upgrade SS table failed
- Cluster redundancy sync configuration failed
- Cluster redundancy restoring configuration failed
- Not all APs rehome after timeout
- Over switch max capacity

- [AP is connected to Standby Cluster Over The Expiration Date](#)
- [Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy](#)
- [External DP Connected to Standby Cluster after Rehome Timeout](#)

Parent topic: [Alarm Types](#)

## New node failed to join

**Table 1.** New node failed to join alarm

Alarm	New node failed to join
Alarm Type	newNodeJoinFailed
Alarm Code	801
Severity	Critical
Aggregation Policy	From the event code 803 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 802.
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	New node [{nodeMac}] ([{nodeName}]) failed to join cluster [{clusterName}]
Description	This alarm is triggered when a node fails to join a cluster session. The web interface displays the error message.
Recommended Actions	When the operation fails, the user can run the <b>join process</b> . If it continues to fail, please send the complete system log files (stored in the path <code>-/opt/ruckuswireless/controller/log/system</code> for analysis to RUCKUS support. Possible causes are:

Alarm	New node failed to join
	<ul style="list-style-type: none"> <li>The joining node is unable to complete the syncing of data in time. This could be due to the existing node performing compaction/repair etc.</li> <li>The communication between the nodes may be broken. This could cause the operation to timeout such as IP address change or due to other events, which affects the network. Usually, it does not last for a long period of time.</li> </ul>

Parent topic: [Cluster Alarms](#)

## Node removal failed

**Table 1.** 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}].

Alarm	Node removal failed
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 <code>-/opt/ruckuswireless/controller/log/system</code> for analysis to RUCKUS support.

Parent topic: [Cluster Alarms](#)

## Node out of service

**Table 1.** 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.

Alarm	Node out of service
Recommended Actions	The operator/user needs to check the application/ interface state.

Parent topic: [Cluster Alarms](#)

## Cluster in maintenance state

**Table 1.** Cluster in maintenance state alarm

Alarm	Cluster in maintenance state
Alarm Type	clusterInMaintenanceState
Alarm Code	804
Severity	Critical
Aggregation Policy	From the event code 807 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 808.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] is in maintenance state
Description	This alarm is triggered when a cluster is in a maintenance state.
Recommended Actions	<p>Possible causes:</p> <ul style="list-style-type: none"> <li>• The entire system backup is in process.</li> <li>• In a two-node cluster, the remove-node process is working.</li> </ul>

Alarm	Cluster in maintenance state
	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.

Parent topic: [Cluster Alarms](#)

## Cluster backup failed

**Table 1.** 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	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:

Alarm	Cluster backup failed
	<ul style="list-style-type: none"> <li>• Insufficient disk space.</li> <li>• Communication between nodes may be broken.</li> <li>• Errors due to the underlying Python script.</li> </ul>

Parent topic: [Cluster Alarms](#)

## Cluster restore failed

**Table 1.** Cluster restore failed alarm

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

Alarm	Cluster restore failed
	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.

Parent topic: [Cluster Alarms](#)

## Cluster upgrade failed

**Table 1.** 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	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

Alarm	Cluster upgrade failed
	<p>log files (stored in the path - /opt/ ruckuswireless/ controller/log/system to RUCKUS support for analysis. Possible causes:</p> <ul style="list-style-type: none"> <li>• Insufficient disk space</li> <li>• Communication between nodes might be broken.</li> <li>• Errors due to the underlying Python script.</li> </ul>

Parent topic: [Cluster Alarms](#)

## Cluster application stopped

**Table 1.** Cluster application stopped alarm

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

Alarm	Cluster application 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 <code>-/opt/ ruckuswireless/controller/log/system</code> to the application owner for analysis.

Parent topic: [Cluster Alarms](#)

## Node bond interface down

**Table 1.** 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.

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

Parent topic: [Cluster Alarms](#)

## Node physical interface down

**Table 1.** Node physical interface down alarm

Alarm	Node physical interface down
Alarm Type	nodePhyInterfaceDown
Alarm Code	810
Severity	Critical
Aggregation Policy	From the event code 824 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 825.
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx: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

Alarm	Node physical interface down
	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.

Parent topic: [Cluster Alarms](#)

## Cluster node rebooted

**Table 1.** 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.

Parent topic: [Cluster Alarms](#)

## Cluster node shut down

**Table 1.** Cluster node shut down alarm

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

Parent topic: [Cluster Alarms](#)

## Node IP Changed

**Table 1.** Node IP Changed alarm

Alarm	Node IP Changed
Alarm Type	nodeIPChanged
Alarm Code	823

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

Parent topic: [Cluster Alarms](#)

## Disk usage exceed threshold

**Table 1.** 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} %.

Alarm	Disk usage exceed threshold
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.

Parent topic: [Cluster Alarms](#)

## Cluster out of service

**Table 1.** 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.

Parent topic: [Cluster Alarms](#)

## Cluster upload AP firmware failed

**Table 1.** 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.

Parent topic: [Cluster Alarms](#)

## Cluster add AP firmware failed

**Table 1.** Cluster add AP firmware failed alarm

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

Alarm	Cluster add AP firmware failed
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.

Parent topic: [Cluster Alarms](#)

## Unsync NTP time

**Table 1.** 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"

Alarm	Unsync NTP time
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.

Parent topic: [Cluster Alarms](#)

## Cluster upload KSP file failed

**Table 1.** 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.

Parent topic: [Cluster Alarms](#)

## Configuration backup failed

**Table 1.** 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.

Parent topic: [Cluster Alarms](#)

## Configuration restore failed

**Table 1.** Configuration restore failed alarm

Alarm	Configuration restore failed
Alarm Type	clusterCfgRestoreFailed
Alarm Code	864

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

Parent topic: [Cluster Alarms](#)

## AP certificate updated

**Table 1.** 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.

Alarm	AP certificate updated
Attribute	"count"="XXX"
Displayed on the web interface	[[count]] APs need to update their certificates.
Description	This alarm is triggered when the AP certificate expires.
Recommended Actions	Certificates on some APs need to be refreshed. On the web interface navigate to <b>Administration &gt; AP Certificate</b> replacement page to verify and follow the certificate refresh process.

Parent topic: [Cluster Alarms](#)


## Upgrade SS table failed

**Table 1.** 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.

Parent topic: [Cluster Alarms](#)

## Cluster redundancy sync configuration failed


 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** Cluster redundancy sync configuration failed alarm

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

Parent topic: [Cluster Alarms](#)

## Cluster redundancy restoring configuration failed

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** Cluster redundancy restoring configuration failed alarm

Alarm	Cluster redundancy restoring configuration failed
Alarm Type	clusterRedundantRestoreCfgFailed
Alarm Code	877

Alarm	Cluster redundancy restoring configuration failed
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.

Parent topic: [Cluster Alarms](#)

## Not all APs rehome after timeout

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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.

Alarm	Not all APs rehome after timeout
Description	This alarm is triggered when the AP is still connected to the standby cluster.

Parent topic: [Cluster Alarms](#)

## Over switch max capacity

**Table 1.** Over switch max capacity alarm

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

Parent topic: [Cluster Alarms](#)

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

**Table 1.** AP is connected to standby cluster over the expiration date alarm

Alarm	AP Certificate Expired
Alarm Type	ApConnectedToStandbyClusterOverTheExpirationDate
Alarm Code	188
Severity	Critical

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

Parent topic: [Cluster Alarms](#)

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

**Table 1.** Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy alarm

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

Parent topic: [Cluster Alarms](#)

## External DP Connected to Standby Cluster after Rehome Timeout

**Table 1.** External DP Connected to Standby Cluster after Rehome Timeout alarm

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

Parent topic: [Cluster Alarms](#)

## Certificate is about to Expire

**Table 1.** Certificate is about to Expire alarm

Alarm	Certificate is about to Expire
Alarm Type	certificateAboutToExpire
Alarm Code	890
Severity	Major
Aggregation Policy	From the event code 890 an alarm is raised for every event. A single event triggers a single alarm.

Alarm	Certificate is about to Expire
Auto Clearance	
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate [{certName}] is about to expire in [{days}] days [{expireDateTime}]
Description	This alarm occurs when a certificate is about to expire.
Recommended Actions	Renew the certificate that is about to expire or import another valid certificate to replace the current one.

Parent topic: [Cluster Alarms](#)

## Certificate is already Expired

**Table 1.** Certificate is already Expired alarm

Alarm	Certificate is already Expired
Alarm Type	restoreClusterExpired
Alarm Code	891
Severity	Major
Aggregation Policy	From the event code 891 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate [{certName}] is already expired since {expireDateTime}

Alarm	Certificate is already Expired
Description	This alarm occurs when certificate already expires.
Recommended Actions	Renew the certificate that already expires or import another valid certificate to replace the current one.

Parent topic: [Cluster Alarms](#)

## Configuration Alarms

Following are the alarms related to configuration.

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

Parent topic: [Alarm Types](#)

## Zone configuration preparation failed

**Table 1.** 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.

Alarm	Zone configuration preparation failed
Attribute	"nodeMac"="50:A7:33:24:E7:90","zoneName"="open Zone"
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.

Parent topic: [Configuration Alarms](#)

## AP configuration generation failed

**Table 1.** 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"="open Zone","apCfgGenFailedCount"="25"
Displayed on the web interface	Failed to generate configuration for [{apCfgGenFailedCount}] AP(s) under zone[{zoneName}]

Alarm	AP configuration generation failed
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.

Parent topic: [Configuration Alarms](#)

## End-of-life AP model detected

**Table 1.** 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"="open Zone","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	These obsoleted APs occupies licensed AP space. Disconnect these unsupported AP models from the given zone by:

Alarm	End-of-life AP model detected
	<ul style="list-style-type: none"> <li>Reset the APs to a factory setting using the AP command line</li> <li>Delete these APs through the <b>controller Web Interface &gt; Configuration AP List</b></li> </ul>

 **Note:**

Refer to [Configuration Events](#).

Parent topic: [Configuration Alarms](#)

## VLAN configuration mismatch on non DHCP/NAT WLAN

**Table 1.** VLAN configuration mismatch on non DHCP/NAT WLAN alarm

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

Alarm	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN
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.

Parent topic: [Configuration Alarms](#)

## VLAN configuration mismatch on DHCP/NAT WLAN

**Table 1.** 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"="xxxx", "wlanID"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [{apMac}] detected VLAN configuration mismatch on DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This alarm is triggered when the AP detects a DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

Parent topic: [Configuration Alarms](#)

# Data Plane Alarms

 **Note:**

Alarms 510, 516, 517 and 519 are supported on the SZ300 controllers only and not applicable for vSZ-H.

The following alarms are related to data plane.

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

Parent topic: [Alarm Types](#)

## Data plane configuration update failed

**Table 1.** 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: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.

Parent topic: [Data Plane Alarms](#)

## Data plane disconnected

**Table 1.** Data plane disconnected alarm

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

Parent topic: [Data Plane Alarms](#)

## Data plane physical interface down


**Table 1.** Data plane physical interface down alarm

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

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

Parent topic: [Data Plane Alarms](#)

## Data plane rebooted

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** Data plane rebooted alarm

Alarm	Data plane rebooted
Alarm Type	dpReboot
Alarm Code	510
Severity	Minor

Alarm	Data plane rebooted
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: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.

Parent topic: [Data Plane Alarms](#)

## Data plane packet pool is under low water mark

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** 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:xx", "id"="x"

Alarm	Data plane packet pool is under low water mark
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.

Parent topic: [Data Plane Alarms](#)

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

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** 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.

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

Parent topic: [Data Plane Alarms](#)

## Data plane core dead

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Data Plane Alarms](#)


## Data plane process restarted

**Table 1.** 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.
Recommended Actions	No action required.

Parent topic: [Data Plane Alarms](#)

## Data plane license is not enough

 **Note:** Alarm 538 is applicable only for vSZ-H.


**Table 1.** Data plane license is not enough alarm

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

Alarm	Data plane license is not enough
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.


Parent topic: [Data Plane Alarms](#)

## Data plane upgrade failed

 **Note:** Alarm 553 is applicable only for vSZ-H

**Table 1.** 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.

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

Parent topic: [Data Plane Alarms](#)

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

**Table 1.** 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.

Parent topic: [Data Plane Alarms](#)

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

**Table 1.** 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	Data plane fails to connects to the other data plane
Alarm Code	1261
Severity	Major
Aggregation Policy	From the event code 1261 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] fails connects to the other Data Plane[{targetDpKey&&targetDpIP}]
Description	This alarm is triggered when the data plane fails to connect to another data plane.
Recommended Actions	Check the connectivity between data planes.

Parent topic: [Data Plane Alarms](#)

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

**Table 1.** Data plane DHCP IP pool usage rate is 100 percent alarm

Alarm	Data plane DHCP IP pool usage rate is 100 percent
Alarm Type	dpDhcpIpPoolUsageRate100
Alarm Code	1265
Severity	Critical
Aggregation Policy	From the event code 1265 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"

Alarm	Data plane DHCP IP pool usage rate is 100 percent
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.

Parent topic: [Data Plane Alarms](#)

## Data Streaming Alarms

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

Parent topic: [Alarm Types](#)


### Connecting Failure to a Data Streaming Profile

**Table 1.** Connecting Failure to a Data Streaming Profile alarm

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

Parent topic: [Data Streaming Alarms](#)

# Gn/S2a Interface Alarms


 **Note:** The Gn/S2a interface alarms are supported on the SmartZone 300 controllers only. These alarms are not applicable for vSZ-H controllers.

The following alarms are related to Gn/S2a interface.

- [GGSN restarted](#)
- [GGSN not reachable](#)
- [GGSN not resolved](#)
- [PDNGW could not be resolved](#)
- [PDNGW version not supported](#)
- [Associated PDNGW down](#)
- [Create session response failed](#)
- [Decode failed](#)
- [Modify bearer response failed](#)
- [Delete session response failed](#)
- [Delete bearer request failed](#)
- [Update bearer request failed](#)
- [CGF server not configured](#)

Parent topic: [Alarm Types](#)

## GGSN restarted


 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Gn/S2a Interface Alarms](#)

## GGSN not reachable

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** GGSN not reachable alarms

Alarm	GGSN not reachable
Alarm Type	ggsnNotReachable

Alarm	GGSN not reachable
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.

Parent topic: [Gn/S2a Interface Alarms](#)

## GGSN not resolved

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** GGSN not resolved alarm

Alarm	GGSN not resolved
Alarm Type	ggsnNotResolved
Alarm Code	1215

Alarm	GGSN not resolved
Severity	Major
Aggregation Policy	From the event code 1215 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	<pre> “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”, </pre>
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.

Parent topic: [Gn/S2a Interface Alarms](#)

## PDNGW could not be resolved

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** PDNGW could not be resolved alarm

Alarm	PDNGW could not be resolved
Alarm Type	pdnGwNotResolved

Alarm	PDNGW could not be resolved
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.

Parent topic: [Gn/S2a Interface Alarms](#)

## PDNGW version not supported

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** PDNGW version not supported alarm

Alarm	PDNGW version not supported
Alarm Type	pdnGwVersionNotSupportedMsgReceived
Alarm Code	1952

Alarm	PDNGW version not supported
Severity	Major
Aggregation Policy	From the event code 1952 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	<code>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff"</code> <code>"srcProcess"="sm_process" "realm"="NA"</code> <code>"gtpclp"="5.5.5.5" "pgwlp"="1.1.1.1"</code> <code>"SCGMgmtIp"="2.2.2.2"</code>
Displayed on the web interface	[[srcProcess]] Version not supported message received from PDN GW with IP [[pgwlp]] on {produce.short.name} [[SCGMgmtIp]].
Description	This alarm is triggered when the version is not supported for messages received from PDN GW.
Recommended Actions	Verify and correct the GPRS tunneling protocol (GTP) version supported in the PGW is GTPv1 and GTPv2.

Parent topic: [Gn/S2a Interface Alarms](#)

## Associated PDNGW down

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** Associated PDNGW down alarm

Alarm	Associated PDNGW down
Alarm Type	pdnGwAssociationDown
Alarm Code	1953
Severity	Critical

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

Parent topic: [Gn/S2a Interface Alarms](#)

## Create session response failed

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** 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.

Alarm	Create session response failed
Attribute	<pre> “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” “pgwIp”=“1.1.1.1” “SCGMgmtIp”=“2.2.2.2” “ueMacAddr”=“aa:bb:cc:gg:hh:ii” “ueImei”=“12345” “ueMsisdn”=“98787” “apn”=“ruckus.com” “cause”=“&lt;reason for failure&gt;” </pre>
Displayed on the web interface	<pre> [{{srcProcess}}] Create Session response from PDN GW with IP [{{pgwIp}}] on {produce.short.name} [{{SCGMgmtIp}}] failed, for UE with username [{{ueImei}}@{realm}] because [{{cause}}] </pre>
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.

Parent topic: [Gn/S2a Interface Alarms](#)

## Decode failed

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.


**Table 1.** 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.

Alarm	Decode failed
Attribute	<pre>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"= "NA" "gtpclp"="5.5.5.5" "pgwlp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2"</pre>
Displayed on the web interface	[[srcProcess]] Decode of message received from PDN GW with IP [[pgwlp]] on {produce.short.name} [[SCGMgmtIp]] 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.

Parent topic: [Gn/S2a Interface Alarms](#)

## Modify bearer response failed

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** 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	<pre>"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" "SCGMgmtIp"="2.2.2.2"</pre>

Alarm	Modify bearer response failed
	<pre>"ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "apn"="ruckus.com" "cause"="&lt;reason for failure&gt;"</pre>
Displayed on the web interface	<pre>[[srcProcess]] Modify Bearer Response from PDN GW with IP [[pgwIp]] on {produce.short.name} [[SCGMgmtIp]] failed, for UE with username [[ueImsi]]@{realm}} because [[cause]]</pre>
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.

Parent topic: [Gn/S2a Interface Alarms](#)

## Delete session response failed

**Table 1.** 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	<pre>"mvnold"="12" "wlanId"="1" "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"=" wlan.mnc080.mcc405.3gppnetwork.org" "gtppIp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345"</pre>

Alarm	Delete session response failed
	<pre>"ueMsisdn"="98787" "apn"="ruckus.com" "cause"="&lt;reason for failure&gt;"</pre>
Displayed on the web interface	<pre>{{srcProcess}} Delete Session response from PDN GW with IP {{pgwIp}} on {produce.short.name} {{SCGMgmtIp}} failed, for UE with username {{ueImsi}}@{realm}} because {{cause}}</pre>
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.

Parent topic: [Gn/S2a Interface Alarms](#)

## Delete bearer request failed

**Table 1.** 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	<pre>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "gtpcIp"="5.5.5.5" "pgwIp"="1.1.1.1" "SCGMgmtIp"="2.2.2.2" "cause"="&lt;reason for failure&gt;"</pre>
Displayed on the web interface	<pre>{{srcProcess}} Delete Bearer Request from PDN GW with IP {{pgwIp}} on {produce.short.name}</pre>

Alarm	Delete bearer request failed
	[[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.

Parent topic: [Gn/S2a Interface Alarms](#)

## Update bearer request failed

**Table 1.** Update bearer request failed alarm

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

Parent topic: [Gn/S2a Interface Alarms](#)


## CGF server not configured

**Table 1.** 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.

Parent topic: [Gn/S2a Interface Alarms](#)

## GR Interface Alarms

 **Note:** This section is not applicable for vSZ-H.

Following are the alarms related to GR interface.

- [Destination not reachable](#)
- [App server down](#)
- [App server inactive](#)
- [Association establishment failed](#)
- [Association down](#)
- [Outbound routing failure](#)
- [Did allocation failure](#)

Parent topic: [Alarm Types](#)

## Destination not reachable

**Table 1.** 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

Alarm	Destination not reachable
Description	This alarm is triggered when the point code is unreachable due to a pause indicator.
Recommended Actions	Manual intervention is required.

Parent topic: [GR Interface Alarms](#)

## App server down

**Table 1.** 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)

Alarm	App server down
	received from the remote IP security protocol (IPSP) or signalling gateway (SG).
Recommended Actions	Manual intervention is required.

Parent topic: [GR Interface Alarms](#)

## App server inactive

**Table 1.** 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

Alarm	App server inactive
	(ASP_INACTIVE_ACK) from remote IP security protocol (IPSP) or signalling gateway (SG).
Recommended Actions	Manual intervention is required.

Parent topic: [GR Interface Alarms](#)

## Association establishment failed

**Table 1.** 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}]

Alarm	Association establishment failed
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.

Parent topic: [GR Interface Alarms](#)

## Association down

**Table 1.** Association down alarm

Alarm	Association down
Alarm Type	assocDown
Alarm Code	1627
Severity	Critical
Aggregation Policy	From the event code 1627 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1628.
Attribute	"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.

Alarm	Association down
Recommended Actions	Manual intervention is required.

Parent topic: [GR Interface Alarms](#)

## Outbound routing failure

**Table 1.** 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", "ueImsi"="04844624203918"
Displayed on the web interface	Unable to route [{operation}] for IMSI [{ueImsi}] 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.

Parent topic: [GR Interface Alarms](#)


## Did allocation failure

**Table 1.** Did allocation failure alarm

Alarm	Did allocation failure
Alarm Type	didAllocationFailure
Alarm Code	1637
Severity	Critical
Aggregation Policy	From the event code 1637 an alarm is raised for every 50 events. Alarm is raised for 50 or more events or events occurring within a span of 60 seconds.
Attribute	"mvnold"="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.

Parent topic: [GR Interface Alarms](#)

## IPMI Alarms

 **Note:** This section is not applicable for vSZ-H.

Following are the alarms related to IPMIs.

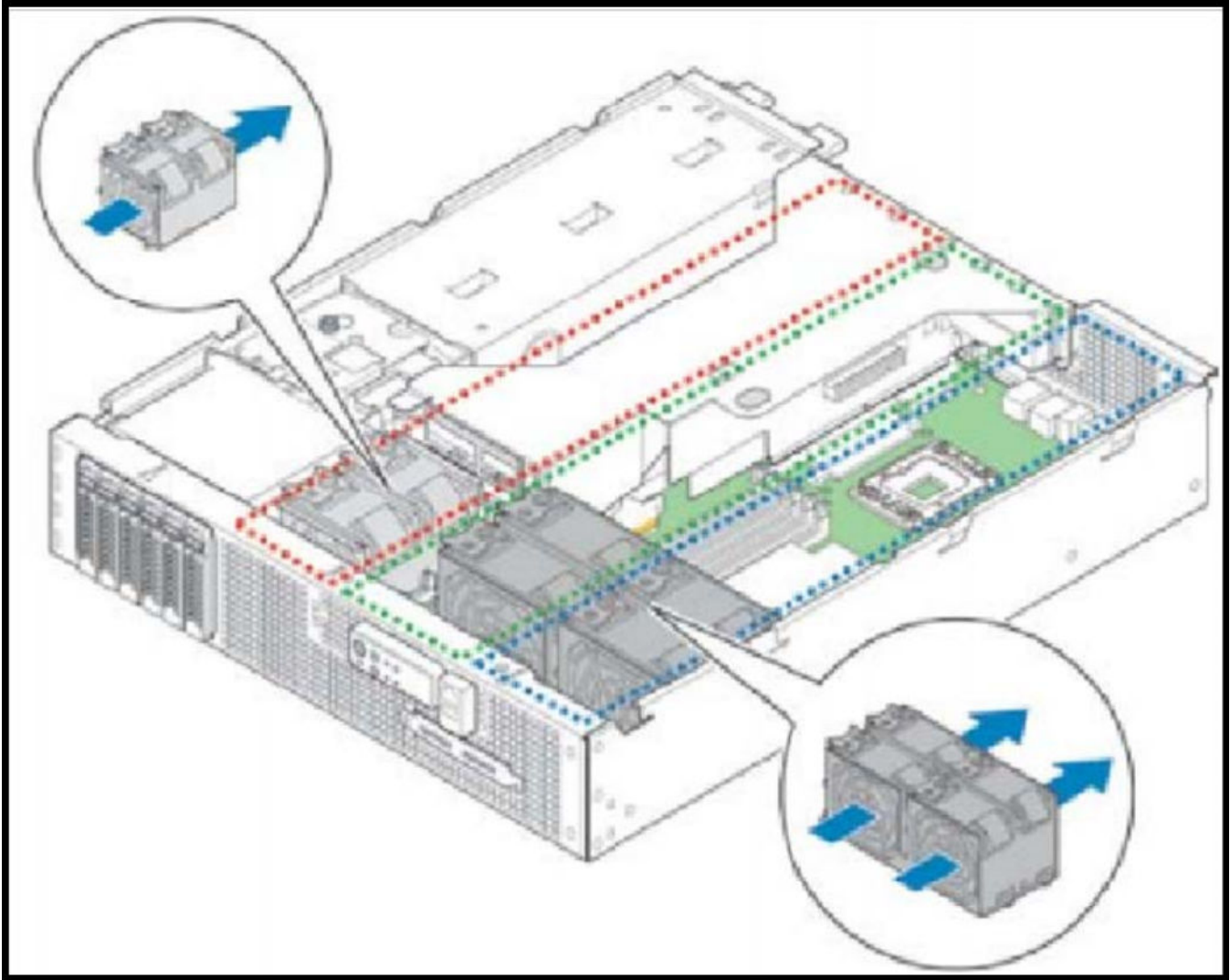
- [ipmiVoltage](#)
- [ipmiThempBB](#)
- [ipmiThempFP](#)

- [ipmiThempIOH](#)
- [ipmiThempMemP](#)
- [ipmiThempPS](#)
- [ipmiThempP](#)
- [ipmiThempHSBP](#)
- [ipmiFan](#)
- [ipmiPower](#)
- [ipmiCurrent](#)
- [ipmiFanStatus](#)
- [ipmiPsStatus](#)
- [ipmiDrvStatus](#)

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 1](#):

- 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 1.** Server Cooling Areas



Parent topic: [Alarm Types](#)

# ipmiVoltage

Table 1. ipmiVoltage alarm

Alarm	ipmiVoltage
Alarm Type	ipmiVotage
Alarm Code	901
Severity	Major

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

Parent topic: [IPMI Alarms](#)

## ipmiThempBB

**Table 1.** ipmiThempBB alarm

Alarm	ipmiThempBB
Alarm Type	ipmiThempBB
Alarm Code	902

Alarm	ipmiThempBB
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	This alarm is triggered due to the increase/decrease of the baseboard temperature status of the control plane. Baseboard threshold temperatures are in the range of 10 <sup>0</sup> Celsius to 61 <sup>0</sup> Celsius. The default threshold is 61 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

Parent topic: [IPMI Alarms](#)

## ipmiThempFP

**Table 1.** ipmiThempFP alarm

Alarm	ipmiThempFP
Alarm Type	ipmiThempFP
Alarm Code	903
Severity	Major

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

Parent topic: [IPMI Alarms](#)

## ipmiThempIOH

**Table 1.** 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.

Alarm	ipmiThempIOH
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 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

Parent topic: [IPMI Alarms](#)

## ipmiThempMemP

**Table 1.** 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.

Alarm	ipmiThempMemP
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 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

Parent topic: [IPMI Alarms](#)

## ipmiThempPS

**Table 1.** 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"

Alarm	ipmiThempPS
Displayed on the web interface	Power supply [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's power supply shows the status as either an increase/decrease in temperature. Power supply 1 and power supply 2 threshold temperatures are in the range of -20 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Recommended Actions	Replace the power supply cord. If the problem persists, decrease the ambient temperature.

Parent topic: [IPMI Alarms](#)

## ipmiThempP

**Table 1.** 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}]

Alarm	ipmiThempP
Description	This alarm is triggered when the reading surpasses threshold value is $\leq 55^{\circ}$ Celsius. The default threshold is $55^{\circ}\text{C}$ .
Recommended Actions	Check and replace the CPU fan module if required. Decrease the ambient temperature if the fan module is working.

Parent topic: [IPMI Alarms](#)

## ipmiThempHSBP

**Table 1.** ipmiThempHSBP alarm

Alarm	ipmiThempHSBP
Alarm Type	ipmiThempHSBP
Alarm Code	908
Severity	Major
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 $9^{\circ}$ Celsius to $55^{\circ}$ Celsius. The default threshold is $55^{\circ}\text{C}$ .

Alarm	ipmiThempHSBP
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

Parent topic: [IPMI Alarms](#)

## ipmiFan

**Table 1.** 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.

Parent topic: [IPMI Alarms](#)

## ipmiPower

**Table 1.** 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.
Recommended Actions	Replace the power supply cord.

Parent topic: [IPMI Alarms](#)

## ipmiCurrent

**Table 1.** ipmiCurrent alarm

Alarm	ipmiCurrent
Alarm Type	ipmiCurrent
Alarm Code	911

Alarm	ipmiCurrent
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.

Parent topic: [IPMI Alarms](#)

## ipmiFanStatus

**Table 1.** 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.

Alarm	ipmiFanStatus
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.

Parent topic: [IPMI Alarms](#)

## ipmiPsStatus

**Table 1.** ipmiPsStatus alarm

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

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

Parent topic: [IPMI Alarms](#)

## ipmiDrvStatus

**Table 1.** 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"="xxxx", "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.

Alarm	ipmiDrvStatus
Recommended Actions	The operator / user needs to replace the hard disk drive.

Parent topic: [IPMI Alarms](#)

## Licensing Alarms

### Note:

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

Following are the alarms related to licensing:

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

Parent topic: [Alarm Types](#)

## TTG session critical threshold

**Table 1.** TTG session critical threshold alarm

Alarm	TTG session critical threshold
Alarm Type	ttgSessionCriticalThreshold
Alarm Code	1242

Alarm	TTG session critical threshold
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.

Parent topic: [Licensing Alarms](#)

## TTG session license exhausted

**Table 1.** 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"

Alarm	TTG session license exhausted
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.

Parent topic: [Licensing Alarms](#)

## License going to expire

**Table 1.** License going to expire alarm

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

Parent topic: [Licensing Alarms](#)

## Insufficient license capacity

**Table 1.** 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.

Parent topic: [Licensing Alarms](#)

## Data plane DHCP IP license insufficient

**Table 1.** Data plane DHCP IP license insufficient alarm

Alarm	Data plane DHCP IP license insufficient
Alarm Type	dpDhcpIpLicenseNotEnough
Alarm Code	1277

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

Parent topic: [Licensing Alarms](#)

## Data plane NAT session license insufficient

**Table 1.** Data plane 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",

Alarm	Data plane NAT session license insufficient
	"availableLicenseCnt"="1234567890"
Displayed on the web interface	This alarm occurs when Data Plane NAT session license insufficient. ( total <code>[[totalLicenseCnt]]</code> , consumed <code>[[consumedLicenseCnt]]</code> , available <code>[[availableLicenseCnt]]</code> )
Description	This alarm is triggered when the data plane NAT server license is insufficient.

Parent topic: [Licensing Alarms](#)

## Insufficient license capacity

**Table 1.** Insufficient license capacity alarm

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

Parent topic: [Licensing Alarms](#)

# PMIPv6 Alarms

## Note:

This section is not applicable for vSZ-H.

Following are the alarms related to PMIPv6.

- [Config update failed](#)
- [DHCP connection lost](#)

Parent topic: [Alarm Types](#)

## Config update failed


**Table 1.** 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 triggered when the PMIPv6 gets an error or a negative acknowledgment or improper/incomplete information from the D-bus client.

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 if it is missing.

Parent topic: [PMIPv6 Alarms](#)

## DHCP connection lost

 **Note:** This alarm is not applicable for vSZ-H.

**Table 1.** DHCP connection lost alarm

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

Alarm	DHCP connection lost
Recommended Actions	Download the PMIPv6d and dynamic host configuration protocol (DHCP) server logs from the controller to check the error cause.

Parent topic: [PMIPv6 Alarms](#)

## SCI Alarms

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

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

Parent topic: [Alarm Types](#)

## Connect to SCI failure

**Table 1.** Connect to SCI failure alarm

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

Parent topic: [SCI Alarms](#)

## SCI has been disabled

**Table 1.** SCI has been disabled alarm

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

Parent topic: [SCI Alarms](#)


## SCI and FTP have been disabled

**Table 1.** SCI and FTP have been disabled alarm

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

Parent topic: [SCI Alarms](#)

## Session Alarms

 **Note:** This section is not applicable for vSZ-H.

Following is the alarm related to session.

- [Binding failed](#)

Parent topic: [Alarm Types](#)

## Binding failed

**Table 1.** 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 triggered when the mobile node binding fails.

Alarm	Binding failed
Recommended Actions	No action is required.

Parent topic: [Session Alarms](#)

## System Alarms

Following are the alarms with the system log severity:

 **Note:** {produce.short.name} refers to the controller.

- [No LS responses](#)
- [LS authentication failure](#)
- [{produce.short.name}](#)
- [Syslog server unreachable](#)
- [CSV export FTP maximum retry](#)
- [CSV export disk threshold exceeded](#)
- [CSV export disk max capacity reached](#)
- [Process restart](#)
- [Service unavailable](#)
- [Keepalive failure](#)
- [Resource unavailable](#)
- [HIP failed over](#)
- [Unconfirmed program detection](#)
- [Diameter initialization error](#)
- [Diameter peer transport failure](#)

- Diameter CER error
- Diameter peer add error
- Diameter peer remove successful
- Diameter realm entry error
- Diameter failover to alternate peer
- Diameter fail back to peer
- Diameter CEA unknown peer
- Diameter no common application
- Process initiated
- PMIPv6 unavailable
- Memory allocation failed
- The last one data plane is disconnected...

Parent topic: [Alarm Types](#)

## No LS responses

**Table 1.** 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"=""

Alarm	No LS responses
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.

Parent topic: [System Alarms](#)

## LS authentication failure

**Table 1.** LS authentication failure alarm

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

Parent topic: [System Alarms](#)

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

**Table 1.** {produce.short.name} failed to connect to LS alarm

Alarm	{produce.short.name} failed to connect to LS
Alarm Type	scgLBSCConnectFailed
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.

Parent topic: [System Alarms](#)

## Syslog server unreachable

**Table 1.** Syslog server unreachable alarm

Alarm	Syslog server unreachable
Alarm Type	syslogServerUnreachable
Alarm Code	751

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

Parent topic: [System Alarms](#)

## CSV export FTP maximum retry

**Table 1.** 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.

Alarm	CSV export FTP maximum retry
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.

Parent topic: [System Alarms](#)

## CSV export disk threshold exceeded

**Table 1.** 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	

Parent topic: [System Alarms](#)

## CSV export disk max capacity reached

**Table 1.** 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.
Recommended Actions	

Parent topic: [System Alarms](#)

## Process restart

**Table 1.** 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.

Alarm	Process restart
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.

Parent topic: [System Alarms](#)

## Service unavailable

**Table 1.** 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]]

Alarm	Service unavailable
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.

Parent topic: [System Alarms](#)

## Keepalive failure

**Table 1.** Keepalive failure alarm

Alarm	Keepalive failure
Alarm Type	keepAliveFailure
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 <b>mon/nc</b> restarts the process due to a keep alive failure.
Recommended Actions	Download the process log file from the controller web interface to locate the cause of the error.

Parent topic: [System Alarms](#)


# Resource unavailable

**Table 1.** Resource unavailable alarm

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

Parent topic: [System Alarms](#)

## HIP failed over

 **Note:** This alarm is not applicable for vSZ-H.

**Table 1.** HIP failed over alarm

Alarm	HIP failed over
Alarm Type	hipFailover
Alarm Code	1016
Severity	Major
Aggregation Policy	Alarm is raised for every event from event code 1016. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP",  "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	[[srcProcess]] Node transitioned to Active on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered when the standby host identity protocol (HIP) transits to an active node and is included in control plane identifier of the newly active HIP.
Recommended Actions	A manual intervention is required.

Parent topic: [System Alarms](#)

## Unconfirmed program detection


**Table 1.** Unconfirmed program detection alarm

Alarm	Unconfirmed program detection
Alarm Type	Unconfirmed Program Detection
Alarm Code	1019

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

Parent topic: [System Alarms](#)

## Diameter initialization error

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter initialization error alarm

Alarm	Diameter initialization error
Alarm Type	dialNitalizeErr
Alarm Code	1401
Severity	Critical
Aggregation Policy	An alarm is raised for every 2events within a duration of 30 minutes.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "desc" = "Diameter Stack Initialization Failure on {produce.short.name}"

Alarm	Diameter initialization error
Displayed on the web interface	[[srcProcess]] Diameter Stack Initialization Failure on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered due to stack initialization failure.
Recommended Actions	Check the network interface settings and port settings. The port could be in use by another application.

Parent topic: [System Alarms](#)

## Diameter peer transport failure

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** 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"

Alarm	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 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.

Parent topic: [System Alarms](#)

## Diameter CER error

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** 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"

Alarm	Diameter CER error
Displayed on the web interface	[[srcProcess]] Failed to decode CER from Peer [[peerName]] Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered when the diameter stack fails to decode the capabilities exchange request (CER) received from peer.
Recommended Actions	Check if the transport is up for the peer. Peer application may not be running.

Parent topic: [System Alarms](#)

## Diameter peer add error

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter peer add error alarm

Alarm	Diameter peer add error
Alarm Type	diaPeerAddError
Alarm Code	1407
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerIp" = "3.3.3.3" "peerName" = "OCS1" "peerRealmName" = "organization.com" "desc" = "Failed to add Peer" "cause"="Cause Value"

Alarm	Diameter peer add error
Displayed on the web interface	[[srcProcess]] Failed to add Peer [[peerName]], Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered when the diameter stack fails to add a peer to the peer table.
Recommended Actions	Check if the peer IP address is reachable and if the peer responds to the configured port.

Parent topic: [System Alarms](#)

## Diameter peer remove successful

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter peer remove successful alarm

Alarm	Diameter peer remove successful
Alarm Type	diaPeerRemoveSuccess
Alarm Code	1409
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerIp" = "3.3.3.3" "peerName" = "OCS1" "peerRealmName" = "organization.com" "desc" = "Peer removal success"

Alarm	Diameter peer remove successful
Displayed on the web interface	{{srcProcess}} Peer {{peerName}} Realm {{peerRealmName}} removal is successful on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the peer is removed successfully from the table. The remote peer sends a diameter disconnect peer request (DPR) with the cause of not wanting to talk.
Recommended Actions	Ensure that the peer removal is intentional. It is also removed when the peer sends a cause message.

Parent topic: [System Alarms](#)

## Diameter realm entry error

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter realm entry error alarm

Alarm	Diameter realm entry error
Alarm Type	diaRealmEntryErr
Alarm Code	1410
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerRealmName" = "organization.com" "peerName" = "OCS1" "desc" = "Failed to add route for Realm"

Alarm	Diameter realm entry error
Displayed on the web interface	[[srcProcess]] Failed to add route for Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered due to realm route entry add error. This may arise when the realm entry exists and another realm entry is added. Creating two diameter services with same realm name causes this problem.
Recommended Actions	Ensure that peer supports the application for the given realm and is up and running.

Parent topic: [System Alarms](#)

## Diameter failover to alternate peer

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter failover to alternate peer alarm

Alarm	Diameter failover to alternate peer
Alarm Type	diaFailOverToAltPeer
Alarm Code	1411
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"=ÖCS1 "peerRealmName" = "organization.com" "altPeerName" = "OCS2" "altPeerRealmName" = "india.internal.net" "desc" = "Fwd to alt peer"

Alarm	Diameter failover to alternate peer
Displayed on the web interface	[[srcProcess]] Fwd from Peer [[peerName]] to AltPeer [[altPeerName]] Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered due to retransmission to an alternate peer.
Recommended Actions	Verify that the failover has occurred to the alternate peer and the request is processed by the same peer. Also verify if the primary peer is having a problem or is not reachable.

Parent topic: [System Alarms](#)

## Diameter fail back to peer

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter fail back to peer alarm

Alarm	Diameter fail back to peer
Alarm Type	diaFailbackToPeer
Alarm Code	1412
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="<Application Name>" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"=ÖCS1 "peerRealmName" = "organization.com" "altPeerName" = "OCS2" "altPeerRealmName" = "india.internal.net" "desc" = "Failback to main peer"

Alarm	Diameter fail back to peer
Displayed on the web interface	[[srcProcess]] Failback to Main Peer [[peerName]] Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered due to retransmission to the main peer in case of a failover.
Recommended Actions	Verify that the primary peer is restored and the request is processed by the primary peer.

Parent topic: [System Alarms](#)

## Diameter CEA unknown peer

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter CEA unknown peer alarm

Alarm	Diameter CEA unknown peer
Alarm Type	diaCEAUnknownPeer
Alarm Code	1414
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="SessMgr" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"=ÖCS8 "peerRealmName" = "organization.com" "desc" = "CEA received from Unknown peer"

Alarm	Diameter CEA unknown peer
Displayed on the web interface	[[srcProcess]] CEA received from Unknown Peer [[peerName]] Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]
Description	This alarm is triggered when the capabilities exchange answer (CEA) is received from an unknown peer.
Recommended Actions	Verify that the origin host received from capabilities exchange answer (CEA) is not in the remote service configuration.

Parent topic: [System Alarms](#)

## Diameter no common application

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** Diameter no common application alarm

Alarm	Diameter no common application
Alarm Type	diaNoCommonApp
Alarm Code	1415
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.
Attribute	<pre> "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "mvnold"=12 "srcProcess"="&lt;Application Name&gt;" "realm"="ruckus.com" "originHost" = "Node1" "SCGMgmtIp"="2.2.2.2" "peerName"=ÖCS1 "peerRealmName" = "organization.com""desc" = "No common App with peer" </pre>

Alarm	Diameter no common application
Displayed on the web interface	{{srcProcess}} No common App with Peer {{peerName}} Realm {{peerRealmName}} on {produce.short.name} {{SCGMgmtIp}}
Description	This alarm is triggered when the common application is not with the peer.
Recommended Actions	Verify that the peer is in the remote service configuration and is sending the capability negotiation message that the authentication application identifier is not compliant to the remote service.

Parent topic: [System Alarms](#)

## Process initiated

 **Note:** This alarm is not applicable for vSZ-H.


**Table 1.** 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}}

Alarm	Process initiated
Description	This alarm is triggered when PMIPv6 process restarts.
Recommended Actions	A manual intervention is required. Download the PMIPv6d log file from the controller to check the cause of error.

Parent topic: [System Alarms](#)

## PMIPv6 unavailable


 **Note:** This alarm is not applicable for vSZ-H.

**Table 1.** PMIPv6 unavailable alarm

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

Parent topic: [System Alarms](#)

## Memory allocation failed

 **Note:** This alarm is not applicable for vSZ-H.

**Table 1.** Memory allocation failed alarm

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

Parent topic: [System Alarms](#)

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

**Table 1.** 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 triggered when the last data plane disconnects from the zone affinity.

Parent topic: [System Alarms](#)

## scheduleZoneFirmwareUpgrade

**Table 1.** scheduleZoneFirmwareUpgrade Alarms

Alarm	scheduleZoneFirmwareUpgrade
Alarm Type	scheduleZoneFirmwareUpgrade
Alarm Code	195
Severity	Major

Alarm	scheduleZoneFirmwareUpgrade
Attributes	“failedNumber”=“number” “notAvailableNumber”=“number” “name”=“XXX”
Displayed on the web interface	[{failedNumber}] zone(s) upgrade failed and [{notAvailableNumber}] zone(s) not available in schedule upgrade task [{name}]
Description	This alarm triggers when the [{failedNumber}] zone(s) upgrade failed and [{notAvailableNumber}] zone(s) not available in schedule upgrade task [{name}]

Parent topic: [System Alarms](#)

## Switch

Following are the alarms related to switch severity:

- [Power supply failure](#)
- [Fan failure](#)
- [Module insertion](#)
- [Module removal](#)
- [Temperature above threshold warning](#)
- [Stack member unit failure](#)
- [PoE power allocation failure](#)
- [DHCP\\_Snooping](#)
- [Port put into error disable state](#)
- [Switch offline](#)
- [Switch duplicated](#)
- [Reject certificate signing request](#)
- [Pending certificate signing request](#)

- Switch CPU major threshold exceed
- Switch CPU critical threshold exceed
- Switch memory major threshold exceed
- Switch memory critical threshold exceed
- Switch customer major threshold exceed
- Switch customer critical threshold exceed
- Switch Firmware Upgrade Failed
- Switch Configuration Update Failed

Parent topic: [Alarm Types](#)

## Power supply failure

**Table 1.** Power supply failure alarm

Alarm	Power supply failure
Alarm Type	PowerSupplyfailure
Alarm Code	20000
Severity	Critical
Aggregation Policy	From the event code 20000, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	[[switchSerialNumber] / {switchName}] {switchMsg} EX: System: Stack unit 3 Power supply 2 is not present
Description	This alarm is triggered when there is power supply failure.

Alarm	Power supply failure
Recommended Actions	Check the status of Switch power supply.

Parent topic: [Switch](#)

## Fan failure

**Table 1.** Fan failure alarm

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

Parent topic: [Switch](#)

## Module insertion

**Table 1.** Module insertion alarm

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

Parent topic: [Switch](#)

## Module removal

**Table 1.** Module removal alarm

Alarm	Module removal
Alarm Type	ModuleRemoval
Alarm Code	20003
Severity	Critical

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

Parent topic: [Switch](#)

## Temperature above threshold warning

**Table 1.** Temperature above threshold warning alarm

Alarm	Temperature above threshold warning
Alarm Type	TemperatureAboveThresholdWarning
Alarm Code	20004
Severity	Critical
Aggregation Policy	From the event code 20004, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x",switchName = "x", "switchMsg"="x"
Displayed on the web interface	[[switchSerialNumber] / {switchName}] {switchMsg} EX: Temperature is over warning level.

Alarm	Temperature above threshold warning
Description	This alarm is triggered when the temperature is above the warning level.
Recommended Actions	Check the status of Switch unit.

Parent topic: [Switch](#)

## Stack member unit failure

**Table 1.** Stack member unit failure alarm

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

Parent topic: [Switch](#)

## PoE power allocation failure

**Table 1.** PoE power allocation failure alarm

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

Parent topic: [Switch](#)

## DHCP\_Snooping: DHCP offer dropped message

**Table 1.** DHCP\_Snooping: DHCP offer dropped message alarm

Alarm	DHCP_Snooping: DHCP offer dropped message
Alarm Type	DhcpOfferDroppedMessage
Alarm Code	20007
Severity	Critical

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

Parent topic: [Switch](#)

## Port put into error disable state

**Table 1.** Port put into error disable state alarm

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

Alarm	Port put into error disable state
Description	This alarm is triggered when the port is in error-disable state.
Recommended Actions	Check port status.

Parent topic: [Switch](#)

## Switch offline

**Table 1.** Switch offline alarm

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

Parent topic: [Switch](#)

## Switch duplicated

**Table 1.** Switch duplicated alarm

Alarm	Switch duplicated
Alarm Type	SwitchDuplicated

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

Parent topic: [Switch](#)

## Reject certificate signing request

**Table 1.** Reject certificate signing request alarm

Alarm	Reject certificate signing request
Alarm Type	rejectCertificateSigningRequest
Alarm Code	22003
Severity	Major
Aggregation Policy	From the event code 22003, an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x"

Alarm	Reject certificate signing request
Displayed on the web interface	[SCEP - {switchSerialNumber}] Reject Certificate Signing Request.
Description	This alarm is triggered when there is a SCEP Reject certificate signing request.
Recommended Actions	Check if the switches are under the trust list.

Parent topic: [Switch](#)

## Pending certificate signing request

**Table 1.** Pending certificate signing request alarm

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

Parent topic: [Switch](#)

## Switch CPU major threshold exceed

**Table 1.** Switch CPU major threshold exceed alarm

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

Parent topic: [Switch](#)

## Switch CPU critical threshold exceed

**Table 1.** Switch CPU critical threshold exceed alarm

Alarm	Switch CPU critical threshold exceed
Alarm Type	criticalCpuThresholdExceed
Alarm Code	22012
Severity	Critical

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

Parent topic: [Switch](#)

## Switch memory major threshold exceed

**Table 1.** Switch memory major threshold exceed alarm

Alarm	Switch memory major threshold exceed
Alarm Type	majorMemoryThresholdExceed
Alarm Code	22021
Severity	Major
Aggregation Policy	From the event code 22021 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"

Alarm	Switch memory major threshold exceed
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This alarm is triggered when the memory capacity exceeds the major threshold limit, which is based on the utilization rate.

Parent topic: [Switch](#)

## Switch memory critical threshold exceed

**Table 1.** Switch memory critical threshold exceed alarm

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

Parent topic: [Switch](#)

## Switch custom major threshold exceed

**Table 1.** Switch custom major threshold exceed alarm

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

Parent topic: [Switch](#)

## Switch custom critical threshold exceed

**Table 1.** Switch custom critical threshold exceed alarm

Alarm	Switch custom critical threshold exceed
Alarm Type	hitCriticalSwitchCombinedEvent
Alarm Code	22032
Severity	Critical
Aggregation Policy	From the event code 22032 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	UserDefinedDescription = "x"

Alarm	Switch custom critical threshold exceed
Displayed on the web interface	[Custom Critical Event] {userDefinedDescription}
Description	This alarm is triggered when the switch custom crosses the critical threshold limit.

Parent topic: [Switch](#)

## Switch Firmware Upgrade Failed

**Table 1.** Switch Firmware Upgrade Failed alarm

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

Parent topic: [Switch](#)

## Switch Configuration Update Failed

**Table 1.** Switch Configuration Update Failed alarm

Alarm	Switch Configuration Update Failed
Alarm Type	SwitchConfigurationUpdateFailed
Alarm Code	22052

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

Parent topic: [Switch](#)

## Threshold Alarms

Following are the alarms related to threshold system set:

- [CPU threshold exceeded](#)
- [Memory threshold exceeded](#)
- [Disk usage threshold exceeded](#)
- [The drop of client count threshold exceeded](#)
- [License threshold exceeded](#)
- [Rate limit for TOR surpassed](#)
- [The number of users exceeded its limit](#)
- [The number of devices exceeded its limit](#)
- [Over AP maximum capacity](#)
- [Over Device maximum capacity](#)

Parent topic: [Alarm Types](#)

# CPU threshold exceeded

**Table 1.** CPU threshold exceeded alarm

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

Parent topic: [Threshold Alarms](#)

# Memory threshold exceeded

**Table 1.** Memory threshold exceeded alarm

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

Parent topic: [Threshold Alarms](#)

# Disk usage threshold exceeded

**Table 1.** 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.

Parent topic: [Threshold Alarms](#)

## The drop of client count threshold exceeded

**Table 1.** The drop of client count threshold exceeded alarm

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

Parent topic: [Threshold Alarms](#)

## License threshold exceeded


**Table 1.** 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.

Alarm	License threshold exceeded
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.

Parent topic: [Threshold Alarms](#)

## HDD Health Degradation

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

**Table 1.** HDD Health Degradation Alarm

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

Alarm	HDD health degradation
Description	This alarm is triggered when the hard drive detects a health degradation on the control plane.

Parent topic: [Threshold Alarms](#)

## Rate limit for TOR surpassed

**Table 1.** 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	"mvnold"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd",  "UserName"=abc@xyz.com, "realm"="wlan.3gppnetwork"  "SCGMgmtIp"="2.2.2.2", "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct", "ueMacAddr"="aa:bb:cc:gg:hh:ii"  "MOR"=1000, "THRESHOLD"="500", "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.

Alarm	Rate limit for TOR surpassed
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.

Parent topic: [Threshold Alarms](#)

## The number of users exceeded its limit

**Table 1.** 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.

Parent topic: [Threshold Alarms](#)

## The number of devices exceeded its limit

**Table 1.** 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.

Parent topic: [Threshold Alarms](#)

## Over AP maximum capacity

**Table 1.** Over AP maximum capacity alarm

Alarm	Over AP maximum capacity
Alarm Type	apCapacityReached
Alarm Code	962
Severity	Warning
Aggregation Policy	From the event code 962, an alarm is raised for every event. A single event triggers a single alarm.

Alarm	Over AP maximum capacity
Displayed on the web interface	The volume of AP is over system capacity.
Description	This alarm is triggered when the volume of AP is over system capacity.

Parent topic: [Threshold Alarms](#)

## Over Device maximum capacity

**Table 1.** Over Device maximum capacity alarm

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

Parent topic: [Threshold Alarms](#)

## Tunnel Alarms - Access Point

Following are the alarms related to tunnel.

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

Parent topic: [Alarm Types](#)

## AP softGRE gateway not reachable

**Table 1.** 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	This alarm is triggered when the AP fails to connect to the Soft-GRE gateway.
Recommended Actions	Check the primary and secondary soft-GRE gateway.

Parent topic: [Tunnel Alarms - Access Point](#)

## AP is disconnected from secure gateway

**Table 1.** AP is disconnected from secure gateway alarm

Alarm	AP is disconnected from secure gateway
Alarm Type	ipsecTunnelDisassociated

Alarm	AP is disconnected from secure gateway
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.

Parent topic: [Tunnel Alarms - Access Point](#)

## AP secure gateway association failure

**Table 1.** 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

Alarm	AP secure gateway association failure
Attribute	apMac="xx:xx:xx:xx:xx:xx","ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is unable to establish secure gateway with [{ipsecGWAddress}
Description	This alarm is triggered when the AP is unable to connect to the secure gateway.
Recommended Actions	No action required.

**Parent topic:** [Tunnel Alarms - Access Point](#)

# Events Types

---

3rd Party Access Point Events

Accounting Events

AP Authentication Events

AP Communication Events

AP LBS Events

AP Mesh Events

AP State Change Events

AP USB Events

Authentication Events

Authorization Events

Control and Data Plane Interface

Client Events

Cloud Events

Cluster Events

Configuration Events

Datablade Events

Data Plane Events

Data Streaming Event

DHCP Events

GA Interface Events

Gn/S2a Interface Events

Gr Interface Event

IPMI Events

[Licensing Interface Events](#)

[Location Delivery Events](#)

[PMIPv6 Events](#)

[Session Events](#)

[STA Interface Events](#)

[System Events](#)

[Switch Events](#)

[Threshold Events](#)

[Tunnel Events - Access Point \(AP\)](#)


[Tunnel Events - Data Plane](#)

[AP Ethernet Phy Error Count](#)

[AP Ethernet PHY Down Shift](#)

[AP BAND Change](#)

# 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](#)

Parent topic: [Events Types](#)

## 3rd party AP connected


Table 1. 3rdparty AP connected event

Event	3rd party AP connected
Event Type	3rdPartyAPConnected
Event Code	1801

Event	3rd party AP connected
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.

Parent topic: [3rd Party Access Point Events](#)

## Accounting Events

 **Note:** This event is not applicable for vSZ-H.


Following events are related to accounting.

- [Accounting session disabled](#)
- [Accounting server not reachable](#)
- [Accounting failed over to secondary](#)
- [Accounting fallback to primary](#)
- [AP accounting message mandatory parameter missing](#)
- [Unknown realm](#)
- [AP accounting message decode failed](#)
- [AP accounting retransmission message dropped](#)
- [AP accounting response while invalid config](#)

- AP account message drop while no accounting start message
- Unauthorized COA/DM message dropped

Parent topic: [Events Types](#)

## Accounting session disabled


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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}]
Description	This event occurs when the accounting is disabled for the session.

Parent topic: [Accounting Events](#)

## Accounting server not reachable


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Accounting Events](#)

## Accounting failed over to secondary

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** Accounting failed over to secondary event

Event	Accounting failed over to secondary
Event Type	accFailedOverToSecondary
Event Code	1653
Severity	Major

Event	Accounting failed over to secondary
Attribute	<pre> "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" </pre>
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.

Parent topic: [Accounting Events](#)

## Accounting fallback to primary

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** Accounting fallback to primary event

Event	Accounting fallback to primary
Event Type	accFallbackToPrimary
Event Code	1654
Severity	Major
Attribute	<pre> "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" </pre>

Event	Accounting fallback to primary
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.

Parent topic: [Accounting Events](#)

## AP accounting message mandatory parameter missing

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** AP accounting message mandatory parameter missing event

Event	AP accounting message mandatory parameter missing
Event Type	apAcctMsgMandatoryPrmMissing
Event Code	1901
Severity	Critical
Attribute	"mvnold"="12","wlanId"="1","zoneld"="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}]

Event	AP accounting message mandatory parameter missing
	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.

Parent topic: [Accounting Events](#)

## Unknown realm

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** Unknown realm event

Event	Unknown realm
Event Type	unknownRealmAccounting
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}]

Event	Unknown realm
Description	This event occurs when the controller fails to find realm configuration for the accounting messages received from the AP.

Parent topic: [Accounting Events](#)

## AP accounting message decode failed


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Accounting Events](#)

## AP accounting retransmission message dropped

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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", "ueImei"="12345", "ueMsisdn"="98787" "apIpAddress"="10.1.4.11"
Displayed on the web interface	[{srcProcess}] Accounting message from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}] dropped, {produce.short.name} did not receive Accounting start message.
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.

Parent topic: [Accounting Events](#)

## AP accounting response while invalid config

**Table 1.** AP accounting response while invalid config event

Event	AP accounting response while invalid config
Event Type	apAcctRespWhileInvalidConfig
Event Code	1909
Severity	Debug

Event	AP accounting response while invalid config
Attribute	<pre>mvnold="12 "wlanId"=1,"zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut" "realm"="wlan.3gppnetwork.org", "userName"="abc@xyz.com",  "SCGMgmtIp"="2.2.2.2","apIpAddress"="10.1.4.11"</pre>
Displayed on the web interface	<pre>{{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</pre>
Description	<p>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.</p>

Parent topic: [Accounting Events](#)

## AP account message drop while no accounting start message

**Table 1.** 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	<pre>mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org", "userName"="abc@xyz.com", "SCGMgmtIp"="2.2.2.2", "apIpAddress"="10.1.4.11"</pre>

Event	AP account message drop while no accounting start message
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).

Parent topic: [Accounting Events](#)

## Unauthorized COA/DM message dropped

**Table 1.** 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

Event	Unauthorized COA/DM message dropped
Description	This event occurs when the controller receives a change of authorization (CoA) or dynamic multipoint (DM) messages from an unauthorized AAA server.

Parent topic: [Accounting Events](#)

## AP Authentication Events

Following are the events related to authentication.

- [Radius server reachable](#)
- [Radius server unreachable](#)
- [LDAP server reachable](#)
- [LDAP server unreachable](#)
- [AD server reachable](#)
- [AD server unreachable](#)
- [Wechat ESP authentication server reachable](#)
- [WeChat ESP authentication server unreachable](#)
- [WeChat ESP authentication server resolvable](#)
- [WeChat ESP authentication server unresolvable](#)
- [WeChat ESP DNAT server reachable](#)
- [WeChat ESP DNAT server unreachable](#)
- [WeChat ESP DNAT server resolvable](#)
- [WeChat ESP DNAT server unresolvable](#)
- [Authentication attempt](#)
- [Authentication unsuccessful](#)

- [Authentication re-attempt](#)
- [Authentication 8021](#)
- [AP local session timeout](#)
- [AP Remote session timeout](#)
- [AP Interactive session termination](#)

Parent topic: [Events Types](#)

## Radius server reachable

**Table 1.** 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.

Parent topic: [AP Authentication Events](#)

## Radius server unreachable

**Table 1.** 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

Parent topic: [AP Authentication Events](#)

## LDAP server reachable

**Table 1.** LDAP server reachable event

Event	LDAP server reachable
Event Type	ldapServerReachable
Event Code	2121
Severity	Informational

Event	LDAP server reachable
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.

Parent topic: [AP Authentication Events](#)

## LDAP server unreachable

**Table 1.** 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.

Event	LDAP server unreachable
Auto Clearance	This event triggers the alarm 2122, which is auto cleared by the event code 2121.

Parent topic: [AP Authentication Events](#)

## AD server reachable

**Table 1.** 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.

Parent topic: [AP Authentication Events](#)

## AD server unreachable

**Table 1.** AD server unreachable event

Event	AD server unreachable
Event Type	adServerUnreachable

Event	AD server unreachable
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.

Parent topic: [AP Authentication Events](#)

## Wechat ESP authentication server reachable

**Table 1.** 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"=""

Event	Wechat ESP authentication server reachable
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.

Parent topic: [AP Authentication Events](#)

## WeChat ESP authentication server unreachable

**Table 1.** 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

Parent topic: [AP Authentication Events](#)

## WeChat ESP authentication server resolvable

**Table 1.** 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.

Parent topic: [AP Authentication Events](#)

## WeChat ESP authentication server unresolvable

**Table 1.** 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"

Event	WeChat ESP authentication server unresolvable
	","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.

Parent topic: [AP Authentication Events](#)

## WeChat ESP DNAT server reachable

**Table 1.** 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.

Parent topic: [AP Authentication Events](#)

## WeChat ESP DNAT server unreachable

**Table 1.** 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

Parent topic: [AP Authentication Events](#)

## WeChat ESP DNAT server resolvable

**Table 1.** WeChat ESP DNAT server resolvable event

Event	WeChat ESP DNAT server resolvable
Event Type	espDNATServerResolvable
Event Code	2163
Severity	Informational

Event	WeChat ESP DNAT server resolvable
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.

Parent topic: [AP Authentication Events](#)

## WeChat ESP DNAT server unresolvable

**Table 1.** 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.

Event	WeChat ESP DNAT server unresolvable
Auto Clearance	This event triggers the alarm 2164, which is auto cleared by the event code 2163

Parent topic: [AP Authentication Events](#)

## Authentication Attempts

**Table 1.** Authentication attempt event

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

Parent topic: [AP Authentication Events](#)

## Authentication Unsuccessful

**Table 1.** Authentication unsuccessful event

Event	Authentication Unsuccessful
Event Type	authUnsucces
Event Code	99006

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

Parent topic: [AP Authentication Events](#)

## Authentication Re-attempt

**Table 1.** Authentication re-attempt event

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

Parent topic: [AP Authentication Events](#)

## Authentication 8021

**Table 1.** Authentication 8021 client event

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

Parent topic: [AP Authentication Events](#)

## AP Local Session Timeout

**Table 1.** AP local session timeout event

Event	AP Local Session Timeout
Event Type	apLocalSessionTimeout
Event Code	99015
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Local AP [{apMac}] session terminates due to session timeout.

Event	AP Local Session Timeout
Description	This event occurs when local AP session terminates due to session timeout.

Parent topic: [AP Authentication Events](#)

## AP Remote Session Timeout

**Table 1.** AP Remote session timeout event

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

Parent topic: [AP Authentication Events](#)

## AP Interactive Session Termination

**Table 1.** AP Interactive Session Termination event

Event	AP Interactive Session Termination
Event Type	apInteractiveSessionTerm
Event Code	99017

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

Parent topic: [AP Authentication Events](#)

## 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](#)
- [AP managed](#)
- [AP rejected](#)
- [AP firmware updated](#)
- [AP firmware update failed](#)
- [Updating AP firmware](#)
- [Updating AP configuration](#)
- [AP configuration updated](#)
- [AP configuration update failed](#)
- [AP pre-provision model mismatched](#)
- [AP swap model mismatched](#)
- [AP WLAN oversubscribed](#)

- AP join zone failed
- AP illegal to change country code
- AP configuration get failed
- Rogue AP
- Rogue AP disappeared
- Classified Rogue AP
- AP image signing failed
- Jamming attack
- Rogue client
- Key gen fail
- Key dis fail
- Key dis fail GTK
- wpaendec fail
- IPsec ses fail
- Fw manual initiation
- AP Management TSF data
- AP TSF failure
- AP Self tests
- Firmware initiation update
- SSH initiation
- SSH termination
- SSH failure
- TLS initiation

- [TLS termination](#)
- [TLS failure](#)
- [IP sec initiation](#)
- [IP sec termination](#)
- [IP sec failure](#)

Parent topic: [Events Types](#)

## AP discovery succeeded

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP managed

**Table 1.** AP managed event

Event	AP managed
Event Type	apStatusManaged

Event	AP managed
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.

Parent topic: [AP Communication Events](#)

## AP rejected

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP firmware updated

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP firmware update failed

**Table 1.** 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"

Event	AP firmware update failed
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.

Parent topic: [AP Communication Events](#)

## Updating AP firmware

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## Updating AP configuration

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP configuration updated

**Table 1.** 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}]

Event	AP configuration updated
Description	This event occurs when the AP successfully updates the existing configuration details to the controller.

Parent topic: [AP Communication Events](#)

## AP configuration update failed

**Table 1.** AP configuration update failed event

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

Parent topic: [AP Communication Events](#)

## AP pre-provision model mismatched

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP swap model mismatched

**Table 1.** 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"

Event	AP swap model mismatched
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.

Parent topic: [AP Communication Events](#)

## AP WLAN oversubscribed

**Table 1.** AP WLAN oversubscribed event

Event	AP WLAN oversubscribed
Event Type	apWlanOversubscribed
Event Code	114
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName}&{apMac}] does not have enough capacity to deploy all 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.

Parent topic: [AP Communication Events](#)

## AP join zone failed

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP illegal to change country code

**Table 1.** 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"

Event	AP illegal to change country code
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.

Parent topic: [AP Communication Events](#)

## AP configuration get failed

**Table 1.** AP configuration get failed event

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

Parent topic: [AP Communication Events](#)

## Rogue AP

**Table 1.** Rogue AP event

Event	Rogue AP
Event Type	genericRogueAPDetected
Event Code	180

Event	Rogue AP
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxxx", "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.

Parent topic: [AP Communication Events](#)

## Rogue AP disappeared

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## Classified Rogue AP

**Table 1.** 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.

Parent topic: [AP Communication Events](#)

## AP image signing failed

**Table 1.** AP image signing failed event

Event	AP image signing failed
Event Type	apSigningInformation
Event Code	187
Severity	Informational

Event	AP image signing failed
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.

Parent topic: [AP Communication Events](#)

## Jamming attack

**Table 1.** Jamming attack event


Event	Jamming attack
Event Type	jammingDetected
Event Code	189
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	A jamming rogue AP[{{rogueMac}}] with SSID[{{ssid}}] is detected by [{{apName&&apMac}}] on channel[{{channel}}].
Description	This event occurs when an AP detects a radio jamming attack.

Parent topic: [AP Communication Events](#)

## Rogue client

**Table 1.** Rogue client

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

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

**Parent topic:** [AP Communication Events](#)

## Key gen fail

**Table 1.** Key gen fail event

Event	Key gen fail
Event Type	KeyGenFail
Event Code	99000
Severity	Critical

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

Parent topic: [AP Communication Events](#)

## Key dis fail

**Table 1.** Key dis fail event

Event	Key gen fail
Event Type	KeyDisFail
Event Code	99001
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	4-way handshake is failure, AP [{apMac}].
Description	This event occurs when 4-way handshake is failure.

Parent topic: [AP Communication Events](#)

## Key dis fail GTK

**Table 1.** Key dis fail GTK event

Event	Key dis fail
Event Type	KeyDisFailGTK

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

Parent topic: [AP Communication Events](#)

## wpaendec fail

**Table 1.** WpaEnDec fail event

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

Parent topic: [AP Communication Events](#)

## IPsecSes fail

**Table 1.** IPsecSes fail event

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

Parent topic: [AP Communication Events](#)

## Fw manual initiation

**Table 1.** Fw manual initiation event

Event	Fw manual initiation
Event Type	FwManualInitiation
Event Code	99009
Severity	Informational
Attribute	<p>"apIP"="e.f.g.h", "dpIP"="a.b.c.d" "tunnelType"=RGRE/SGRE</p> <p>"apMac"="xx:xx:xx:xx:xx:xx", " Manual FW update initiated"</p>

Event	Fw manual initiation
	<p>"apMac"="xx:xx:xx:xx:xx:xx", " Manual FW:'fwname' update, not needed. it is same!"</p> <p>"apMac"="xx:xx:xx:xx:xx:xx", " Manual FW:'fwname' update, not needed."</p> <p>"apMac"="xx:xx:xx:xx:xx:xx", "Manual FW:%s update successful"</p> <p>"apMac"="xx:xx:xx:xx:xx:xx", " Manual FW update failed with failcode:3"</p>
Displayed on the web interface	AP [{apMac}] attempt to initiate a manual update, reason: [{reason}].
Description	This event occurs whenever there is manual firmware update.

Parent topic: [AP Communication Events](#)

## AP Management TSF data

**Table 1.** AP Management TSF data event

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

Parent topic: [AP Communication Events](#)

## AP TSF failure

**Table 1.** AP TSF failure event

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

Parent topic: [AP Communication Events](#)

## AP Self tests

**Table 1.** AP Self tests event

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

Event	AP Self tests
Description	This event occurs whenever all self tests are passed for fips_sku builds

Parent topic: [AP Communication Events](#)

## Firmware initiation update

**Table 1.** Firmware initiation update event

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

Parent topic: [AP Communication Events](#)

## SSH initiation

**Table 1.** SSH initiation event

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

Parent topic: [AP Communication Events](#)

## SSH termination

**Table 1.** SSH termination event

Event	SSH termination
Event Type	sshTermination
Event Code	99019
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "SSH session exited"
Displayed on the web interface	There is exit from established SSH session, AP: {{apMac}}.

Event	SSH termination
Description	This event occurs whenever there is exit from established SSH session

Parent topic: [AP Communication Events](#)

## SSH failure

**Table 1.** SSH failure event

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

Parent topic: [AP Communication Events](#)

## TLS initiation

**Table 1.** TLS initiation event

Event	TLS initiation
Event Type	tlsInitiation
Event Code	99021

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

Parent topic: [AP Communication Events](#)

## TLS termination

**Table 1.** TLS termination event

Event	TLS termination
Event Type	tlsTermination
Event Code	99022
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "HTTPS Logout successful"
Displayed on the web interface	There is logout from AP [{apMac}] web-GUI session.
Description	This event occurs whenever there is logout from AP web-GUI session or AP gracefully terminates a trusted TLS connection.

Parent topic: [AP Communication Events](#)

## TLS failure

**Table 1.** TLS failure event

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

Parent topic: [AP Communication Events](#)

## IP sec initiation

**Table 1.** IP sec initiation event

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

Event	IP sec initiation
Description	This event occurs whenever there is ipsec session initiation.

Parent topic: [AP Communication Events](#)

## IP sec termination

**Table 1.** IP sec termination event

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

Parent topic: [AP Communication Events](#)

## IP sec failure

**Table 1.** IP sec failure event

Event	IP sec failure
Event Type	IPsecFailure
Event Code	99026

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

Parent topic: [AP Communication Events](#)

## AP LBS Events

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

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

Parent topic: [Events Types](#)

## No LS responses

**Table 1.** 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.

Parent topic: [AP LBS Events](#)

## LS authentication failure

**Table 1.** 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}]

Event	LS authentication failure
Description	This event occurs due to the authentication failure on connecting to the location based service.

Parent topic: [AP LBS Events](#)

## AP connected to LS

**Table 1.** AP connected to LS event

Event	AP connected to LS
Event Type	apLBSCConnectSuccess
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.

Parent topic: [AP LBS Events](#)

## AP failed to connect to LS

**Table 1.** AP failed to connect to LS event

Event	AP failed to connect to LS
Event Type	apLBSCConnectFailed
Event Code	704

Event	AP failed to connect to LS
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.

Parent topic: [AP LBS Events](#)

## AP started location service

**Table 1.** 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.

Parent topic: [AP LBS Events](#)

## AP stopped location service

**Table 1.** AP stopped location service event

Event	AP stopped location service
Event Type	apLBSSStopLocationService
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.

Parent topic: [AP LBS Events](#)

## AP received passive calibration request

**Table 1.** AP received passive calibration request event

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

Event	AP received passive calibration request
Description	This event occurs when the AP receives the passive calibration request.

Parent topic: [AP LBS Events](#)

## AP received passive footfall request

**Table 1.** 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.

Parent topic: [AP LBS Events](#)

## AP received unrecognized request

**Table 1.** AP received unrecognized request event

Event	AP received unrecognized request
Event Type	apLBSRcvdUnrecognizedRequest

Event	AP received unrecognized request
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.

Parent topic: [AP LBS Events](#)

## AP Mesh Events

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

- [EMAP downlink connected to MAP](#)
- [EMAP downlink disconnected from MAP](#)
- [EMAP uplink connected to MAP](#)
- [EMAP uplink disconnected from MAP](#)
- [MAP disconnected](#)
- [MAP downlink connected](#)
- [MAP downlink connected to EMAP](#)
- [MAP downlink disconnected from EMAP](#)
- [RAP downlink connected to MAP](#)
- [MAP uplink connected to EMAP](#)
- [MAP uplink disconnected from EMAP](#)

- [MAP uplink connected to RAP](#)
- [MAP uplink connected to MAP](#)
- [Mesh state updated to MAP](#)
- [Mesh state updated to MAP no channel](#)
- [Mesh state updated to RAP](#)
- [Mesh state update to RAP no channel](#)
- [MAP downlink connected to MAP](#)
- [MAP downlink disconnected from MAP](#)
- [RAP downlink disconnected from MAP](#)

Parent topic: [Events Types](#)

## EMAP downlink connected to MAP

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## EMAP downlink disconnected from MAP

**Table 1.** 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

Parent topic: [AP Mesh Events](#)

## EMAP uplink connected to MAP

**Table 1.** 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}]

Event	EMAP uplink connected to MAP
Description	This event occurs when Ethernet Mesh AP uplink connection to MAP is successful.

Parent topic: [AP Mesh Events](#)

## EMAP uplink disconnected from MAP

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## MAP disconnected

**Table 1.** MAP disconnected event

Event	MAP disconnected
Event Type	mapDisconnected
Event Code	411

Event	MAP disconnected
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.

Parent topic: [AP Mesh Events](#)

## MAP downlink connected

**Table 1.** MAP downlink connected event

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

Parent topic: [AP Mesh Events](#)

## MAP downlink connected to EMAP

**Table 1.** MAP downlink connected to EMAP event

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

Parent topic: [AP Mesh Events](#)

## MAP downlink disconnected from EMAP

**Table 1.** MAP downlink disconnected from EMAP event

Event	MAP downlink disconnected from EMAP
Event Type	mapDlinkDisconnectWitheMap
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}]

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

Parent topic: [AP Mesh Events](#)

## RAP downlink connected to MAP

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## MAP uplink connected to EMAP

**Table 1.** MAP uplink connected to EMAP event

Event	MAP uplink connected to EMAP
Event Type	mapUlinkConnectToEMap
Event Code	417

Event	MAP uplink connected to EMAP
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).

Parent topic: [AP Mesh Events](#)

## MAP uplink disconnected from EMAP

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## MAP uplink connected to RAP

**Table 1.** 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).

Parent topic: [AP Mesh Events](#)

## MAP uplink connected to MAP

**Table 1.** 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"

Event	MAP uplink connected to MAP
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).

Parent topic: [AP Mesh Events](#)

## Mesh state updated to MAP

**Table 1.** 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).

Parent topic: [AP Mesh Events](#)

## Mesh state updated to MAP no channel

**Table 1.** 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).

Parent topic: [AP Mesh Events](#)

## Mesh state updated to RAP

**Table 1.** 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"

Event	Mesh state updated to RAP
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).

Parent topic: [AP Mesh Events](#)

## Mesh state update to RAP no channel

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## MAP downlink connected to MAP

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## MAP downlink disconnected from MAP

**Table 1.** MAP downlink disconnected from MAP event

Event	MAP downlink disconnected from MAP
Event Type	mapDlinkDisconnectWithMap
Event Code	426
Severity	Informational
Attribute	"secondMapMac"=" xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{secondMapName&&secondMapMac}] disconnected from MAP [{apName&&apMac}]

Event	MAP downlink disconnected from MAP
Description	This event occurs when the MAP disconnects from a second MAP.

Parent topic: [AP Mesh Events](#)

## RAP downlink disconnected from MAP

**Table 1.** 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.

Parent topic: [AP Mesh Events](#)

## AP State Change Events

Following are the events related to access point state changes:

Event	Event	Event
<a href="#">AP rebooted by user</a>	<a href="#">AP rebooted by system</a>	<a href="#">AP disconnected</a>

Event	Event	Event
AP IP address updated	AP reset to factory default	AP channel updated
AP country code updated	AP channel updated because dynamic frequency selection (DFS) detected a radar	AP change control plane
AP connected	AP deleted	AP heartbeat lost
AP tagged as critical	AP cable modem interface down	AP brownout
AP cable modem power-cycled by user	AP smart monitor turn off WLAN	AP client load balancing limit reached
AP client load balancing limit recovered	AP WLAN state changed	AP capacity reached
AP capacity recovered	AP cable modem interface up	AP cable modem soft-rebooted by user
AP cable modem set to factory default by user	AP health high latency flag	AP health low capacity flag
AP health high connection failure flag	AP health high client count flag	AP health high latency clear
AP health low capacity clear	AP health high connection failure clear	AP health high client count clear
Primary DHCP AP is down	Primary DHCP AP is up	Secondary DHCP AP is down
Secondary DHCP AP is up	Primary or secondary DHCP AP detects 90% of the configured total IPs	Both primary and secondary DHCP server APs are down
AP NAT gateway IP failover detected for particular VLAN pool	AP NAT gateway IP fall back detected for particular VLAN pool	NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive

Event	Event	Event
		NAT gateway AP IPs are down for 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	AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down	AP health high airtime utilization flag
AP health high airtime utilization clear	AP cluster failover	AP cluster rehome
AP switchover cluster failed	AP MAC OUI violation	Backhaul switched to primary
Backhaul switched to secondary	LTE network connectivity lost	Ethernet network connectivity lost
LTE DHCP timeout	Ethernet link down	Ethernet link up
SIM switch	Remote host blacklisted	SIM removal
LTE network reg status	LTE connection status	LTE good rssi status
LTE weak rssi status	AP client load bal limit reached	AP client load bal limit recovered
AP System Anomaly		

Parent topic: [Events Types](#)

## AP rebooted by user

**Table 1.** AP rebooted by user event

Event	AP rebooted by user
Event Type	apRebootByUser
Event Code	301

Event	AP rebooted by user
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.

Parent topic: [AP State Change Events](#)

## AP rebooted by system

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP disconnected

**Table 1.** AP disconnected event

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

Parent topic: [AP State Change Events](#)

## AP IP address updated

**Table 1.** 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

Event	AP IP address updated
Description	This event occurs when the AP is reset due to a change in the IP address.

Parent topic: [AP State Change Events](#)

## AP reset to factory default

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP channel updated

**Table 1.** AP channel updated event

Event	AP channel updated
Event Type	apChannelChanged
Event Code	306

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

Parent topic: [AP State Change Events](#)

## AP country code updated

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

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

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP change control plane

**Table 1.** AP change control plane event

Event	AP change control plane
Event Type	apChangeControlBlade
Event Code	311
Severity	Informational

Event	AP change control plane
Attribute	<pre>"apMac"="xx:xx:xx:xx:xx:xx", "oldwsgIP"="xxx.xxx.xxx.xxx", "newwsgIP"="xxx.xxx.xxx.xxx"</pre>
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.

Parent topic: [AP State Change Events](#)

## AP connected

**Table 1.** AP connected event

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

Parent topic: [AP State Change Events](#)

## AP deleted

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP heartbeat lost

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP tagged as critical

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP cable modem interface down

**Table 1.** 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.

Event	AP cable modem interface down
Auto Clearance	This event triggers the alarm 308, which is auto cleared by the event code 325.

Parent topic: [AP State Change Events](#)

## AP brownout

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP cable modem power-cycled by user

**Table 1.** AP cable modem power-cycled by user event

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

Event	AP cable modem power-cycled by user
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.

Parent topic: [AP State Change Events](#)

## AP smart monitor turn off WLAN

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP client load balancing limit reached

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP client load balancing limit recovered

**Table 1.** AP client load balancing limit recovered event

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

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.

Parent topic: [AP State Change Events](#)

## AP WLAN state changed

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP capacity reached

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP capacity recovered

**Table 1.** AP capacity recovered event

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

Event	AP capacity recovered
Description	This event occurs when the AP starts accepting clients again because the current client association is below the threshold limit.

Parent topic: [AP State Change Events](#)

## AP cable modem interface up

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP cable modem soft-rebooted by user

**Table 1.** AP cable modem soft-rebooted by user event

Event	AP cable modem soft-rebooted by user
Event Type	cmResetByUser
Event Code	326

Event	AP cable modem soft-rebooted by user
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.

Parent topic: [AP State Change Events](#)

## AP cable modem set to factory default by user

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health high latency flag

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health low capacity flag

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health high connection failure flag

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health high client count flag

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health high latency clear

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health low capacity clear

**Table 1.** 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}}.

Event	AP health low capacity clear
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.

Parent topic: [AP State Change Events](#)

## AP health high connection failure clear

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health high client count clear

**Table 1.** 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",

Event	AP health high client count clear
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.

Parent topic: [AP State Change Events](#)

## Primary DHCP AP is down

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## Primary DHCP AP is up

**Table 1.** 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"

Event	Primary DHCP AP is up detected by secondary DHCP AP. Stopping DHCP service on secondary.
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.

Parent topic: [AP State Change Events](#)

## Secondary DHCP AP is down

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## Secondary DHCP AP is up

**Table 1.** 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"

Event	Secondary DHCP AP is up detected by primary DHCP AP.
Displayed on the web interface	Secondary DHCP server [{{secondaryServerMac}}] is up detected by primary DHCP server [{{primaryServerMac}}].
Description	This event occurs when the primary DHCP AP detects that secondary DHCP AP is UP.

Parent topic: [AP State Change Events](#)

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

**Table 1.** 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	apDHCIPPoolMaxThresholdReached
Event Code	340
Severity	Warning
Attribute	"zoneName"="ZoneName", "poolId"="xxxx", "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.

Parent topic: [AP State Change Events](#)

## Both primary and secondary DHCP server APs are down

**Table 1.** 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

Event	Both primary and secondary DHCP server APs are down
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.

Parent topic: [AP State Change Events](#)

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

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

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

**Table 1.** 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	AP NAT gateway IP fall back detected for particular VLAN pool
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.

Parent topic: [AP State Change Events](#)

## 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 1.** 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

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
	three (3) consecutive NAT gateway AP IP failure for a particular VLAN pool.

Parent topic: [AP State Change Events](#)

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

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

Parent topic: [AP State Change Events](#)

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

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP health high airtime utilization flag

**Table 1.** 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}].

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

Parent topic: [AP State Change Events](#)

## AP health high airtime utilization clear

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP cluster failover

**Table 1.** AP cluster failover event

Event	AP cluster failover
Event Type	apClusterFailover
Event Code	349
Severity	Informational

Event	AP cluster failover
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.

Parent topic: [AP State Change Events](#)


## AP cluster rehome

**Table 1.** 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.

Parent topic: [AP State Change Events](#)

## AP switchover cluster failed

 **Note:** This alarm is supported on the SmartZone 300 controllers only. This alarm is not applicable for vSZ-H.

**Table 1.** AP switchover cluster failed event

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

Parent topic: [AP State Change Events](#)

## AP MAC OUI violation

**Table 1.** AP MAC OUI violation

Event	AP MAC OUI violation
Event Type	AP MAC OUI violation
Event Code	1294
Severity	Major
Attribute	AP Name, AP MAC

Event	AP MAC OUI violation
Displayed on the web interface	APName @ AP MAC
Description	This event occurs when an approved AP is rejected due to violation of AP MAC OUI (Organization Unique ID) rule.

Parent topic: [AP State Change Events](#)

## Backhaul switched to primary

**Table 1.** Backhaul switched to primary event

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

Parent topic: [AP State Change Events](#)

## Backhaul switched to secondary

**Table 1.** Backhaul switched to secondary event

Event	Backhaul switched to secondary
Event Type	changeToSecondaryBackhaul

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

Parent topic: [AP State Change Events](#)

## LTE network connectivity lost

**Table 1.** LTE network connectivity lost event

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

Parent topic: [AP State Change Events](#)

## Ethernet network connectivity lost

**Table 1.** Ethernet network connectivity lost vent

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

Parent topic: [AP State Change Events](#)

## LTE DHCP timeout

**Table 1.** LTE DHCP timeout event

Event	LTE DHCP timeout
Event Type	lteDhcpTimeout
Event Code	9104
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 1"
Displayed on the web interface	AP [{apName&&apMac}] LTE DHCP timeout on [{currSim}]
Description	This event occurs when LTE DHCP timeout.

Parent topic: [AP State Change Events](#)

## Ethernet link down

**Table 1.** Ethernet link down event

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

Parent topic: [AP State Change Events](#)

## Ethernet link up

**Table 1.** Ethernet link up event

Event	Ethernet link up
Event Type	ethernetLinkUp
Event Code	9106
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currlface = "eth0"
Displayed on the web interface	AP [{apName&&apMac}] Ethernet link up on [{currlface}]

Event	Ethernet link up
Description	This event occurs when Ethernet link is up.

Parent topic: [AP State Change Events](#)

## SIM switch

**Table 1.** SIM switch event

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

Parent topic: [AP State Change Events](#)

## Remote host blacklisted

**Table 1.** Remote host blacklisted event

Event	Remote host blacklisted
Event Type	remoteHostBlacklisted
Event Code	9108
Severity	Informational

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

Parent topic: [AP State Change Events](#)

## SIM removal

**Table 1.** SIM removal event

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

Parent topic: [AP State Change Events](#)

## LTE network registration status

**Table 1.** LTE network registration status event

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

Parent topic: [AP State Change Events](#)

## LTE connection status


**Table 1.** LTE connection status event

Event	LTE connection status
Event Type	IteConnectionStatus
Event Code	9111
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currConnStatus = "3G"
Displayed on the web interface	AP [{apName&&apMac}] [{currSim}] Cellular connection status - [{currConnStatus}]

Event	LTE connection status
Description	This event occurs whenever there is a change in the LTE connection status.

Parent topic: [AP State Change Events](#)

## LTE good rssi status


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** LTE good rssi status event

Event	LTE good rssi status
Event Type	lteGoodRssiStatus
Event Code	9112
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currRssiStatus = "good"
Displayed on the web interface	AP [{apName&&apMac}] [{currSim}] Cellular signal strength is [{currRssiStatus}] now
Description	This event occurs whenever there is a change in the RSSI from weak to good.

Parent topic: [AP State Change Events](#)

## LTE weak rssi status


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** LTE weak rssi status event

Event	LTE weak rssi status
Event Type	lteWeakRssiStatus
Event Code	9113
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currSim = "SIM 0", currRssiStatus = "weak"
Displayed on the web interface	AP [{apName&&apMac}] [{currSim}] Cellular signal strength is [{currRssiStatus}] now
Description	This event occurs whenever there is a change in the RSSI from good to weak.

Parent topic: [AP State Change Events](#)

## AP client load balancing limit reached

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** AP client load balancing limit reached event

Event	AP client load balancing limit reached
Event Type	apCLBCapacityLimitReached
Event Code	9114
Severity	Informational
Attribute	"apMac" = "xx:xx:xx:xx:xx:xx", "nbrAvlCapAvg" = "1000", "localAvlCap" = "1100", "wifiInterface"="2.4G WLANs"

Event	AP client load balancing limit reached
Displayed on the web interface	AP [RuckusAP@EC:8C:A2:26:06:F0] reached the capacity limit, localAvlCap=1000, nbrAvlCapAvg=900 on WLAN [2.4G WLANs]
Description	This event is raised by AP when the capacity of the AP is less than the average of the neighbor AP's capacity.

Parent topic: [AP State Change Events](#)

## AP client load balancing limit recovered

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** AP client load balancing limit recovered event

Event	AP client load balancing limit recovered
Event Type	apCLBCapacityLimitRecovered
Event Code	9115
Severity	Informational
Attribute	apMac = "xx:xx:xx:xx:xx:xx", "nbrAvlCapAvg" = "1100" , "localAvlCap" = "1000", "wifiInterface"="2.4G WLANs"
Displayed on the web interface	AP [RuckusAP@EC:8C:A2:26:06:F0] recovered the capacity limit, localAvlCap=800, nbrAvlCapAvg=1000 on WLAN [2.4G WLANs].
Description	This event is raised by AP when the capacity of the AP is more than the average of the neighbor AP's capacity.

Parent topic: [AP State Change Events](#)

## AP System Anomaly

**Table 1.** AP System Anomaly event

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

Parent topic: [AP State Change Events](#)

## AP Temp AF Threshold Exceeded

**Table 1.** AP Temp AF Threshold Exceeded

Event	AP Temp AF Threshold Exceeded
Event Type	apTmpfsThresholdExceeded
Event Code	99101
Severity	Informational
Attribute	\ "reason\"=\"tmp/ use%: %f%% threshold value is %f%%
Displayed on the web interface	
Description	This event occurs when the /tmp file system's usage percentage crosses the threshold value of 85%.

Parent topic: [AP State Change Events](#)

## AP Writable File Threshold Exceeded

**Table 1.** AP Writable File Threshold Exceeded

Event	AP Writable File Threshold Exceeded
Event Type	apWritablefsThresholdExceeded
Event Code	99102
Severity	Informational
Attribute	\ "reason\"=\ "writable/ use%%: %f%% threshold value is %f%%
Displayed on the web interface	
Description	This event occurs when the /writable file system's usage percentage crosses the threshold value of 85%.

Parent topic: [AP State Change Events](#)

## AP Operate in BT

**Table 1.** AP PoE Mode Change

Event	AP PoE Mode Change
Event Type	apOperateinBT5-35w
Event Code	1350
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "switchVendor"="xxxxx"

Event	AP PoE Mode Change
Displayed on the web interface	AP [{apName}&&apMac]} operating in bt5 35w with switch vendor[{switchVendor]}].
Description	This event triggers when R760 operates in BT5-35W.

Parent topic: [AP State Change Events](#)

## AP MDU Port Status Down

Table 1. APMduPortSetDown

Event	MDU Port Set down
Event Type	APMduPortStatusDown
Event Code	1030
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "ethPort" = "xxx"
Displayed on the web interface	For AP [{apName}&&apMac]} [{ethPort}] set down due to non-assignment of VNI.
Description	This event occurs when SmartZone set Mdu port down due to non-assignment of VNI.

Parent topic: [AP State Change Events](#)

## AP USB Events

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

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

Parent topic: [Events Types](#)

## AP USB software package downloaded

**Table 1.** 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.

Parent topic: [AP USB Events](#)

## AP USB software package download failed

**Table 1.** 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}]

Event	AP USB software package download failed
Description	This event occurs when the AP fails to download its USB software package.

Parent topic: [AP USB Events](#)

# Authentication Events

The following are the events related to authentication.

- [Authentication server not reachable](#)
- [Unknown realm](#)
- [Authentication succeeded](#)
- [Authentication failed](#)
- [Pseudonym authentication succeeded](#)
- [Pseudonym authentication failed](#)
- [Fast re-authentication succeeded](#)
- [Fast re-authentication failed](#)
- [Authentication failed over to secondary](#)
- [Authentication fallback to primary](#)
- [AD/LDAP connected successfully](#)
- [AD/LDAP connectivity failure](#)
- [Bind fails with AD/LDAP](#)
- [Bind success with LDAP, but unable to find clear text password for the user](#)
- [RADIUS fails to connect to AD NPS server](#)
- [RADIUS fails to authenticate with AD NPS server](#)

- Successfully established the TLS tunnel with AD/LDAP
- Fails to establish TLS tunnel with AD/LDAP

Parent topic: [Events Types](#)


## Authentication server not reachable

**Table 1.** 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.

Parent topic: [Authentication Events](#)

## Unknown realm

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Authentication Events](#)

## Authentication succeeded

**Table 1.** Authentication succeeded event

Event	Authentication succeeded
Event Type	authSuccess
Event Code	1604
Severity	Debug
Attribute	"mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "authType"="EAP-SIM/AKA"

Event	Authentication succeeded
Displayed on the web interface	Authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	<p>This event occurs when the RADIUS accept is sent back to the AP. This event applies only for TTG/PDG session.</p> <p>Note: The attribute Permanent ID is used for authentication.</p>

Parent topic: [Authentication Events](#)

## Authentication failed


**Table 1.** Authentication failed event

Event	Authentication failed
Event Type	authFailed
Event Code	1605
Severity	Debug
Attribute	<pre>"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"="&lt;Cause of failure&gt;" "authType"="EAP-SIM/ AKA"</pre>
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).

Event	Authentication failed
	Note: The attribute Permanent ID is used for authentication.

Parent topic: [Authentication Events](#)

## Pseudonym authentication succeeded


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Pseudonym authentication succeeded event

Event	Pseudonym authentication succeeded
Event Type	pseudonymAuthSuccess
Event Code	1606
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" "ueImei"="12345","ueMsisdn"="98787" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Pseudonym ID based authentication successful for UE with IMSI [{ueImei}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS accept is sent back to the AP. This event is applicable when the controller acts as a host AAA server and is applicable only for TTG/PDG session.  <b>Note:</b> The attribute <b>Pseudonym ID</b> is used for authentication.

Parent topic: [Authentication Events](#)

## Pseudonym authentication failed


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Pseudonym authentication failed event

Event	Pseudonym authentication failed
Event Type	pseudonymAuthFailed
Event Code	1607
Severity	Debug
Attribute	<pre>"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" "ueImei"="12345","ueMsisdn"="98787" "cause"="&lt;Cause of failure&gt;" "authType"="EAP-SIM/ AKA"</pre>
Displayed on the web interface	<p>Pseudonym ID based authentication failed for UE with IMSI [{ueImei}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]</p>
Description	<p>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).</p> <p><b>Note:</b> The attribute <b>Pseudonym ID</b> is used for authentication.</p>

Parent topic: [Authentication Events](#)

## Fast re-authentication succeeded


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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"
Displayed on the web interface	Fast re-auth ID based authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs after resending RADIUS accept back to AP. This event is applicable when, the {produce.short.name} acts as a hosted AAA server and for TTG/PDG session.  <b>Note:</b> FastReauth ID is used for authentication.

Parent topic: [Authentication Events](#)

## Fast re-authentication failed

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Fast re-authentication failed event

Event	Fast re-authentication failed
Event Type	fastReauthFailed
Event Code	1609
Severity	Debug
Attribute	<pre>"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"="&lt;Cause of failure&gt;" "authType"="EAP-SIM/AKA"</pre>
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	<p>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).</p> <p><b>Note:</b> Attribute <b>FastReuathID</b> is used for reauthentication.</p>

Parent topic: [Authentication Events](#)

## Authentication failed over to secondary

**Table 1.** Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651

Event	Authentication failed over to secondary
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.

Parent topic: [Authentication Events](#)

## Authentication fallback to primary

**Table 1.** 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

Event	Authentication fallback to primary
	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.

Parent topic: [Authentication Events](#)

## AD/LDAP connected successfully

**Table 1.** 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", "authSrvrIp"= "1.1.1.1"  "SCGMgmtIp"="2.2.2.2", "desc"="Successful connection to AD/LDAP"
Displayed on the web interface	[{srcProcess}] Connect to AD/LDAP[{authSrvrIp}] successfully from SCG[{SCGMgmtIp}]
Description	This event occurs when RADIUS connection to AD/LDAP server is successful.

Parent topic: [Authentication Events](#)

## AD/LDAP connectivity failure

**Table 1.** 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", "authSrvrIp"="1.1.1.1", "SCGMgmtIp"="2.2.2.2"  "desc"= "Connection to AD/LDAP fails"
Displayed on the web interface	[[srcProcess]] Connect to AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]]
Description	This event occurs when RADIUS fails to connect to AD/LDAP server.

Parent topic: [Authentication Events](#)

## Bind fails with AD/LDAP

**Table 1.** 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"

Event	Bind fails with AD/LDAP
	"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.

Parent topic: [Authentication Events](#)

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

**Table 1.** 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]]

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

Parent topic: [Authentication Events](#)

## RADIUS fails to connect to AD NPS server

**Table 1.** 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.

Parent topic: [Authentication Events](#)

## RADIUS fails to authenticate with AD NPS server

**Table 1.** 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.

Parent topic: [Authentication Events](#)

## Successfully established the TLS tunnel with AD/LDAP

**Table 1.** 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"

Event	Successfully established the TLS tunnel with AD/LDAP
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.

Parent topic: [Authentication Events](#)

## Fails to establish TLS tunnel with AD/LDAP

**Table 1.** Fails to establish TLS tunnel with AD/LDAP event

Event	Fails to establish TLS tunnel with AD/LDAP
Event Type	racADLDAPTLSFailed
Event Code	1762
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12 "srcProcess"="radiusd", "authSrvrIp"="1.1.1.1" "authSrvrPort"="636", "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish TLS Tunnel with LDAP/AD"
Displayed on the web interface	[[srcProcess]] Establishes the TLS connection with AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]]
Description	This event occurs when the TLS connection between the controller and AD/LDAP fails.
Auto Clearance	This event triggers the alarm 1762, which is auto cleared by the event code 1761.

Parent topic: [Authentication Events](#)

## TLS Establishment Failed between SZ and external AAA Server

**Table 1.** TLS Establishment Failed between SZ and external AAA Server event

Event	TLS Establishment Failed between SZ and external AAA Server
Event Type	racTLSEstablishmentFailedBetweenSZandExternalAAA Server

Event	TLS Establishment Failed between SZ and external AAA Server
Event Code	1763
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish "
Displayed on the web interface	[[srcProcess]] Establishes the TLS connection fails between SZ and external AAA Server from SCG[[SCGMgmtIp]]
Description	This event is triggered when TLS connection between the controller and AD/LDAP fails.

Parent topic: [Authentication Events](#)

## RAC DNS Resolve Failed

**Table 1.** racDNSResolveFailed

Event	Radius Fails to resolve the FQDN of AAA
Event Type	racDNSResolveFailed
Event Code	1771
Severity	Major
Attribute	racDNSResolveFailed"desc"="DNS resolution failed for FQDN"
Displayed on the web interface	DNS Resolution Failed for FQDN[[FQDNName]] from [[SCGMgmtIp]]

Event	Radius Fails to resolve the FQDN of AAA
Description	This event occurs when RADIUS fails to resolve the FQDN.

Parent topic: [Authentication Events](#)

## Authorization Events

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

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

Parent topic: [Events Types](#)

## DM received from AAA

**Table 1.** DM received from AAA event

Event	DM received from AAA
Event Type	dmRcvdAAA
Event Code	1641

Event	DM received from AAA
Severity	Debug
Attribute	"mvnold"="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.

Parent topic: [Authorization Events](#)

## DM NACK sent to AAA

**Table 1.** DM NACK sent to AAA event

Event	DM NACK sent to AAA
Event Type	dmNackSntAAA
Event Code	1642
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "rmtRadSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected not acknowledged message to the AAA server.

Parent topic: [Authorization Events](#)

## DM sent to NAS

**Table 1.** DM sent to NAS event

Event	DM sent to NAS
Event Type	dmSntNAS
Event Code	1643
Severity	Debug
Attribute	"mvnold"="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].

Parent topic: [Authorization Events](#)

## DM NACK received from NAS

**Table 1.** DM NACK received from NAS event

Event	DM NACK received from NAS
Event Type	dmNackRcvdNAS
Event Code	1644
Severity	Debug

Event	DM NACK received from NAS
Attribute	"mvnold"="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.

Parent topic: [Authorization Events](#)

## CoA received from AAA

**Table 1.** CoA received from AAA event

Event	CoA received from AAA
Event Type	coaRcvdAAA
Event Code	1645
Severity	Debug
Attribute	"mvnold"="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.

Parent topic: [Authorization Events](#)

## CoA NACK sent to AAA

**Table 1.** CoA NACK sent to AAA event

Event	CoA NACK sent to AAA
Event Type	coaNackSntAAA
Event Code	1646
Severity	Debug
Attribute	"mvnold"="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.

Parent topic: [Authorization Events](#)

## CoA sent NAS

**Table 1.** CoA sent NAS event

Event	CoA sent NAS
Event Type	coaSentNas
Event Code	1647
Severity	Debug
Attribute	"mvnold"="12" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "userName"="abc@xyz.com"

Event	CoA sent NAS
	"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.

Parent topic: [Authorization Events](#)

## CoA NAK received NAS

**Table 1.** CoA NAK received NAS event

Event	CoA NAK received NAS
Event Type	coaNakRcvdNas
Event Code	1648
Severity	Debug
Attribute	"mvnold"="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.

Parent topic: [Authorization Events](#)

## CoA authorize only access reject

**Table 1.** CoA authorize only access reject event

Event	CoA authorize only access reject
Event Type	coaAuthorizeOnlyAccessReject
Event Code	1649
Severity	Critical
Attribute	"mvnold"="12" "wlanId"="1", "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImei"="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.

Parent topic: [Authorization Events](#)

## CoA RWSG MWSG notification failure

**Table 1.** CoA RWSG MWSG notification failure event

Event	CoA RWSG MWSG notification failure
Event Type	coaRWSGMWSGNotifFailure
Event Code	1650
Severity	Major

Event	CoA RWSG MWSG notification failure
Attribute	mvnold="12" wlanId="1" "zoneId"="10" ctrlBladeMac="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "userName"=abc@xyz.com "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "apType" = " "ueMacAddr"="aa:bb:cc:gg:hh:ii"
Displayed on the web interface	Session Modify MWSG-RWSG Notification Failure/No response received
Description	This event occurs when the change of authorization in RADIUS /metro wireless service gateway notification fails.

Parent topic: [Authorization Events](#)

## 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](#)
- [GtpManager \(DP\) disconnected](#)
- [Session updated at DP](#)
- [Session update at DP failed](#)
- [Session deleted at DP](#)
- [Session delete at DP failed](#)
- [C2d configuration failed](#)

Parent topic: [Events Types](#)

## DP connected

**Table 1.** 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.

Parent topic: [Control and Data Plane Interface](#)

## GtpManager (DP) disconnected

**Table 1.** 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",

Event	GtpManager (DP) disconnected
	"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.

Parent topic: [Control and Data Plane Interface](#)

## Session updated at DP

**Table 1.** Session updated at DP event

Event	Session updated at DP
Event Type	sessUpdatedAtDblade
Event Code	1205
Severity	Debug
Attribute	"mvnold"="12", "wlanId"="1", "zoneId"="10", "srcProcess"="aut", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "realm"="realm sent by UE", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"

Event	Session updated at DP
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been updated at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session updates the request (C-D-SESS-UPD-REQ) successfully.

Parent topic: [Control and Data Plane Interface](#)

## Session update at DP failed

**Table 1.** Session update at DP failed event

Event	Session update at DP failed
Event Type	sessUpdateErrAtDblade
Event Code	1206
Severity	Debug
Attribute	"mvnold"="12", "wlanId"="1", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff",  "srcProcess"="aut", "zoneId"="10", "realm"="realm sent by UE",  "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii",  "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to update at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]

Event	Session update at DP failed
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.

Parent topic: [Control and Data Plane Interface](#)

## Session deleted at DP

**Table 1.** Session deleted at DP event

Event	Session deleted at DP
Event Type	sessDeletedAtDblade
Event Code	1207
Severity	Debug
Attribute	"mvnold"="12", "wlanId"="1" "zoneld"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="realm sent by UE", "ctrlBladeIp"="1.1.1.1", "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsisdn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been deleted from Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session deletes request (C-D-SESS-DEL-REQ) is successfully acknowledged.

Parent topic: [Control and Data Plane Interface](#)

## Session delete at DP failed

**Table 1.** 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.

Parent topic: [Control and Data Plane Interface](#)

## C2d configuration failed

**Table 1.** C2d configuration failed event

Event	C2d configuration failed
Event Type	c2dCfgFailed
Event Code	1209
Severity	Warning

Event	C2d configuration failed
Attribute	<pre> “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”=“&lt;what was configured&gt;” </pre>
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.

Parent topic: [Control and Data Plane Interface](#)

## 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](#)
- [Client joined](#)
- [Client failed to join](#)
- [Client disconnected](#)
- [Client connection timed out](#)
- [Client authorization successfully](#)
- [Client authorization failed](#)
- [Client session expired](#)
- [Client roaming](#)
- [Client logged out](#)

- 3rd party client join
- 3rd party client inactivity timeout
- 3rd party client authorization
- 3rd party client authorization failure
- 3rd party client session expiration
- 3rd party client roaming
- 3rd party client session logout
- Client roaming disconnected
- Client blocked
- Client grace period
- Onboarding registration succeeded
- Onboarding registration failed
- Remediation succeeded
- Remediation failed
- Force DHCP disconnected
- WDS device joined
- WDS device left
- Client is blocked because of barring UE rule
- Client is unblocked by barring UE rule
- Start CALEA mirroring client
- Stop CALEA mirroring client
- Wired client joined
- Wired client failed to join

- [Wired client disconnected](#)
- [Wired client authorization successfully](#)
- [Wired client session expired](#)
- [Application identified](#)
- [Application denied](#)
- [URL filtering server unreachable](#)
- [URL filtering server reachable](#)
- [Packet spoofing detected](#)
- [Packet spoofing detected](#)
- [Packet spoofing detected](#)
- [Packet spoofing detected](#)

Parent topic: [Events Types](#)

## Client authentication failed

**Table 1.** 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.

Event	Client authentication failed
Description	This event occurs when the client fails to join WLAN on the AP due to an authentication failure.

Parent topic: [Client Events](#)

## Client joined

**Table 1.** 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.

Parent topic: [Client Events](#)

## Client failed to join

**Table 1.** Client failed to join event

Event	Client failed to join
Event Type	clientJoinFailure
Event Code	203
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx",  "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx"  "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join WLAN [{ssid}] from AP [{apName}&&apMac]}.
Description	This event occurs when the client fails to connect to the WLAN on the AP.

Parent topic: [Client Events](#)

## Client disconnected

**Table 1.** 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",

Event	Client disconnected
	<pre> "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" </pre>
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.

Parent topic: [Client Events](#)

## Client connection timed out

**Table 1.** Client connection timed out event

Event	Client connection timed out
Event Type	clientInactivityTimeout
Event Code	205
Severity	Informational
Attribute	<pre> "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx",  "ssid"="xxxxx", "assoicationTime"="600", "wlanId"="xxxxx", </pre>

Event	Client connection timed out
	<pre>"userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="",  "apLocation"="", "username"="", "osType"="", "radio"="",  "vlanId"=, "sessionDuration"=, "txBytes"=, "rxBytes"=, "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="",, "userId"="uuid"</pre>
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.

Parent topic: [Client Events](#)

## Client authorization successfully

**Table 1.** Client authorization successfully event

Event	Client authorization successfully
Event Type	clientAuthorization
Event Code	206
Severity	Informational
Attribute	<pre>""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"</pre>

Event	Client authorization successfully
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.

Parent topic: [Client Events](#)

## Client authorization failed

**Table 1.** 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.

Parent topic: [Client Events](#)

## Client session expired

**Table 1.** Client session expired event

Event	Client session expired
Event Type	clientSessionExpiration
Event Code	208
Severity	Informational
Attribute	<pre>"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"</pre>
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.

Parent topic: [Client Events](#)

## Client roaming

**Table 1.** Client roaming event

Event	Client roaming
Event Type	clientRoaming
Event Code	209
Severity	Informational

Event	Client roaming
Attribute	<pre>"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"</pre>
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.

Parent topic: [Client Events](#)

## Client logged out


**Table 1.** Client logged out event

Event	Client logged out
Event Type	clientSessionLogout
Event Code	210
Severity	Informational
Attribute	<pre>"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"</pre>
Displayed on the web interface	Client [{userName}   IP   clientMac] session logout.

Event	Client logged out
Description	This event occurs when a client session is logged out.

Parent topic: [Client Events](#)

## 3rd party client join


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 3rd party client join event

Event	3rd party client join
Event Type	3rdPtyClientJoin
Event Code	211
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx",  "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd party client [{clientIP}   {clientMac}] joined Zone [{zoneName}] on DP [{dpName}&&dpKey}].
Description	This event occurs when a 3rd party client joins the AP zone session on the data plane.

Parent topic: [Client Events](#)

## 3rd party client inactivity timeout


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Client Events](#)

## 3rd party client authorization

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** 3rd party client authorization event

Event	3rd party client authorization
Event Type	3rdPtyClientAuthorization
Event Code	213
Severity	Informational

Event	3rd party client authorization
Attribute	<pre>"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx",  "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"</pre>
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.

Parent topic: [Client Events](#)

## 3rd party client authorization failure

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** 3rd party client authorization failure event

Event	3rd party client authorization failure
Event Type	3rdPtyClientAuthorizationFailure
Event Code	214
Severity	Informational
Attribute	<pre>"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx",  "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"</pre>
Displayed on the web interface	3rd party client [{clientIP}   clientMac] of Zone [{zoneName}] on DP [{dpName}&&dpKey}] was not authorized.

Event	3rd party client authorization failure
Description	This event occurs when the 3rd party client on the AP zone session is not authorized.

Parent topic: [Client Events](#)

## 3rd party client session expiration


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Client Events](#)

## 3rd party client roaming


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Client Events](#)

## 3rd party client session logout

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 3rd party client session logout event

Event	3rd party client session logout
Event Type	3rdPtyClientSessionLogout

Event	3rd party client session logout
Event Code	217
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx",  "clientIP"="x.x.x.x", "zoneUUID"="xxxxxx", "userId"="uuid"
Displayed on the web interface	3rd party client [{clientIP}   {clientMac}] of Zone [{zoneName}] on DP [{dpName}   {dpKey}] occurred session logout.
Description	This event occurs when 3rd party client on AP zone data plane occurs. This results in a session logs out.

Parent topic: [Client Events](#)

## Client roaming disconnected

**Table 1.** Client roaming disconnected event

Event	Client roaming disconnected
Event Type	smartRoamDisconnect
Event Code	218
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "assoicationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="",

Event	Client roaming disconnected
	<pre>"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"</pre>
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 WLAN due to a smart roam policy.

Parent topic: [Client Events](#)

## Client blocked

**Table 1.** Client blocked event

Event	Client blocked
Event Type	clientBlockByDeviceType
Event Code	219
Severity	Informational
Attribute	<pre>"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "deviceType"="xxxxx", "ssid"="xxxxx", "wlanId"="xxxxx",</pre>
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.

Parent topic: [Client Events](#)

## Client grace period

**Table 1.** 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.

Parent topic: [Client Events](#)

## Onboarding registration succeeded

**Table 1.** 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",

Event	Onboarding registration succeeded
	"apLocation"="xxxx", "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.

Parent topic: [Client Events](#)

## Onboarding registration failed

**Table 1.** Onboarding registration failed event

Event	Onboarding registration failed
Event Type	onboardingRegistrationFailure
Event Code	222
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid", "apLocation"="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.

Parent topic: [Client Events](#)

## Remediation succeeded

**Table 1.** 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.

Parent topic: [Client Events](#)

## Remediation failed

**Table 1.** Remediation failed event

Event	Remediation failed
Event Type	remediationFailure
Event Code	224
Severity	Informational

Event	Remediation failed
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.

Parent topic: [Client Events](#)

## Force DHCP disconnected

**Table 1.** Force DHCP disconnected event

Event	Force DHCP disconnected
Event Type	forceDHCPDisconnect
Event Code	225
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "bssid"="", "wlanId"="xxxxx", "tenantUUID"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "vlanId"="", "radio"="", "encryption"=""
Displayed on the web interface	Client [{userName}   {IP}   {clientMac}] disconnected from WLAN [{ssid}] on AP [{apName}&{apMac}] due to force-dhcp.
Description	This event occurs when the client disconnects by force from the dynamic host configuration protocol.

Parent topic: [Client Events](#)

## WDS device joined

**Table 1.** WDS device joined event

Event	WDS device joined
Event Type	wdsDeviceJoin
Event Code	226
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "wdsDeviceMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Device [{wdsDeviceMac}] sends traffic via Client [{clientMac}] in AP [{apName}&&apMac}].
Description	This event occurs when a subscriber device joins the network provided by a Customer-Premises Equipment (CPE) of a client associated AP through a wireless distribution system (WDS) mode.

Parent topic: [Client Events](#)

## WDS device left

**Table 1.** WDS device left event

Event	WDS device left
Event Type	wdsDeviceLeave
Event Code	227
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "wdsDeviceMac"="xx:xx:xx:xx:xx:xx"

Event	WDS device left
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.

Parent topic: [Client Events](#)

## Client is blocked because of barring UE rule

**Table 1.** Client is blocked because of barring UE rule event

Event	Client is blocked because of barring UE rule
Event Type	clientBlockByBarringUERule
Event Code	228
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Client [clientMac] of WLAN [{ssid}] from AP [{apName}&&apMac} was blocked because of barring UE rule.
Description	This event occurs when a client is temporarily blocked by the UE barring rule. Barring UE rule is to block a user after multiple authentication failures.

Parent topic: [Client Events](#)

## Client is unblocked by barring UE rule

**Table 1.** Client is unblocked by barring UE rule event

Event	Client is unblocked by barring UE rule
Event Type	clientUnblockByBarringUERule
Event Code	229
Severity	Informational

Event	Client is unblocked by barring UE rule
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.

Parent topic: [Client Events](#)

## Start CALEA mirroring client

**Table 1.** 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.

Parent topic: [Client Events](#)

## Stop CALEA mirroring client

**Table 1.** 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",

Event	Stop CALEA mirroring client
	"apMac"="xx:xx:xx:xx:xx:xx", "authType"="xxxxx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	Stop CALEA mirroring client [{userName}   IP     clientMac}] on WLAN [{ssid}] with authentication type [{authType}] from AP [{apName&&apMac}]. TxBytes[{txBytes}], RxBytes[{rxBytes}].
Description	This event occurs when CALEA stops mirroring the client image.

Parent topic: [Client Events](#)

## Client information updated

**Table 1.** Client information updated event

Event	Client Info Update
Event Type	clientInfoUpdate
Event Code	236
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP     clientMac}] info update on WLAN [{ssid}] from AP [{apName&&apMac}].
Description	This event occurs when a client obtains IP address.

Parent topic: [Client Events](#)

## Wired client joined

**Table 1.** Wired client joined event

Event	Wired client joined
Event Type	wiredClientJoin
Event Code	2802

Event	Wired client joined
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.

Parent topic: [Client Events](#)

## Wired client failed to join

**Table 1.** 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.

Parent topic: [Client Events](#)

## Wired client disconnected

**Table 1.** 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"
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.

Parent topic: [Client Events](#)

## Wired client authorization successfully

**Table 1.** 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",

Event	Wired client authorization successfully
	"iface"="xxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxx", "vlanId"="x", "userName"="xxx"
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.

Parent topic: [Client Events](#)

## Wired client session expired

**Table 1.** 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"="xxxx", "ethPort"="x", "iface"="xxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxx", "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.

Event	Wired client session expired
Description	This event occurs when a client exceeds the session time limit, which results in a session termination.

Parent topic: [Client Events](#)

## Application identified

**Table 1.** Application identified event

Event	Application identified
Event Type	application of user is identified
Event Code	8001
Severity	Informational
Attribute	
Displayed on the web interface	APP[{{APP}}] identified from AP[{{apMac}}] for client [{{STA_MAC}}] with source[{{SRC_IP}}:{{SRC_PORT}}] destination[{{DST_IP}}:{{DST_PORT}}] Proto[{{PROTO}}]
Description	This event occurs when the user of the application is identified.

Parent topic: [Client Events](#)

## Application denied

**Table 1.** 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}}]

Event	Application denied
Description	This event occurs when the application of the user is denied.

Parent topic: [Client Events](#)

## URL filtering server unreachable

**Table 1.** 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.

Parent topic: [Client Events](#)

## URL filtering server reachable

**Table 1.** 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.

Parent topic: [Client Events](#)

## Packet spoofing detected

**Table 1.** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWireless
Event Code	232
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "ssid"="xxxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}] from client [{clientMac}&&clientIP}] on WLAN [{ssid}] [{networkInterface}] from AP [{apName}&&apMac}]
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature.

Parent topic: [Client Events](#)

## Packet spoofing detected

**Table 1.** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWirelessSourceMacSpoofed
Event Code	233
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "ssid"="xxxxx", "networkInterface"

Event	Packet spoofing detected
	= "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}], packets [{packetDropCount}] were dropped on WLAN [{ssid}] [{networkInterface}] from AP [{apName}&&apMac}]
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature. It is a source MAC address spoof.

Parent topic: [Client Events](#)

## Packet spoofing detected

**Table 1.** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWired
Event Code	234
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}] from client [{clientMac}&&clientIP}] on [{networkInterface}] from AP [{apName}&&apMac}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature.

Parent topic: [Client Events](#)

# Packet spoofing detected

**Table 1.** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWiredSourceMacSpoofed
Event Code	235
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}], packets [{packetDropCount}] were dropped on [{networkInterface}] from AP [{apName}&&apMac}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature. It is a source MAC address spoof.

Parent topic: [Client Events](#)

## Cloud Events

The following are the events related to Cloud Based Service.

- [Cloud services enabled](#)
- [Cloud services disabled](#)
- [Cloud analytics enabled](#)
- [Cloud analytics disabled](#)
- [Cloud services token refreshed](#)
- [Cloud services token renewed](#)

Parent topic: [Events Types](#)

## Cloud Services Enabled

**Table 1.** Cloud services enabled event

Event	Cloud services enabled
Event Type	CloudServicesEnabled
Event Code	4501
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services have been enabled successfully.
Description	This event occurs when the controller successfully enables the Cloud Services.

Parent topic: [Cloud Events](#)

## Cloud Services Disabled

**Table 1.** Cloud services disabled event

Event	Cloud services disabled
Event Type	CloudServicesdisabled
Event Code	4502
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services have been disabled successfully.

Event	Cloud services disabled
Description	This event occurs when controller successfully disables the Cloud Services.

Parent topic: [Cloud Events](#)

## Cloud Analytics Enabled

**Table 1.** Cloud analytics enabled event

Event	Cloud analytics enabled
Event Type	CloudAnalyticsEnabled
Event Code	4503
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics service has been enabled successfully.
Description	This event occurs when the controller successfully enables Cloud Analytics service.

Parent topic: [Cloud Events](#)

## Cloud Analytics Disabled

**Table 1.** Cloud analytics disabled event

Event	Cloud analytics disabled
Event Type	CloudAnalyticsDisabled
Event Code	4504
Severity	Informational

Event	Cloud analytics disabled
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This event occurs when the controller successfully disables Cloud Analytics service.

Parent topic: [Cloud Events](#)

## Cloud Services Token Refreshed

**Table 1.** Cloud services token refreshed event

Event	Cloud services token refreshed
Event Type	CloudServicesTokenRefreshed
Event Code	4601
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services token has been refreshed successfully.
Description	This event occurs when the controller successfully refreshes the Cloud Services access token.

Parent topic: [Cloud Events](#)

## Cloud Analytics Token Renewed

**Table 1.** Cloud analytics token renewed event

Event	Cloud analytics token renewed
Event Type	cloudAnalyticsTokenRenewed

Event	Cloud analytics token renewed
Event Code	4602
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics token has been renewed successfully.
Description	This event occurs when the controller successfully renews Cloud Analytics access token.

Parent topic: [Cloud Events](#)

## Cloud Analytics Service has been Enabled

**Table 1.** Cloud Analytics Service has been Enabled event

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

Parent topic: [Cloud Events](#)

## Cloud Analytics service has been disabled

**Table 1.** Cloud Analytics service has been disabled event

Event	Cloud Analytics service has been disabled
Event Type	cloudAnalyticsDisabled
Event Code	4504
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This event occurs when SZ successfully disabled Cloud Analytics service.

Parent topic: [Cloud Events](#)

## Cloud Analytics Disconnected

**Table 1.** Cloud Analytics Disconnected event

Event	Cloud Analytics Disconnected
Event Type	cloudAnalyticsDisconnected
Event Code	4505
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service cannot be connected.
Description	This event occurs when Smart Zone can't send heartbeat to Cloud Analytics service.

Parent topic: [Cloud Events](#)

## cloudAPRegistrarSyncEnabled

**Table 1.** cloudAPRegistrarSyncEnabled event

Event	cloudAPRegistrarSyncEnabled
Event Type	cloudAPRegistrarSyncEnabled
Event Code	4801
Severity	Informational
Attribute	
Displayed on the web interface	Cloud AP Registrar Synchronization have been enabled successfully.
Description	This event occurs when Smart Zone successfully enables Cloud AP Registrar Synchronization.

Parent topic: [Cloud Events](#)

## cloudAPRegistrarSyncDisabled

**Table 1.** cloudAPRegistrarSyncDisabled event

Event	cloudAPRegistrarSyncDisabled
Event Type	cloudAPRegistrarSyncDisabled
Event Code	4802
Severity	Informational
Attribute	
Displayed on the web interface	Cloud AP Registrar Synchronization have been disabled successfully.
Description	This event occurs when Smart Zone successfully disables Cloud AP Registrar Synchronization.

Parent topic: [Cloud Events](#)

## cloudAPRegistrarSyncSZInfo

**Table 1.** cloudAPRegistrarSyncEnabled event

Event	cloudAPRegistrarSyncSZInfo
Event Type	cloudAPRegistrarSyncSZInfo
Event Code	4803
Severity	Informational
Attribute	
Displayed on the web interface	Cloud AP Registrar have been synced with latest SZ info successfully.
Description	This event occurs when Smart Zone successfully syncs Smartzone info to AP Registrar.

Parent topic: [Cloud Events](#)

## cloudAPRegistrarSyncAPInfo

**Table 1.** cloudAPRegistrarSyncAPInfo event

Event	cloudAPRegistrarSyncAPInfo
Event Type	cloudAPRegistrarSyncAPInfo
Event Code	4804
Severity	Informational
Attribute	
Displayed on the web interface	Cloud AP Registrar have been synced with latest SZ info successfully.
Description	This event occurs when Smart Zone successfully synced AP info to AP Registrar.

Parent topic: [Cloud Events](#)

# Cluster Events

Following are the events related to clusters.

Event	Event	Event
Cluster created successfully	New node joined successfully	New node failed to join
Node removal completed	Node removal failed	Node out of service
Cluster in maintenance state	Cluster back in service	Cluster backup completed
Cluster backup failed	Cluster restore completed	Cluster restore failed
Cluster node upgrade completed	Entire cluster upgraded successfully	Cluster upgrade failed
Cluster application stopped	Cluster application started	Cluster backup started
Cluster upgrade started	Cluster leader changed	Node bond interface down
Node bond interface up	Node IP address changed	Node physical interface down
Node physical interface up	Cluster node rebooted	NTP time synchronized
Cluster node shutdown	Cluster upload started	Cluster upload completed
Cluster upload failed	SSH tunnel switched	Cluster remove node started
Node back in service	Disk usage exceed threshold	Cluster out of service
Initiated moving APs in node to a new cluster	Cluster upload vSZ-D firmware started	Cluster upload vSZ-D firmware completed
Cluster upload vSZ-D firmware failed	Cluster upload AP firmware started	Cluster upload AP firmware completed
Cluster upload AP firmware failed	Cluster add AP firmware started	Cluster add AP firmware completed

Event	Event	Event
Cluster add AP firmware failed	Cluster name is changed	Unsync NTP Time
Cluster upload KSP file started	Cluster upload KSP file completed	Cluster upload KSP file failed
NTP unreachable server	Configuration backup started	Configuration backup succeeded
Configuration backup failed	Configuration restore succeeded	Configuration restore failed
AP Certificate Expired	AP Certificate Updated	Configuration restore started
Upgrade SSTable failed	Reindex elastic search finished	Initiated APs contact APR
All nodes back in service	Not management service ready	Management service ready
Configuration sync failed	Node IPv6 address deleted	Node IPv6 address added
AP is connected to Standby Cluster over the Expiration Date	Sync Configuration Failed for Cluster Redundancy	Standby Cluster Failed to Restore a Configuration for Cluster Redundancy
Standby Cluster Back to Monitoring Mode for Cluster Redundancy	Standby Cluster Restored a Configuration Success for Cluster Redundancy	AP Connected to Standby Cluster after Rehome Timeout
External DP Connected to Standby Cluster after Rehome Timeout	Sync Configuration started for Cluster Redundancy	Standby Cluster Restores a Configuration for Cluster Redundancy
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy		

**Parent topic:** [Events Types](#)

## Cluster created successfully

**Table 1.** Cluster created successfully event

Event	Cluster created successfully
Event Type	clusterCreatedSuccess
Event Code	801
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Cluster [{clusterName}] created with node [{nodeName}]
Description	This event occurs when a cluster and a node are created.

Parent topic: [Cluster Events](#)

## New node joined successfully

**Table 1.** 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"

Event	New node joined successfully
Displayed on the web interface	New node [{nodeName}] joined cluster [{clusterName}]
Description	This event occurs when a node joins a cluster session.

Parent topic: [Cluster Events](#)

## New node failed to join

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Node removal completed

**Table 1.** Node removal completed event

Event	Node removal completed
Event Type	removeNodeSuccess
Event Code	804
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] removed from cluster [{clusterName}]
Description	This event occurs when a node is removed from the cluster session.

Parent topic: [Cluster Events](#)

## Node removal failed

**Table 1.** 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"

Event	Node removal failed
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.

Parent topic: [Cluster Events](#)

## Node out of service

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster in maintenance state

**Table 1.** Cluster in maintenance state event

Event	Cluster in maintenance state
Event Type	clusterInMaintenanceState
Event Code	807
Severity	Critical
Attribute	"clusterName"="xxx"
Displayed on the web interface	[[clusterName]] is in maintenance state
Description	This event occurs when a node is in a maintenance state.
Auto Clearance	This event triggers the alarm 804, which is auto cleared by the event code 808.

Parent topic: [Cluster Events](#)

## Cluster back in service

**Table 1.** 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

Event	Cluster back in service
Description	This event occurs when a cluster is back in service.

Parent topic: [Cluster Events](#)

## Cluster backup completed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster backup failed

**Table 1.** Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810
Severity	Major

Event	Cluster backup failed
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.

Parent topic: [Cluster Events](#)

## Cluster restore completed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster restore failed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster node upgrade completed

**Table 1.** 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",

Event	Cluster node upgrade completed
	"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.

Parent topic: [Cluster Events](#)

## Entire cluster upgraded successfully

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upgrade failed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster application stopped

**Table 1.** Cluster application stopped event

Event	Cluster application stopped
Event Type	clusterAppStop
Event Code	816
Severity	Critical
Attribute	"appName"="xxxx", "nodeName"="xxx",

Event	Cluster application stopped
	"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.

Parent topic: [Cluster Events](#)

## Cluster application started

**Table 1.** Cluster application started event

Event	Cluster application started
Event Type	clusterAppStart
Event Code	817
Severity	Informational
Attribute	"appName"="xxx", "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.

Parent topic: [Cluster Events](#)

## Cluster backup started

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upgrade started

**Table 1.** 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}]

Event	Cluster upgrade started
Description	This event occurs when an upgrade for a node commences.

Parent topic: [Cluster Events](#)

## Cluster leader changed

**Table 1.** Cluster leader changed event

Event	Cluster leader changed
Event Type	clusterLeaderChanged
Event Code	820
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] promoted to leader
Description	This event occurs when a node is changed to a lead node.

Parent topic: [Cluster Events](#)

## Node bond interface down

**Table 1.** Node bond interface down event

Event	Node bond interface down
Event Type	nodeBondInterfaceDown
Event Code	821

Event	Node bond interface down
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.

Parent topic: [Cluster Events](#)

## Node bond interface up

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Node IP address changed

**Table 1.** Node IP address changed event

Event	Node IP address changed
Event Type	nodeIPChanged
Event Code	823
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx", "ip"="xxx.xxx.xxx.xxx"
Displayed on the web interface	IP address of network interface [{networkInterface}   ifName}] on node [{nodeName}] changed to [{ip}].
Description	This event occurs when the node's network interface IP address changes.

Parent topic: [Cluster Events](#)

## Node physical interface down

**Table 1.** 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.

Event	Node physical interface 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.

Parent topic: [Cluster Events](#)

## Node physical interface up

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster node rebooted

**Table 1.** Cluster node rebooted event

Event	Cluster node rebooted
Event Type	nodeRebooted

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

Parent topic: [Cluster Events](#)

## NTP time synchronized

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster node shutdown

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload started

**Table 1.** 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}].

Event	Cluster upload started
Description	This event occurs when the cluster upload process starts.

Parent topic: [Cluster Events](#)

## Cluster upload completed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload failed

**Table 1.** Cluster upload failed event

Event	Cluster upload failed
Event Type	uploadClusterFailed
Event Code	832
Severity	Major

Event	Cluster upload failed
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.

Parent topic: [Cluster Events](#)

## SSH tunnel switched

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster remove node started

**Table 1.** Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName" = "xxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Start to remove node [{nodeName}] from cluster [{clusterName}]
Description	This event occurs when the node start is removed.

Parent topic: [Cluster Events](#)

## Node back in service

**Table 1.** 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

Event	Node back in service
Description	This event occurs when a node status changes to 'in service'.

Parent topic: [Cluster Events](#)

## Disk usage exceed threshold

**Table 1.** 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%.

Parent topic: [Cluster Events](#)

## Cluster out of service

**Table 1.** Cluster out of service event

Event	Cluster out of service
Event Type	clusterOutOfService
Event Code	843

Event	Cluster out of service
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.
Auto Clearance	This event triggers the alarm 843, which is auto cleared by the event code 808.

Parent topic: [Cluster Events](#)

## Initiated moving APs in node to a new cluster

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload vSZ-D firmware started

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload vSZ-D firmware completed

**Table 1.** 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"

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.

Parent topic: [Cluster Events](#)

## Cluster upload vSZ-D firmware failed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload AP firmware started

**Table 1.** Cluster upload AP firmware started event

Event	Cluster upload AP firmware started
Event Type	clusterUploadAPFirmwareStart

Event	Cluster upload AP firmware started
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.

Parent topic: [Cluster Events](#)

## Cluster upload AP firmware completed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload AP firmware failed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster add AP firmware started

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster add AP firmware completed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster add AP firmware failed

**Table 1.** Cluster add AP firmware failed event

Event	Cluster add AP firmware failed
Event Type	clusterAddAPFirmwareFailed
Event Code	853
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} add AP firmware failed. Reason:{{reason}}.

Event	Cluster add AP firmware failed
Description	This event occurs when the cluster add process to the AP firmware fails.

Parent topic: [Cluster Events](#)

## Cluster name is changed

**Table 1.** Cluster name is changed event

Event	Cluster name is changed
Event Type	clusterNameChanged
Event Code	854
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster name is changed to [[clusterName]]
Description	<p>This event occurs when the cluster node name is modified. By enabling email and SNMP notification in the controller user interface (<b>Configuration &gt; System &gt; Event Management</b>) of the event, SNMP trap and email will be generated on successful cluster-name modification.</p> <p>Cluster name change will fail if any node in either a two, three or four node cluster is out of service. For example, if in a three node cluster, any one node is powered off or the Ethernet cable is unplugged, cluster name change will fail.</p>

Parent topic: [Cluster Events](#)

## Unsync NTP Time

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Cluster upload KSP file started

**Table 1.** Cluster upload KSP file started event

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

Parent topic: [Cluster Events](#)

## Cluster upload KSP file completed

**Table 1.** 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 ksp file successfully.

Parent topic: [Cluster Events](#)

## Cluster upload KSP file failed

**Table 1.** 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 ksp file.
Auto Clearance	This event triggers the alarm 858, which is auto cleared by the event code 857.

Parent topic: [Cluster Events](#)

## NTP unreachable server

**Table 1.** NTP unreachable server

Event	NTP unreachable server
Event Type	NTP server reach failed
Event Code	859
Severity	Critical
Attribute	NTP server
Displayed on the web interface	System cannot reach NTP sever [NTP Server]
Description	This event occurs when system fails to reach the NTP server.

Parent topic: [Cluster Events](#)

## Configuration backup started

**Table 1.** Configuration backup started event

Event	Configuration backup started
Event Type	clusterCfgBackupStart
Event Code	860
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration backup is started.
Description	This event occurs when cluster configuration backup starts.

Parent topic: [Cluster Events](#)

## Configuration backup succeeded

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Configuration backup failed

**Table 1.** 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.

Event	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.

Parent topic: [Cluster Events](#)

## Configuration restore succeeded

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Configuration restore failed

**Table 1.** Configuration restore failed event

Event	Configuration restore failed
Event Type	clusterCfgRestoreFailed

Event	Configuration restore failed
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.

Parent topic: [Cluster Events](#)

## AP Certificate Expired

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## AP Certificate Updated

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Configuration restore started

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Upgrade SStable failed

**Table 1.** Upgrade SStable failed event

Event	Upgrade SStable failed
Event Type	upgradeSStableFailed
Event Code	868
Severity	Major

Event	Upgrade SSTable failed
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.

Parent topic: [Cluster Events](#)

## Reindex elastic search finished

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Initiated APs contact APR

**Table 1.** Initiated APs contact APR event

Event	Initiated APs contact APR
Event Type	clusterInitContactApr
Event Code	870
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{ clusterName}] initiated APs contact APR
Description	This event occurs on receiving APs contact APR configuration command.

Parent topic: [Cluster Events](#)

## All nodes back in service

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Not management service ready

**Table 1.** 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

Parent topic: [Cluster Events](#)

## Management service ready

**Table 1.** Management service ready event

Event	Management service ready
Event Type	allServiceInService

Event	Management service ready
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.

Parent topic: [Cluster Events](#)

## Configuration sync failed

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Node IPv6 address added

**Table 1.** Node IPv6 address added event

Event	Node IPv6 address added
Event Type	nodeIPv6Added
Event Code	2501

Event	Node IPv6 address added
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.

Parent topic: [Cluster Events](#)

## AP is connected to standby cluster over the expiration date

**Table 1.** AP is connected to standby cluster over the expiration date event

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

Parent topic: [Cluster Events](#)

## Node IPv6 address deleted

**Table 1.** 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.

Parent topic: [Cluster Events](#)

## Sync Configuration started for Cluster Redundancy

**Table 1.** Sync Configuration started for Cluster Redundancy Event

Event	Sync Configuration started for Cluster Redundancy
Event Type	SyncCfgStartClusterRedundancy
Event Code	875
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] sync configuration start for cluster redundancy.
Description	This event occurs when sync configuration start for cluster redundancy.

Parent topic: [Cluster Events](#)

## Sync Configuration Success for Cluster Redundancy

**Table 1.** Sync Configuration Success for Cluster Redundancy Event

Event	Sync Configuration Success for Cluster Redundancy
Event Type	SyncCfgSuccessClusterRedundancy
Event Code	876
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] sync configuration success for cluster redundancy.
Description	This event occurs when sync configuration success for cluster redundancy.

Parent topic: [Cluster Events](#)

## Standby Cluster Failed to Restore a Configuration for Cluster Redundancy

**Table 1.** Standby Cluster Failed to Restore a Configuration for Cluster Redundancy event

Event	Cluster restore failed
Event Type	RestoreClusterFailedforClusterRedundancy
Event Code	877
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] restore failed for cluster redundancy. Reason[{reason}].
Description	This event occurs when standby cluster failed to restore a configuration for cluster redundancy.

Parent topic: [Cluster Events](#)

## Standby Cluster Restores a Configuration for Cluster Redundancy

**Table 1.** Standby Cluster Restores a Configuration for Cluster Redundancy event

Event	Standby Cluster Restores a Configuration for Cluster Redundancy
Event Type	StandbyClusterRestoresConfigurationForClusterRedundancy
Event Code	878
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] restores for cluster redundancy.
Description	This event occurs when standby cluster restored a configuration success for cluster redundancy.

Parent topic: [Cluster Events](#)

## Standby Cluster Restored a Configuration Success for Cluster Redundancy

**Table 1.** Standby Cluster Restored a Configuration Success for Cluster Redundancy event

Event	Standby Cluster Restored a Configuration Success for Cluster Redundancy
Event Type	StandbyClusterRestoredaConfigurationSuccessforClusterRedundancy
Event Code	879
Severity	Informational

Event	Standby Cluster Restored a Configuration Success for Cluster Redundancy
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] restored a configuration success for cluster redundancy.
Description	This event occurs when standby cluster restored a configuration success for cluster redundancy.

Parent topic: [Cluster Events](#)

## Standby Cluster Back to Monitoring Mode for Cluster Redundancy

**Table 1.** Standby Cluster Back to Monitoring Mode for Cluster Redundancy event

Event	Standby Cluster Back to Monitoring Mode for Cluster Redundancy
Event Type	StandbyClusterBacktoMonitoringModeforClusterRedundancy
Event Code	880
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] back to monitoring mode for cluster redundancy.
Description	This event occurs when standby cluster back to monitoring mode for cluster redundancy.

Parent topic: [Cluster Events](#)

## AP Connected to Standby Cluster after Rehome Timeout

**Table 1.** AP Connected to Standby Cluster after Rehome Timeout event

Event	AP Connected to Standby Cluster after Rehome Timeout
Event Type	APConnectedtoStandbyClusterAfterRehomeTimeout
Event Code	881
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Standby Cluster [{clusterName}] AP connected after rehome timeout
Description	This event occurs when there is still AP connected to standby cluster after rehome timeout.

Parent topic: [Cluster Events](#)

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

**Table 1.** Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy event

Event	Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Event Type	ActiveClusterUnabletoConnectOtherActiveCustersforClusterRedundancy
Event Code	882
Severity	Major
Attribute	"clusterName"="xxx"

Event	Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Displayed on the web interface	[[clusterName]] Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
Description	This event occurs when active cluster unable to connect to other active clusters for cluster redundancy.

Parent topic: [Cluster Events](#)

## External DP Connected to Standby Cluster after Rehome Timeout

**Table 1.** External DP Connected to Standby Cluster after Rehome Timeout event

Event	External DP Connected to Standby Cluster after Rehome Timeout
Event Type	ExternalDPConnectedtoStandbyClusterafterRehomeTimeout
Event Code	887
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	[[clusterName]]This event occurs when there is still external DP connected to standby cluster after rehome timeout
Description	This event occurs when there is still external DP connected to standby cluster after rehome timeout.

Parent topic: [Cluster Events](#)

## Certificate is about to Expire

**Table 1.** Certificate is about to Expire event

Event	Certificate is about to Expire
Event Type	certificateAboutToExpire
Event Code	890
Severity	Major
Attribute	"certName"="xxx", days="x", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate [{certName}] is about to expire in [{days}] days ({expireDateTime})
Description	This event occurs when certificate is about to expire.

Parent topic: [Cluster Events](#)

## Certificate is already Expired

**Table 1.** Certificate is already Expired event

Event	Certificate is already Expired
Event Type	certificateExpire
Event Code	891
Severity	Major
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate is already expired
Description	This event occurs when certificate is already expired

Parent topic: [Cluster Events](#)

## Result of Renew Certificate

**Table 1.** Result of Renew Certificate event

Event	Result of Renew Certificate
Event Type	certificateGenerateResult
Event Code	892
Severity	Major
Attribute	"certName"="xxx", "result"="xxx"
Displayed on the web interface	Result of renew certificate [{certName}] : {result}
Description	This event occurs to show the result of renew certificate

Parent topic: [Cluster Events](#)

## Cluster node Resource Invalid

**Table 1.** Cluster node Resource Invalid event

Event	Cluster node Resource Invalid
Event Type	clusterNodeResourceInvalid
Event Code	886
Severity	Major
Attribute	
Displayed on the web interface	

Event	Cluster node Resource Invalid
Description	This event occurs when one of the nodes resource is invalid.

Parent topic: [Cluster Events](#)

## Configuration Events

Following are the events related to configuration:

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

Parent topic: [Events Types](#)

## Configuration updated

**Table 1.** 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.

Parent topic: [Configuration Events](#)

## Configuration update failed

**Table 1.** Configuration update failed event

Event	Configuration update failed
Event Type	cfgUpdFailed
Event Code	1008
Severity	Debug

Event	Configuration update failed
Attribute	<pre>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" , "srcProcess"="cnr" "realm"="NA"  "processName"="aut" "SCGMgmtIp"="x.x.x.x" "cause"="xx"</pre>
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.

Parent topic: [Configuration Events](#)

## Configuration receive failed

**Table 1.** Configuration receive failed event

Event	Configuration receive failed
Event Type	cfgRcvFailed
Event Code	1009
Severity	Debug
Attribute	<pre>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="cnr" "realm"="NA"  "SCGMgmtIp"="x.x.x.x", "cause"="xx"</pre>
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

Event	Configuration receive failed
	information from the configuration change notifier (CCN).

Parent topic: [Configuration Events](#)

## Incorrect flat file configuration

**Table 1.** Incorrect flat file configuration event

Event	Incorrect flat file configuration
Event Type	incorrectFlatFileCfg
Event Code	1012
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut", "realm"="NA",  "SCGMgmtIp"="xxx", "cause"="xxx", "file"="xx"
Displayed on the web interface	[[srcProcess]] detected an configuration parameter is incorrectly configured in file [[file]] at {produce.short.name} [[SCGMgmtIp]].
Description	This event occurs when any flat file configuration parameter is not semantically or syntactically correct.

Parent topic: [Configuration Events](#)

## Zone configuration preparation failed

**Table 1.** Zone configuration preparation failed event

Event	Zone configuration preparation failed
Event Type	zoneCfgPrepareFailed

Event	Zone configuration preparation failed
Event Code	1021
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90","zoneName"="open Zone"
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.

Parent topic: [Configuration Events](#)

## AP configuration generation failed

**Table 1.** 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"="open Zone","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.

Parent topic: [Configuration Events](#)

## End-of-life AP model detected

**Table 1.** 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"="open Zone", "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](#).

Parent topic: [Configuration Events](#)

## VLAN configuration mismatch on non-DHCP/NAT WLAN

**Table 1.** 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"

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN.
Displayed on the web interface	DHCP/NAT gateway AP [{{apMac}}] detected VLAN configuration mismatch on non-DHCP/NAT WLAN [{{ssid}}]. Configured VLAN is [{{configuredVlan}}] and resolved VLAN is [{{vlanId}}]. Clients may not be able to get IP or access Internet.
Description	This event occurs when the AP detects a non DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

Parent topic: [Configuration Events](#)


## VLAN configuration mismatch on DHCP/NAT WLAN

**Table 1.** 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.

Parent topic: [Configuration Events](#)

## Generation failed during CCM GPB generation


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Configuration Events](#)

## Preparation failed during AP knowledge generation

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** Preparation failed during AP knowledge generation event

Event	Preparation failed during AP knowledge generation
Event Type	ccmApTraversalPrepareFailed
Event Code	9021
Severity	Major
Attribute	topicName = "SimpleTopci"
Displayed on the web interface	Failed to generate [{{topicName}}] GPB

Event	Preparation failed during AP knowledge generation
Description	This event occurs when controller fails to generate GPB for a certain topic.

Parent topic: [Configuration Events](#)

## Generation failed during AP knowledge generation


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Configuration Events](#)

## End-of-life AP model detected during AP knowledge generation


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Configuration Events](#)

## Notification failed during AP knowledge generation

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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"

Event	Notification failed during AP knowledge generation
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.

Parent topic: [Configuration Events](#)

## Datablade Events

The following are the events related to Datablade Based Service.

- [DP integrity test failed](#)
- [DP CLI enable failed](#)
- [DP re-authentication](#)
- [DP password min length updated](#)
- [DP password changed](#)
- [DP enable password changed](#)
- [DP https authentication failed](#)
- [DP certificate uploaded](#)
- [DP Scg FQDN updated](#)
- [DP initial upgrade](#)
- [DP discontinuous time change NTP server DP Ntp time sync](#)
- [DP user login](#)
- [DP user login failed](#)
- [DP user logout](#)

- [DP account locked](#)
- [DP session idle updated](#)
- [DP session idle terminated](#)
- [DP SSH tunnel failed](#)
- [DP https connection failed](#)
- [DP IPsec tunnel create failed](#)

Parent topic: [Events Types](#)

## DP integrity test failed

**Table 1.** DP integrity test failed event

Event	DP integrity test failed
Event Type	dpIntegrityTestFailed
Event Code	99200
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	Data plane [{dpKey}] self integrity test failed
Description	This event occurs when the data plane self integrity test failed.

Parent topic: [Datablade Events](#)

## DP CLI enable failed

**Table 1.** DP CLI enable failed event

Event	DP CLI enable failed
Event Type	dpCliEnableFailed

Event	DP CLI enable failed
Event Code	99201
Severity	Informational
Attribute	"dpKey"="XXXX", "source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] CLI enabled failed, [{source}].
Description	This event occurs when the data plane CLI enabled failed.

Parent topic: [Datablade Events](#)

## DP re-authentication

**Table 1.** DP re-authentication event

Event	DP re-authentication
Event Type	dpReAuth
Event Code	99202
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console/WebGUI"
Displayed on the web interface	Data plane [{dpKey}] attempt to re-authenticate, [{source}].
Description	This event occurs when the data plane attempt to re-authenticate.

Parent topic: [Datablade Events](#)

## DP password min length updated

**Table 1.** DP password min length updated event

Event	DP password min length updated
Event Type	dpPasswordMinLengthUpdated
Event Code	99203
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console/webGUI"
Displayed on the web interface	Data plane [{dpKey}] min password length changed, [{source}].
Description	This event occurs when the data plane min password length changed.

Parent topic: [Datablade Events](#)

## DP password changed

**Table 1.** DP password changed event

Event	DP password changed
Event Type	dpPasswordChanged
Event Code	99204
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console/webGUI"
Displayed on the web interface	Data plane [{dpKey}] password changed, [{source}].
Description	This event occurs when the data plane password changed.

Parent topic: [Datablade Events](#)

## DP enable password changed

**Table 1.** DP enable password changed event

Event	DP enable password changed
Event Type	dpEnablePasswordChanged
Event Code	99205
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] enable password changed, [{source}].
Description	This event occurs when the data plane enable password changed.

Parent topic: [Datablade Events](#)

## DP https authentication failed

**Table 1.** DP https authentication failed event

Event	DP https authentication failed
Event Type	dpHttpsAuthFailed
Event Code	99206
Severity	Informational
Attribute	"dpKey"="XXXX", "reason"="xxx"
Displayed on the web interface	Data plane [{dpKey}] certificate verification failed, [{source}].

Event	DP https authentication failed
Description	This event occurs when the data plane certificate verification failed.

Parent topic: [Datablade Events](#)

## DP certificate uploaded

**Table 1.** DP certificate uploaded event

Event	DP certificate uploaded
Event Type	dpCertUploaded
Event Code	99207
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	Data plane [{dpKey}] certificate trusted CA chain uploaded.
Description	This event occurs when the data plane certificate trusted CA chain uploaded.

Parent topic: [Datablade Events](#)

## DP Scg FQDN updated

**Table 1.** DP Scg FQDN updated event

Event	DP Scg FQDN updated
Event Type	dpScgFqdnUpdated
Event Code	99208

Event	DP Scg FQDN updated
Severity	Informational
Attribute	"dpKey"="XXXX", "fqdn"="xxx.xxx.xxx"
Displayed on the web interface	SZ [{scgIP}] FQDN [{fqdn}] setting on DP [{dpKey}]
Description	This event occurs when the SZ FQDN setting on data plane.

Parent topic: [Datablade Events](#)

## DP initial upgrade

**Table 1.** DP initial upgrade event

Event	DP initial upgrade
Event Type	dpInitUpgrade
Event Code	99210
Severity	Informational
Attribute	"dpKey"="XXXX", "source"="xxx"
Displayed on the web interface	Data plane [{dpKey}] initiate to upgrade, [{source}].
Description	This event occurs when the data plane initiate to upgrade.

Parent topic: [Datablade Events](#)

## DP discontinuous time change NTP server DP Ntp time sync

**Table 1.** DP discontinuous time change NTP server DP Ntp time sync event

Event	DP discontinuous time change NTP server DP Ntp time sync
Event Type	dpDiscontinuousTimeChangeNTPServerdpNtpTimeSync
Event Code	99211
Severity	Informational
Attribute	"dpKey"="XXXX", "before"="XXXX", "after"="XXXX", "source"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] time change due to ntp sync, from [{before}] to [{after}], Source: [{source}].
Description	This event occurs when the data plane time change due to ntp sync.

Parent topic: [Datablade Events](#)

## DP user login

**Table 1.** DP user login event

Event	DP user login
Event Type	dpUserLogin
Event Code	99212
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User login into data plane [{dpKey}], Source: [{source}].

Event	DP user login
Description	This event occurs when the user login into data plane.

Parent topic: [Datablade Events](#)

## DP user login failed

**Table 1.** DP user login failed event

Event	DP user login failed
Event Type	dpUserLoginFailed
Event Code	99213
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User login into data plane [{dpKey}] and failed, Source: [{source}].
Description	This event occurs when the user login into data plane and failed.

Parent topic: [Datablade Events](#)

## DP user logout

**Table 1.** DP user logout event

Event	DP user logout
Event Type	dpUserLogout
Event Code	99214
Severity	Informational

Event	DP user logout
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User logout to data plane [{dpKey}], Source: [{source}].
Description	This event occurs when the user logout to data plane.

Parent topic: [Datablade Events](#)

## DP account locked

**Table 1.** DP account locked event

Event	DP account locked
Event Type	dpAccountLocked
Event Code	99215
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	User account was locked, data plane: [{dpKey}].
Description	This event occurs when the user account was locked.

Parent topic: [Datablade Events](#)

## DP session idle updated

**Table 1.** DP session idle updated event

Event	DP session idle updated
Event Type	dpSessionIdleUpdated

Event	DP session idle updated
Event Code	99220
Severity	Informational
Attribute	"dpKey"="XXXX", "sessionIdle"="xx", "Source"="console/webGui"
Displayed on the web interface	Data plane [{dpKey}] session timeout [{sessionIdle}] change, [{source}].
Description	This event occurs when the data plane session timeout change.

Parent topic: [Datablade Events](#)

## DP session idle terminated

**Table 1.** DP session idle terminated event

Event	DP session idle terminated
Event Type	dpSessionIdleTerminated
Event Code	99221
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] session terminated due to timeout, [{source}].
Description	This event occurs when the data plane session terminated due to timeout.

Parent topic: [Datablade Events](#)

## DP SSH tunnel failed

**Table 1.** DP SSH tunnel failed event

Event	DP SSH tunnel failed
Event Type	dpSshTunnFailed
Event Code	99230
Severity	Informational
Attribute	"dpKey"="XXXX", "scgIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] establish ssh tunnel failed, SZ [{scgIP}]
Description	This event occurs when the data plane establish ssh tunnel failed.

Parent topic: [Datablade Events](#)

## DP https connection failed

**Table 1.** DP https connection failed event

Event	DP https connection failed
Event Type	dpHttpsConnFailed
Event Code	99231
Severity	Informational
Attribute	"dpKey"="XXXX", "scgIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] https connection failed, SZ [{scgIP}]

Event	DP https connection failed
Description	This event occurs when the data plane https connection failed.

Parent topic: [Datablade Events](#)


## DP IPsec tunnel create failed

**Table 1.** DP IPsec tunnel create failed event

Event	DP IPsec tunnel create failed
Event Type	dpIPsecTunnCreateFailed
Event Code	99240
Severity	Informational
Attribute	"dpKey"="XXXX", "dpIP"="x.x.x.x", apIP="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey&&dpIP}] IPsec tunnel establishment failed, AP [{apIP}].
Description	This event occurs when the data plane IPsec tunnel establishment failed.

Parent topic: [Datablade Events](#)

## Data Plane Events

 **Note:** Events 530, 532, 537, 538, 550, 551, 552 and 553 are not applicable for SZ300/SZ100.

Following are the events related to the data plane:

Event	Event	Event
Data plane discovered	Data plane discovery failed	Data plane configuration updated
Data plane configuration update failed	Data plane rebooted	Data plane heartbeat lost
Data plane IP address updated	Data plane updated to a new control plane	Data plane status update failed
Data plane statistics update failed	Data plane connected	Data plane disconnected
Data plane physical interface down	Data plane physical interface up	Data plane packet pool is under low water mark
Data plane packet pool is under critical low water mark	Data plane packet pool is above high water mark	Data plane core dead
Data plane process restarted	Data plane discovery succeeded	Data plane managed
Data plane deleted	Data plane license is not enough	Data plane upgrade started
Data plane upgrading	Data plane upgrade succeeded	Data plane upgrade failed
Data plane of data center side successfully connects to the CALEA server	Data plane of data center side fails to connect to the CALEA server	Data Plane of data center side disconnects to CALEA server
Data plane successfully connects to the other data plane	Data plane fails to connect to the other data plane	Data plane disconnects to the other data plane
Start CALEA mirroring client in data plane	Data plane DHCP IP pool usage rate is 100 percent	Data plane DHCP IP pool usage rate is 80 percent
Data plane NAT session capacity usage rate is 80 percent	Data plane NAT session capacity usage rate is 100 percent	Data plane DHCP IP capacity usage rate is 80 percent
Data plane DHCP IP capacity usage rate is 100 percent	Data plane backup success	Data plane backup failed

Event	Event	Event
Data plane restore success	Data plane restore failed	Remote Administration
Remote Administration		

Parent topic: [Events Types](#)

## Data plane discovered

**Table 1.** 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}].
Description	This event occurs when the data plane successfully connects to the controller.

Parent topic: [Data Plane Events](#)

## Data plane discovery failed

**Table 1.** Data plane discovery failed event

Event	Data plane discovery failed
Event Type	dpDiscoveryFail (detected on the server side)
Event Code	502

Event	Data plane discovery failed
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] failed to send a discovery request to {produce.short.name} [{cpName   wsgIP}].
Description	This event occurs when the data plane fails to connect to the controller.

Parent topic: [Data Plane Events](#)

## Data plane configuration updated

**Table 1.** Data plane configuration updated event

Event	Data plane configuration updated
Event Type	dpConfUpdated
Event Code	504
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"="123456781234567"
Displayed on the web interface	Data plane [{dpName   dpKey}] updated to configuration [{configID}].
Description	This event occurs when the data plane configuration is updated.

Parent topic: [Data Plane Events](#)

## Data plane configuration update failed

**Table 1.** Data plane configuration update failed event

Event	Data plane configuration update failed
Event Type	dpConfUpdateFailed
Event Code	505
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"="123456781234567"
Displayed on the web interface	Data plane [{dpName}   {dpKey}] failed to update to configuration [{configID}]
Description	This event occurs when the data plane configuration update fails.
Auto Clearance	This event triggers the alarm 501, which is auto cleared by the event code 504.

Parent topic: [Data Plane Events](#)

## Data plane rebooted

**Table 1.** 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",

Event	Data plane rebooted
Displayed on the web interface	Data plane [{dpName     dpKey}] rebooted
Description	This event occurs when the data plane is rebooted.

Parent topic: [Data Plane Events](#)

## Data plane heartbeat lost

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane IP address updated

**Table 1.** Data plane IP address updated event

Event	Data plane IP address updated
Event Type	dpIPChanged
Event Code	508

Event	Data plane IP address updated
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.

Parent topic: [Data Plane Events](#)

## Data plane updated to a new control plane

**Table 1.** 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
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.

Parent topic: [Data Plane Events](#)

## Data plane status update failed

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane statistics update failed

**Table 1.** 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}].

Event	Data plane statistics update failed
Description	This event occurs when the data plane fails to update statistics to the controller.

Parent topic: [Data Plane Events](#)

## Data plane connected

**Table 1.** Data plane connected event

Event	Data plane connected
Event Type	dpConnected
Event Code	512
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] connected to {produce.short.name} [{cpName   wsgIP}].
Description	This event occurs when the data plane connects to the controller.

Parent topic: [Data Plane Events](#)

## Data plane disconnected

**Table 1.** Data plane disconnected event

Event	Data plane disconnected
Event Type	dpDisconnected
Event Code	513

Event	Data plane disconnected
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName   dpKey}] disconnected from {produce.short.name} {cpName   wsgIP}.
Description	This 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.

Parent topic: [Data Plane Events](#)

## Data plane physical interface down

**Table 1.** 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: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.

Parent topic: [Data Plane Events](#)

## Data plane physical interface up

**Table 1.** 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:xx"
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName}     dpKey}] is up.
Description	This event occurs when the network link of the data plane is up.

Parent topic: [Data Plane Events](#)

## Data plane packet pool is under low water mark

**Table 1.** 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.

Event	Data plane packet pool 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.

Parent topic: [Data Plane Events](#)

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

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane packet pool is above high water mark

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane core dead

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane process restarted

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane discovery succeeded

 **Note:**

This event is not applicable to SZ300/SZ100.

**Table 1.** Data plane discovery succeeded event

Event	Data plane discovery succeeded
Event Type	dpDiscoverySuccess

Event	Data plane discovery succeeded
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.

Parent topic: [Data Plane Events](#)

## Data plane managed

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** Data plane managed event

Event	Data plane managed
Event Type	dpStatusManaged
Event Code	532
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] approved by {produce.short.name} [{wsgIP}].

Event	Data plane managed
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.

Parent topic: [Data Plane Events](#)

## Data plane deleted

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane license is not enough

**Table 1.** Data plane license is not enough event

Event	Data plane license is not enough
Event Type	dpLicenseInsufficient

Event	Data plane license is not enough
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.

Parent topic: [Data Plane Events](#)

## Data plane upgrade started

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane upgrading

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane upgrade succeeded

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

## Data plane upgrade failed

**Table 1.** Data plane upgrade failed event

Event	Data plane upgrade failed
Event Type	dpUpgradeFailed
Event Code	553
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to upgrade.
Description	This event occurs when data plane upgrade fails.
Auto Clearance	This event triggers the alarm 553, which is auto cleared by the event code 552.

Parent topic: [Data Plane Events](#)

## Data Plane Upgrade Failed Due to Corrupted RPM

**Table 1.** dpUpgradeFailedDueToCorruptedRpm event

Event	dpUpgradeFailedDueToCorruptedRpm
Event Type	dpUpgradeFailedDueToCorruptedRpm
Event Code	554
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"

Event	dpUpgradeFailedDueToCorruptedRpm
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to upgrade due to corrupted RPM file; data plane would reboot and please upgrade again after the reboot.
Description	This event occurs when the data plane fails to upgrade due to corrupted RPM file.

Parent topic: [Data Plane Events](#)

## Data plane of data center side successfully connects to the CALEA server

### Note:

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** Data plane of data center side successfully connects to the CALEA server event

Event	Data plane of data center side successfully connects to the CALEA server
Event Type	dpDcToCaleaConnected
Event Code	1257
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [{dpName&&dpKey}] successfully connects to the CALEA server[{caleaServerIP}].
Description	This event occurs when the data plane successfully connects to the CALEA server.

Parent topic: [Data Plane Events](#)

## 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 1.** Data plane of data center side fails to connect to the CALEA server event

Event	Data plane of data center side fails to connect to the CALEA server.
Event Type	dpDcToCaleaConnectFail
Event Code	1258
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [{dpName&&dpKey}] fails to connects to the CALEA server[{caleaServerIP}]
Description	This event occurs when the data plane fails to connect to the CALEA server.
Auto Clearance	This event triggers the alarm 1258, which is auto cleared by the event code 1257.

Parent topic: [Data Plane Events](#)

## Data Plane of data center side disconnects to CALEA server

 **Note:**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** 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

Event	Data Plane of data center side disconnects to CALEA server.
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.

Parent topic: [Data Plane Events](#)

## Data plane successfully connects to the other data plane

### Note:

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

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

 **Note:**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** 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}]
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.

Parent topic: [Data Plane Events](#)

## Data plane disconnects to the other data plane

 **Note:**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** 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

Event	Data plane disconnects to the other data plane
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIp"="xxx.x xx.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.

Parent topic: [Data Plane Events](#)

## Start CALEA mirroring client in data plane

### Note:

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** 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.

Parent topic: [Data Plane Events](#)

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

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** Data plane DHCP IP pool usage rate is 100 percent event

Event	Data plane DHCP IP pool usage rate is 100 percent
Event Type	dpDhcplpPoolUsageRate100
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%.

Parent topic: [Data Plane Events](#)

## Data plane DHCP IP pool usage rate is 80 percent

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** Data plane DHCP IP pool usage rate is 80 percent event

Event	Data plane DHCP IP pool usage rate is 80 percent
Event Type	dpDhcplpPoolUsageRate80
Event Code	1266
Severity	Warning
Attribute	"dpName"="xxxxxxx", "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%.

Parent topic: [Data Plane Events](#)

## Data plane NAT session capacity usage rate is 80 percent

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** 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%.

Parent topic: [Data Plane Events](#)

## Data plane NAT session capacity usage rate is 100 percent

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** 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

Event	Data plane NAT session capacity usage rate is 100 percent
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%.

Parent topic: [Data Plane Events](#)

## Data plane DHCP IP capacity usage rate is 80 percent

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** Data plane DHCP IP capacity usage rate is 80 percent event

Event	Data plane DHCP IP capacity usage rate is 80 percent
Event Type	dpDhcpIpCapacityUsageRate80
Event Code	1285
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{{dpKey}}] DHCP IP Capacity usage rate is 80 percent. (total [{{totalLicenseCnt}}], consumed [{{consumedLicenseCnt}}], available [{{availableLicenseCnt}}])
Description	This event occurs when the data plane DHCP IP capacity usage rate is 80%.

Parent topic: [Data Plane Events](#)

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

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** 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%.

Parent topic: [Data Plane Events](#)

## Data plane backup success

**Table 1.** Data plane backup success event

Event	Data plane backup success
Event Type	dpBackupSuccess
Event Code	1290
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"

Event	Data plane backup success
Displayed on the web interface	Data Plane [{dpName&&dpKey}] backup successful.
Description	This event occurs when Data plane backup is successful.

Parent topic: [Data Plane Events](#)

## Data plane backup failed

**Table 1.** Data plane backup failed event

Event	Data plane backup failed
Event Type	dpBackupFailed
Event Code	1291
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] backup failed.
Description	This event occurs when Data plane backup fails.

Parent topic: [Data Plane Events](#)

## Data plane restore success

**Table 1.** Data plane restore success event

Event	Data plane restore success
Event Type	dpRestoreSuccess
Event Code	1292

Event	Data plane restore success
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] restore successful.
Description	This event occurs when Data plane restore is successful.

Parent topic: [Data Plane Events](#)

## Data plane restore failed

**Table 1.** Data plane restore failed event

Event	Data plane restore failed
Event Type	dpRestoreFailed
Event Code	1293
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] restore failed.
Description	This event occurs when Data plane restore fails.

Parent topic: [Data Plane Events](#)

## dplpmiPsStatus

**Table 1.** dplpmiPsStatus event

Event	dplpmiPsStatus
Event Type	dplpmiPsStatus
Event Code	2901
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The voltage [{status}] on the data plane [{dpName&&dpKey}].
Description	This event occurs when the voltage status on the data plane is sent.

Parent topic: [Data Plane Events](#)

## dplpmiThempIOH

**Table 1.** dplpmiThempIOH event

Event	dplpmiThempIOH
Event Type	dplpmiThempIOH
Event Code	2904
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	IOH temperature [{status}] on data plane [{dpName&&dpKey}].

Event	dplpmiThempIOH
Description	This event occurs when the IOH temperature status on the data plane is sent..

Parent topic: [Data Plane Events](#)

## dplpmiThempMemP

**Table 1.** dplpmiThempMemP event

Event	dplpmiThempMemP
Event Type	dplpmiThempMemP
Event Code	2905
Severity	Major
Attribute	"dpKey"="xxxxxxx", "id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The processor memory temperature [{status}] on the data plane[{dpName}&&dpKey}]].
Description	This event occurs when the processor memory temperature status on the data plane is sent.

Parent topic: [Data Plane Events](#)

## dplpmiPsStatus

**Table 1.** dplpmiPsStatus event

Event	dplpmiPsStatus
Event Type	dplpmiPsStatus
Event Code	2913

Event	dplpmiPsStatus
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on data plane [{dpName}&&dpKey}].
Description	This event occurs when the power supply status on the data plane is sent.

Parent topic: [Data Plane Events](#)

## dplpmiREVoltage

**Table 1.** dplpmiREVoltage event

Event	dplpmiREVoltage
Event Type	dplpmiREVoltage
Event Code	2926
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The voltage [{status}] on the data plane [{dpName}&&dpKey}]
Description	This event occurs when the baseboard temperature status recover from the abnormal condition.

Parent topic: [Data Plane Events](#)

## dplpmiREThempIOH

**Table 1.** dplpmiREThempIOH event

Event	dplpmiREThempIOH
Event Type	dplpmiREThempIOH
Event Code	2929
Severity	Major
Attribute	"dpKey"="xxxxxxx", "id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	IOH temperature [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the IOH temperature status recover from abnormal condition.

Parent topic: [Data Plane Events](#)

## dplpmiREThempMemP

**Table 1.** dplpmiREThempMemP event

Event	dplpmiREThempMemP
Event Type	dplpmiREThempMemP
Event Code	2930
Severity	Major
Attribute	"dpKey"="xxxxxxx", "id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The processor memory temperature [{status}] on the data plane[{dpName&&dpKey}]].

Event	dplpmiREThempMemP
Description	This event occurs when the processor memory temperature status recover from abnormal condition.

Parent topic: [Data Plane Events](#)

## dplpmiRePsStatus

**Table 1.** dplpmiRePsStatus event

Event	dplpmiRePsStatus
Event Type	dplpmiRePsStatus
Event Code	2938
Severity	Major
Attribute	"dpKey"="xxxxxxx", "id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on data plane [{dpName}&&dpKey]}.
Description	This event occurs when the power supply status recover from abnormal condition.

Parent topic: [Data Plane Events](#)

## dpSSDHealthDegrade

**Table 1.** dpSSDHealthDegrade event

Event	dpSSDHealthDegrade
Event Type	dpSSDHealthDegrade
Event Code	2961

Event	dpSSDHealthDegrade
Severity	Major
Attribute	"dpKey"="xxxxxxx", "id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	The SSD health is degrading on data plane [{{dpName&&dpKey}}]. [{{status}}]
Description	This event occurs when SSD health is degrading.

Parent topic: [Data Plane Events](#)

## Remote Administration Start

**Table 1.** Remote administration event

Event	Remote administration
Event Type	dpremotheadministration
Event Code	99250
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	No web interface for this event.
Description	This event occurs when data plane SSHD starts.

Parent topic: [Data Plane Events](#)

## Remote Administration Stop

**Table 1.** Remote administration event

Event	Remote administration event
Event Type	remoteadministration
Event Code	99251
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	No web interface for this event.
Description	This event occurs when data plane SSHD stops.

Parent topic: [Data Plane Events](#)

## Data plane Switchover Failed

**Table 1.** Data plane Switchover Failed event

Event	Data plane Switchover Failed
Event Type	dpSwitchoverFailed
Event Code	629
Severity	Minor
Attribute	
Displayed on the web interface	
Description	This event occurs when an DP state or settings does not support switchover to another cluster 1 records.

Parent topic: [Data Plane Events](#)

# Data Streaming Event

[Connected to Data a Streaming Endpoint](#)

[Disconnected to Data a Streaming Endpoint](#)

[Connected to Data a Streaming Endpoint Failure](#)

Parent topic: [Events Types](#)

## Connected to Data a Streaming Endpoint

**Table 1.** Connected to Data a Streaming Endpoint event

Event	Connected to Data a Streaming Endpoint
Event Type	connectedtoDataStreamingEndpoint
Event Code	4701
Severity	Informational
Displayed on the web interface	Connect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ connected to data a streaming endpoint.

Parent topic: [Data Streaming Event](#)

## Disconnected to Data a Streaming Endpoint

**Table 1.** Disconnected to Data a Streaming Endpoint event

Event	Disconnected to Data a Streaming Endpoint
Event Type	disconnectedtoDataStreamingEndpoint
Event Code	4702
Severity	Warning

Event	Disconnected to Data a Streaming Endpoint
Displayed on the web interface	Disconnect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ disconnected to data a streaming endpoint.

Parent topic: [Data Streaming Event](#)


## Connected to Data a Streaming Endpoint Failure

**Table 1.** Connected to Data a Streaming Endpoint Failure event

Event	Connected to Data a Streaming Endpoint Failure
Event Type	connectingFailure
Event Code	4703
Severity	Critical
Displayed on the web interface	name="xxxxx", connectorType="SCI", "ip"="2.2.2.2", "port"="8883"
Description	This event occurs when SZ try to connect to a data streaming profile but failure.

Parent topic: [Data Streaming Event](#)

## 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](#)
- [DHCP dcln received](#)

Parent topic: [Events Types](#)

## DHCP inform received

**Table 1.** DHCP inform received event

Event	DHCP inform received
Event Type	dhcplnfmRcvd
Event Code	1238
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.

Parent topic: [DHCP Events](#)

## DHCP dcln received


**Table 1.** 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"

Event	DHCP dcln received
	<pre>"srcProcess"="aut", "realm"="NA" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "SCGMgmtIp"="2.2.2.2"</pre>
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.

Parent topic: [DHCP Events](#)

## GA Interface Events

 **Note:** This section is not applicable for vSZ-H.

Following are the events related to the GA interface (CDRs and GTP').

- [CGF keepalive not responded](#)
- [CDR transfer succeeded](#)

Parent topic: [Events Types](#)

## Connection to CGF failed

**Table 1.** Connection to CGF failed event

Event	Connection to CGF failed
Event Type	cnxnToCgfFailed
Event Code	1610
Severity	Major

Event	Connection to CGF failed
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA", "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Connection with CGF [{cgfSrvrIp}] from RADServerIP [{radSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when channel interface processor (CIP) or GPRS tunneling protocol prime (GTPP) stack detects a connection loss to the charging gateway function (CGF server).
Auto Clearance	This event triggers the alarm 1610, which is auto cleared by the event code 1613.

Parent topic: [GA Interface Events](#)

## CGF keepalive not responded

**Table 1.** CGF keepalive not responded event

Event	CGF keepalive not responded
Event Type	cgfKeepAliveNotResponded
Event Code	1612
Severity	Informational
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA", "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Heartbeat missed between RAD Server [{radSrvrIp}] and CGF Server [{cgfSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]

Event	CGF keepalive not responded
Description	This event occurs when channel interface processor does not receive an acknowledgment for a keep alive request.

Parent topic: [GA Interface Events](#)

## CDR transfer succeeded

**Table 1.** CDR transfer succeeded event

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

Parent topic: [GA Interface Events](#)

## CDR generation failed

**Table 1.** CDR generation failed event

Event	CDR generation failed
Event Type	cdrGenerationFailed
Event Code	1615
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="wlan.3gppnetwork.org" "radSrvrIp"="7.7.7.7" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Failed to generate CDR by RAD Server [{radSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the controller cannot format/ generate the call detail records.

Parent topic: [GA Interface Events](#)

## CDR transfer failed


**Table 1.** CDR transfer failed event

Event	CDR transfer failed
Event Type	cdrTxfrFailed
Event Code	1614
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40"

Event	CDR transfer failed
	"SCGMgmtIp"="2.2.2.2" "cause"="<reason for failure>"
Displayed on the web interface	CDR Transfer failed from RAD Server [{radSrvrIp}] to CGF [{cgfSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the call detail record transfers fails.

Parent topic: [GA Interface Events](#)

## 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	GGSN not reachable	Echo response not received
GGSN not resolved	PDP context established	PDP create failed
PDP update by HLR succeeded	PDP update by HLR failed	PDP update by roaming succeeded
PDP update by roaming failed	PDP update by GGSN succeeded	PDP update by GGSN failed
PDP delete by TTG succeeded	PDP delete by TTG failed	PDP delete by GGSN succeeded
PDP delete by GGSN failed	IP assigned	IP not assigned
Unknown UE	PDP update success COA	PDP update fail COA
PDNGW could not be resolved	PDNGW version not supported	Associated PDNGW down

Event	Event	Event
Create session response failed	Decode failed	Modify bearer response failed
Delete session response failed	Delete bearer request failed	Update bearer request failed
CGF server not configured		

Parent topic: [Events Types](#)

## GGSN restarted

**Table 1.** 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.

Parent topic: [Gn/S2a Interface Events](#)

## GGSN not reachable

**Table 1.** GGSN not reachable event

Event	GGSN not reachable
Event Type	ggsnNotReachable
Event Code	1211
Severity	Major
Attribute	"mvnold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm", "realm"="NA", "gtpclp"="5.5.5.5", "ggsnlp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{ggsnlp}] connected to {produce.short.name} (GTPC-IP [{gtpclp}]) is not reachable
Description	This event occurs when echo request is timed out.

Parent topic: [Gn/S2a Interface Events](#)

## Echo response not received

**Table 1.** Echo response not received event

Event	Echo response not received
Event Type	echoRspNotRcvd
Event Code	1212
Severity	Informational
Attribute	"mvnold"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm" "realm"="NA" "gtpclp"="5.5.5.5", "ggsnlp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"

Event	Echo response not received
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.

Parent topic: [Gn/S2a Interface Events](#)

## GGSN not resolved

**Table 1.** 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" "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 even occurs when access point name is unable to resolve to gateway GPRS support node.

Parent topic: [Gn/S2a Interface Events](#)

## PDP context established

**Table 1.** PDP context established event

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

Parent topic: [Gn/S2a Interface Events](#)

## PDP create failed

**Table 1.** PDP create failed event

Event	PDP create failed
Event Type	crtPdpFailed
Event Code	1217
Severity	Debug

Event	PDP create failed
Attribute	<pre>"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" "cause"="cause of error"</pre>
Displayed on the web interface	PDP context create failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Cause [{cause}]
Description	This event occurs when create packet data protocol fails.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update by HLR succeeded

**Table 1.** PDP update by HLR succeeded event

Event	PDP update by HLR succeeded
Event Type	initPdpUpdSucHlr
Event Code	1218
Severity	Debug
Attribute	<pre>"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" "hlrEvent"="&lt;event received from HLR&gt;"</pre>

Event	PDP update by HLR succeeded
Displayed on the web interface	PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because of [hlrEvent] 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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update by HLR failed

**Table 1.** PDP update by HLR failed event

Event	PDP update by HLR failed
Event Type	initPdpUpdFailureHlr
Event Code	1219
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" "hlrEvent"="<event received from HLR>"
Displayed on the web interface	PDP context update initiated because of HLR Event [{hlrEvent}] failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Failure Cause [{cause}]

Event	PDP update by HLR failed
Description	This event occurs when update packet data protocol fails. Update is initiated by TTG control plane as a result of HLR initiation.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update by roaming succeeded

**Table 1.** PDP update by roaming succeeded event

Event	PDP update by roaming succeeded
Event Type	initPdpUpdSuccRoam
Event Code	1220
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	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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update by roaming failed

**Table 1.** 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" "gtppclp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImei"="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 [{ueImei}] 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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update by GGSN succeeded

**Table 1.** PDP update by GGSN succeeded event

Event	PDP update by GGSN succeeded
Event Type	recvPdpUpdSuccGgsn
Event Code	1222

Event	PDP update by GGSN succeeded
Severity	Debug
Attribute	<pre>"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"</pre>
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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update by GGSN failed

**Table 1.** PDP update by GGSN failed event

Event	PDP update by GGSN failed
Event Type	recvPdpUpdFailureGgsn
Event Code	1223
Severity	Debug
Attribute	<pre>"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"</pre>

Event	PDP update by GGSN failed
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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP delete by TTG succeeded

**Table 1.** PDP delete by TTG succeeded event

Event	PDP delete by TTG succeeded
Event Type	initPdpDelSucc
Event Code	1224
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	{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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP delete by TTG failed

**Table 1.** PDP delete by TTG failed event

Event	PDP delete by TTG failed
Event Type	initPdpDelFailure
Event Code	1225
Severity	Debug
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" "ueImei"="12345", "ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	{produce.short.name} initiated; PDP context delete failed for UE with IMSI [{ueImei}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Cause [{cause}]
Description	This event occurs when packet data protocol delete fails.

Parent topic: [Gn/S2a Interface Events](#)

## PDP delete by GGSN succeeded

**Table 1.** PDP delete by GGSN succeeded event

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

Event	PDP delete by GGSN succeeded
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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP delete by GGSN failed

**Table 1.** 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}].

Event	PDP delete by GGSN failed
Description	This event occurs when delete packet data protocol fails. Delete is initiated by GGSN.

Parent topic: [Gn/S2a Interface Events](#)

## IP assigned

**Table 1.** 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.

Parent topic: [Gn/S2a Interface Events](#)

## IP not assigned

**Table 1.** IP not assigned event

Event	IP not assigned
Event Type	ipNotAssigned
Event Code	1230
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" "ueImei"="12345", "ueMsisdn"="98787" "cause"="<why IP could not be assigned>"
Displayed on the web interface	IP could not be assigned to UE with IMSI [{ueImei}] 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.

Parent topic: [Gn/S2a Interface Events](#)

## Unknown UE

**Table 1.** Unknown UE event

Event	Unknown UE
Event Type	unknownUE
Event Code	1231
Severity	Minor

Event	Unknown UE
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.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update success COA

**Table 1.** PDP update success COA event

Event	PDP update success COA
Event Type	pdpUpdSuccCOA
Event Code	1244
Severity	Debug
Attribute	"mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtcpIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "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}

Event	PDP update success COA
	{{SCGMgmtIp}} because of COA from AAA server [{{aaaSrvrIp}}]
Description	This event occurs when the packet data protocol update is successful when initiating the update process based on the change of authorization received from the external AAA server.

Parent topic: [Gn/S2a Interface Events](#)

## PDP update fail COA

**Table 1.** PDP update fail COA event

Event	PDP update fail COA
Event Type	pdpUpdFailCOA
Event Code	1245
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" "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 [{{ueImsi}}] 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

Event	PDP update fail COA
	on the change of authorization received from the external AAA server.

Parent topic: [Gn/S2a Interface Events](#)

## PDNGW could not be resolved

**Table 1.** 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.

Parent topic: [Gn/S2a Interface Events](#)

## PDNGW version not supported

**Table 1.** PDNGW version not supported event

Event	PDNGW version not supported
Event Type	pdnGwVersionNotSupportedMsgReceived
Event Code	1952
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii""ueImsi"="12345","u eMsisdn"="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.

Parent topic: [Gn/S2a Interface Events](#)

## Associated PDNGW down

**Table 1.** Associated PDNGW down event

Event	Associated PDNGW down
Event Type	pdnGwAssociationDown
Event Code	1953
Severity	Critical

Event	Associated PDNGW down
Attribute	<pre>"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"</pre>
Displayed on the web interface	<pre>{{srcProcess}} Association with PDN GW with IP {{pgwIp}} from {produce.short.name} {{SCGMgmtIp}} down</pre>
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.

Parent topic: [Gn/S2a Interface Events](#)

## Create session response failed

**Table 1.** Create session response failed event

Event	Create session response failed
Event Type	createSessionResponseFailed
Event Code	1954
Severity	Major
Attribute	<pre>"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"</pre>

Event	Create session response failed
Displayed on the web interface	[[srcProcess]] Create Session response from PDN GW with IP [[pgwIp]] on {produce.short.name} [[SCGMgmtIp]] failed, for UE with username [[ueImsi]]@{realm} because [[cause]]
Description	This event occurs when create session response from PDN GW fails with a cause.

Parent topic: [Gn/S2a Interface Events](#)

## Decode failed

**Table 1.** Decode failed event

Event	Decode failed
Event Type	decodeFailed
Event Code	1955
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "APN"="ruckus.com", "pgwIp"="1.1.1.1"
Displayed on the web interface	[[srcProcess]] Decode of message received from PDN GW with IP [[pgwIp]] on {produce.short.name} [[SCGMgmtIp]] failed
Description	This event occurs when decoding of messages received from PDN GW fails.

Parent topic: [Gn/S2a Interface Events](#)

## Modify bearer response failed

**Table 1.** Modify bearer response failed event

Event	Modify bearer response failed
Event Type	modifyBearerResponseFailed
Event Code	1956
Severity	Major
Attribute	mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787", "APN"="ruckus.com" "cause"="xx","pgwIp"="1.1.1.1"
Displayed on the web interface	[{srcProcess}] Modify Bearer Response from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	This event occurs when modify bearer response from PDN GW fails with a cause.

Parent topic: [Gn/S2a Interface Events](#)

## Delete session response failed

**Table 1.** Delete session response failed event

Event	Delete session response failed
Event Type	deleteSessionResponseFailed
Event Code	1957
Severity	Major

Event	Delete session response failed
Attribute	mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com" "cause"="xx","pgwIp"="1.1.1.1"
Displayed on the web interface	[[srcProcess]] Delete Session response from PDN GW with IP [[pgwIp]] on {produce.short.name} [[SCGMgmtIp]] failed, for UE with username [[ueImsi]]@{realm} because [[cause]]
Description	This event occurs when the delete session response from PDN GW fails.

Parent topic: [Gn/S2a Interface Events](#)

## Delete bearer request failed

**Table 1.** Delete bearer request failed event

Event	Delete bearer request failed
Event Type	deleteBearerRequestFailed
Event Code	1958
Severity	Major
Attribute	mvnold="12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com", "cause"="<reason for failure>","pgwIp"="1.1.1.1"
Displayed on the web interface	[[srcProcess]] Delete Bearer Request from PDN GW with IP [[pgwIp]] on {produce.short.name}

Event	Delete bearer request failed
	[[SCGMgmtIp]] failed, for UE with username [[ueImsi]]@[[realm]] because [[cause]]
Description	This event occurs when the delete bearer request from PDN GW fails with decode error.

Parent topic: [Gn/S2a Interface Events](#)

## Update bearer request failed

**Table 1.** 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" "ueImsi"="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 [[ueImsi]]@[[realm]] because [[cause]]
Description	This event occurs when the update bearer request fails with a decode error.

Parent topic: [Gn/S2a Interface Events](#)


## CGF server not configured

**Table 1.** CGF server not configured event

Event	CGF server not configured
Event Type	cgfServerNotConfigured
Event Code	1960
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="CIP" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "uelmsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com" "cgfSrvrIp" = "1.1.1.1", "ggsnIp"="10.10.10.10"
Displayed on the web interface	CGF server IP [{cgfSrvrIp}] received from PDN GW/ GGSN with IP [{ggsnIp}] on {produce.short.name} [{SCGMgmtIp}] is not configured
Description	This event occurs when the IP address of the charging gateway function server received from GGSN/PDNGW is not configured in the controller web interface.

Parent topic: [Gn/S2a Interface Events](#)

## Gr Interface Event

 **Note:** This section is not applicable for vSZ-H.

Following are the events related to GR interface.

- [Destination not reachable](#)
- [Destination available](#)
- [App server down](#)
- [App server inactive](#)

- [App server active](#)
- [Association establishment failed](#)
- [Association down](#)
- [Association up](#)
- [Send auth info success](#)
- [Auth info sending failed](#)
- [GPRS location update succeeded](#)
- [GPRS location update failed](#)
- [Insert sub data success](#)
- [Insert sub data failed](#)
- [Outbound routing failure](#)
- [Did allocation failure](#)
- [Restore data success](#)
- [Restore data failed](#)

Parent topic: [Events Types](#)

## Destination not reachable

**Table 1.** 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"

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.

Parent topic: [Gr Interface Event](#)

## Destination available

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## App server down

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## App server inactive

**Table 1.** App server inactive event

Event	App server inactive
Event Type	appServerInactive
Event Code	1624
Severity	Critical

Event	App server inactive
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.

Parent topic: [Gr Interface Event](#)

## App server active

**Table 1.** 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}}]

Event	App server active
Description	This event occurs when the local application server is active from the remote IPSP or signalling gateway (SG).

Parent topic: [Gr Interface Event](#)

## Association establishment failed

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## Association down

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## Association up

**Table 1.** Association up event

Event	Association up
Event Type	assocUp
Event Code	1628
Severity	Critical

Event	Association up
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.

Parent topic: [Gr Interface Event](#)

## Send auth info success

**Table 1.** Send auth info success event

Event	Send auth info success
Event Type	sendAuthInfoSuccess
Event Code	1630
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918"
Displayed on the web interface	MAP-SendAuthInfo Operation successful from IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when authentication parameters are successfully retrieved.

Parent topic: [Gr Interface Event](#)

## Auth info sending failed

**Table 1.** Auth info sending failed event

Event	Auth info sending failed
Event Type	sendAuthInfoFailed
Event Code	1631
Severity	Major
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-SendAuthInfo Operation Failed for IMSI [{{ueImsi}}] with [{{hlrInstance}}], cause [{{cause}}]
Description	This event occurs when it fails to retrieve the authentication parameters.

Parent topic: [Gr Interface Event](#)

## GPRS location update succeeded

**Table 1.** GPRS location update succeeded event

Event	GPRS location update succeeded
Event Type	updateGprsLocSuccess
Event Code	1632
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918"

Event	GPRS location update succeeded
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.

Parent topic: [Gr Interface Event](#)

## GPRS location update failed

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## Insert sub data success

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## Insert sub data failed

**Table 1.** 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"

Event	Insert sub data failed
Displayed on the web interface	MAP-InsertSubscriberData Operation Failed for IMSI [{ueImsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to insert the subscriber data operation

Parent topic: [Gr Interface Event](#)

## Outbound routing failure

**Table 1.** 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" "ueImsi"="04844624203918"
Displayed on the web interface	Unable to route [{operation}] for IMSI [{ueImsi}] to HLR [{hlrInstance}]
Description	This event occurs when it is unable to route transaction capabilities application (TCAP) message to the destination.

Parent topic: [Gr Interface Event](#)

## Did allocation failure

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## Restore data success

**Table 1.** 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}}]

Event	Restore data success
Description	This event occurs when it successfully restores the data operation.

Parent topic: [Gr Interface Event](#)


## Restore data failed

**Table 1.** 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.

Parent topic: [Gr Interface Event](#)

## IPMI Events


 **Note:** This section is not applicable for vSZ-H.

Following are the events related to IPMIs:

Event	Event	Event
ipmiVoltage	ipmiThempBB	ipmiThempFP
ipmiThempIOH	ipmiThempMemP	ipmiThempPS
ipmiThempP	ipmiThempHSBP	ipmiFan
ipmiPower	ipmiCurrent	ipmiFanStatus
ipmiPsStatus	ipmiDrvStatus	ipmiREVotage
ipmiREThempBB	ipmiREThempFP	ipmiREThempIOH
ipmiREThempMemP	ipmiREThempPS	ipmiREThempP
ipmiREThempHSBP	ipmiREFan	ipmiREPower
ipmiRECurrent	ipmiREFanStatus	ipmiREPsStatus
ipmiREDrvStatus		

Parent topic: [Events Types](#)

## ipmiVoltage

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** ipmiVoltage event

Event	ipmiVoltage
Event Type	ipmiVoltage
Event Code	901
Severity	Major

Event	ipmiVoltage
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 <sup>0</sup> C  Non critical high - 61 <sup>0</sup> C  Non critical low - 10 <sup>0</sup> C  Critical low - 5 <sup>0</sup> C
Auto Clearance	This event triggers the alarm 901, which is auto cleared by the event code 926.

Parent topic: [IPMI Events](#)

## ipmiThempBB

**Table 1.** ipmiThempBB event

Event	ipmiThempBB
Event Type	ipmiThempBB
Event Code	902
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}]

Event	ipmiThempBB
Description	This event occurs when the baseboard temperature status is sent. Baseboard threshold temperatures are in the range of 10 <sup>0</sup> Celsius to 61 <sup>0</sup> Celsius. The default threshold is 61 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 902, which is auto cleared by the event code 927.

Parent topic: [IPMI Events](#)


## ipmiThempFP

**Table 1.** 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 <sup>0</sup> Celsius to 44 <sup>0</sup> Celsius. The default threshold is 44 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 903, which is auto cleared by the event code 928.

Parent topic: [IPMI Events](#)

# ipmiThempIOH


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 904, which is auto cleared by the event code 929.

Parent topic: [IPMI Events](#)

# ipmiThempMemP


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 905, which is auto cleared by the event code 930.

Parent topic: [IPMI Events](#)

## ipmiThempPS

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** ipmiThempPS event

Event	ipmiThempPS
Event Type	ipmiThempPS
Event Code	906
Severity	Major

Event	ipmiThempPS
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 <sup>0</sup> Celsius to 5 <sup>0</sup> Celsius. The default threshold is 5 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 906, which is auto cleared by the event code 931.

Parent topic: [IPMI Events](#)

## ipmiThempP

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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}]

Event	ipmiThempP
Description	This event is triggered when the threshold value is in the range of 1 <sup>0</sup> to 11 <sup>0</sup> Celsius. The default threshold is 11 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 907, which is auto cleared by the event code 932.

Parent topic: [IPMI Events](#)

## ipmiThempHSBP

**Table 1.** 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 <sup>0</sup> Celsius to 55 <sup>0</sup> Celsius. The default threshold is 55 <sup>0</sup> C.
Auto Clearance	This event triggers the alarm 908, which is auto cleared by the event code 933.

Parent topic: [IPMI Events](#)


## ipmiFan

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiPower

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** ipmiPower event

Event	ipmiPower
Event Type	ipmiPower
Event Code	910
Severity	Major

Event	ipmiPower
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.

Parent topic: [IPMI Events](#)

## ipmiCurrent

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Event	ipmiCurrent
Auto Clearance	This event triggers the alarm 911, which is auto cleared by the event code 936.

Parent topic: [IPMI Events](#)


## ipmiFanStatus

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiPsStatus


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiDrvStatus

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** ipmiDrvStatus event

Event	ipmiDrvStatus
Event Type	ipmiDrvStatus
Event Code	914
Severity	Major

Event	ipmiDrvStatus
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.

Parent topic: [IPMI Events](#)

## ipmiREVotage

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREThempBB

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREThempFP

**Table 1.** 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}].

Event	ipmiREThempFP
Description	This event occurs when the front panel temperature comes back to the normal status.

Parent topic: [IPMI Events](#)

# ipmiREThempIOH



 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

Table 1. 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.

Parent topic: [IPMI Events](#)

# ipmiREThempMemP


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREThempPS

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** ipmiREThempPS event

Event	ipmiREThempPS
Event Type	ipmiREThempPS
Event Code	931
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"

Event	ipmiREThempPS
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.

Parent topic: [IPMI Events](#)

## ipmiREThempP


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREThempHSBP

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREFan

**Table 1.** ipmiREFan event

Event	ipmiREFan
Event Type	ipmiREFan
Event Code	934
Severity	Informational
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}].

Event	ipmiREFan
Description	This event occurs when the system fan module comes back to the normal status.

Parent topic: [IPMI Events](#)

## ipmiREPower



 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

Table 1. 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.

Parent topic: [IPMI Events](#)

## ipmiRECurrent

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREFanStatus


**Table 1.** 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}].

Event	ipmiREFanStatus
Description	This event occurs when the fan module comes back to the normal status.

Parent topic: [IPMI Events](#)

## ipmiREPsStatus


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## ipmiREDrvStatus

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [IPMI Events](#)

## Licensing Interface Events


Following are the events related to licensing:

- [TTG session warning threshold](#)
- [TTG session major threshold](#)
- [TTG session critical threshold](#)
- [TTG session license exhausted](#)
- [License sync succeeded](#)
- [License sync failed](#)
- [License import succeeded](#)
- [License import failed](#)
- [License data changed](#)

- License going to expire
- Insufficient license capacity
- Data plane DHCP IP license insufficient
- Data plane NAT session license insufficient
- AP number limit exceeded
- Insufficient license capacity
- Insufficient license capacity

Parent topic: [Events Types](#)

## TTG session warning threshold


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)

## TTG session major threshold


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)

## TTG session critical threshold

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** TTG session critical threshold event

Event	TTG session critical threshold
Event Type	ttgSessionCriticalThreshold
Event Code	1242

Event	TTG session critical threshold
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut/lic"
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached critical level.
Description	This event occurs when the number of user equipment attached to the system has reached the critical threshold limit.

Parent topic: [Licensing Interface Events](#)

## TTG session license exhausted

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Event	TTG session license exhausted
Description	This event occurs when the number of user equipment attached to the system has exceeded the license limit.

Parent topic: [Licensing Interface Events](#)

## License sync succeeded

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)

## License sync failed

**Table 1.** License sync failed event

Event	License sync failed
Event Type	licenseSyncFail

Event	License sync failed
Event Code	1251
Severity	Warning
Attribute	"nodeName"="xxxxxxx", "licenseServerName"="ruckuswireless.flexeraoperation.com"
Displayed on the web interface	Node [{nodeName}] sync-up license with license server [{licenseServerName}] failed.
Description	This event occurs when the controller fails to synchronize the license data with the license server.

Parent topic: [Licensing Interface Events](#)

## License import succeeded

**Table 1.** 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

Parent topic: [Licensing Interface Events](#)

## License import failed

**Table 1.** 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

Parent topic: [Licensing Interface Events](#)

## License data changed

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)

## License going to expire

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)

## Insufficient license capacity

**Table 1.** 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.

Event	Insufficient license capacity
Description	This event occurs when connected APs are rejected due to insufficient licenses.

Parent topic: [Licensing Interface Events](#)

## Data plane DHCP IP license insufficient

### Note:

This event is not applicable for SZ300/SZ100.

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)

## Data plane NAT session license insufficient

 **Note:**

This event is not applicable for SZ300/SZ100.

**Table 1.** 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 <code>{{totalLicenseCnt}}</code> , consumed <code>{{consumedLicenseCnt}}</code> , available <code>{{availableLicenseCnt}}</code> )
Description	This event occurs when the data plane NAT session license is insufficient.

Parent topic: [Licensing Interface Events](#)

## AP number limit exceeded

**Table 1.** AP number limit exceeded event

Event	AP number limit exceeded
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1280

Event	AP number limit exceeded
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.

Parent topic: [Licensing Interface Events](#)

## Insufficient license capacity

**Table 1.** 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.

Parent topic: [Licensing Interface Events](#)


## Insufficient license capacity

**Table 1.** Insufficient license capacity event

Event	Insufficient license capacity
Event Type	switchConnectionTerminatedDueToInsufficientLicense
Event Code	1289
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing switch connections to terminate.
Description	This event occurs when some connected switches were rejected due to insufficient license capacity.

Parent topic: [Licensing Interface Events](#)

## Location Delivery Events

 **Note:** This section is not applicable for vSZ-H.

Following are the events related to location delivery.

- [Unavailable location info requested](#)
- [Incapable location info requested](#)
- [Unsupported location delivery request](#)

Parent topic: [Events Types](#)

## Unavailable location info requested

**Table 1.** 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.

Parent topic: [Location Delivery Events](#)

## Incapable location info requested

**Table 1.** Incapable location info requested event

Event	Incapable location info requested
Event Type	incapableLocInfoRequested
Event Code	1656
Severity	Debug

Event	Incapable location info requested
Attribute	<p>"mvnold"=12, "wlanId"=1, "zoneId"="10",  "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius"</p> <p>"realm"="operator realm", "radSrvrIp"="1.1.1.1",  "requestedInfo"="target location geo location, etc",  "SCGMgmtIp"="2.2.2.2"</p>
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.

Parent topic: [Location Delivery Events](#)

## Unsupported location delivery request


**Table 1.** Unsupported location delivery request event

Event	Unsupported location delivery request
Event Type	unSupportedLocDeliveryRequest
Event Code	1657
Severity	Debug
Attribute	<p>"mvnold"=12, "wlanId"=1,  "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff",  "srcProcess"="radius"</p> <p>"realm"="operator realm", "radSrvrIp"="1.1.1.1"</p> <p>"requestedMethod"="out of band initial request, etc"  "SCGMgmtIp"="2.2.2.2"</p>

Event	Unsupported location delivery request
Displayed on the web interface	AAA [{radSrvrIp}] requests [{requestedInfo}] that is not supported by {produce.short.name} [{SCGMgmtIp}].
Description	This event occurs when the AAA server requests for a delivery method that is not supported by the controller.

Parent topic: [Location Delivery Events](#)

## PMIPv6 Events

 **Note:** This section is not applicable for vSZ-H.

Following are the events related to PMIPv6.

- [Config update failed](#)
- [LMA ICMP reachable](#)
- [LMA server unreachable](#)
- [DHCP connected](#)
- [DHCP connection lost](#)

Parent topic: [Events Types](#)

## Config update failed

**Table 1.** Config update failed event

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

Event	Config update failed
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.

Parent topic: [PMIPv6 Events](#)

## LMA ICMP reachable

**Table 1.** 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.

Parent topic: [PMIPv6 Events](#)

## LMA server unreachable

**Table 1.** LMA server unreachable event

Event	LMA server unreachable
Event Type	lmaHbUnreachable
Event Code	5007
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2.2","lmaIp"="1.1.1.1"
Displayed on the web interface	[[lmaIp]] fail have been detected on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 daemon detects either restart or failure of the LMA server.

Parent topic: [PMIPv6 Events](#)

## DHCP connected

**Table 1.** 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}]

Event	DHCP connected
Description	This event occurs when the PMIPv6 completes the configuration procedure successfully.

Parent topic: [PMIPv6 Events](#)

## DHCP connection lost

**Table 1.** DHCP connection lost event

Event	DHCP connection lost
Event Type	lostCnxnToDHCP
Event Code	5102
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","SCGMgmtIp"="2.2.2"
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.

Parent topic: [PMIPv6 Events](#)

## Session Events


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

- [Session timeout](#)
- [Delete all sessions](#)

- [Binding succeeded](#)
- [Binding failed](#)
- [Binding time expired](#)
- [Binding revoked](#)
- [Binding released](#)

Parent topic: [Events Types](#)

## Session timeout

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Session timeout event

Event	Session timeout
Event Type	sessTimeout
Event Code	1235
Severity	Debug
Attribute	"mvnold"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "cause"="Session Timeout" "SCGMgmtIp"="2.2.2.2" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	Session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] got deleted due to Session Timeout on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when a session is deleted due to a timeout specified by the AAA server.

Parent topic: [Session Events](#)


## Delete all sessions

**Table 1.** Delete all sessions event

Event	Delete all sessions
Event Type	delAllSess
Event Code	1237
Severity	Minor
Attribute	"mvnold"="NA" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "cause"="Admin Delete" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	All sessions got terminated on {produce.short.name} [{{SCGMgmtIp}}] due to [{{cause}}]
Description	This event occurs when all sessions are deleted based on the indicators received from the controller web interface or CLI.

Parent topic: [Session Events](#)

## Binding succeeded

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** Binding succeeded event

Event	Binding succeeded
Event Type	bindingSuccess
Event Code	5009
Severity	Debug

Event	Binding succeeded
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.

Parent topic: [Session Events](#)

## Binding failed

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** 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]].

Event	Binding failed
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.

Parent topic: [Session Events](#)

## Binding time expired


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Binding time expired event

Event	Binding time expired
Event Type	bindingExpired
Event Code	5011
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2" "lmalp"="1.1.1.1", "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "uelpAddr"="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.

Parent topic: [Session Events](#)

## Binding revoked


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Binding revoked event

Event	Binding revoked
Event Type	bindingRevoked
Event Code	5012
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmalp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "uelpAddr"="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.

Parent topic: [Session Events](#)

## Binding released

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** 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" "lmalp"="1.1.1.1"

Event	Binding released
	"ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "uelpAddr"="5.5.5.5"
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.

Parent topic: [Session Events](#)

## STA Interface Events

 **Note:** This section is not applicable for vSZ-H.

Following are the events related to STA interface.

- [STA successful authentication](#)
- [STA session termination {produce.short.name} initiated success](#)
- [STA session termination AAA initiated success](#)
- [STA session termination AAA initiated failed](#)
- [STA re-authorization successful](#)

Parent topic: [Events Types](#)

## STA successful authentication

**Table 1.** STA successful authentication event

Event	STA successful authentication
Event Type	staSuccessfulAuthentication
Event Code	1550

Event	STA successful authentication
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12, "srcProcess"="STA", "ueImsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvIp"="1.1.1.1"
Displayed on the web interface	[[srcProcess]] Auth of [[ueImsi]]/[[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.

Parent topic: [STA Interface Events](#)

## STA session termination {produce.short.name} initiated success

**Table 1.** STA session termination {produce.short.name} initiated success event

Event	STA session termination {produce.short.name} initiated success
Event Type	staSessionTermSCGInitSuccess
Event Code	1554
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", mvnold"=12,"srcProcess"="STA", "realm"= "wlan.mnc080.mcc405.3gppnetwork.org", "ueImsi"="12345", "ueUsername"="98787", "SCGMgmtIp"="2.2.2.2", "aaaSrvIp"="1.1.1.1"

Event	STA session termination {produce.short.name} initiated success
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.

Parent topic: [STA Interface Events](#)

## STA session termination AAA initiated success

**Table 1.** 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}} sucessful. 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.

Parent topic: [STA Interface Events](#)

## STA session termination AAA initiated failed

**Table 1.** 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.

Parent topic: [STA Interface Events](#)

## STA re-authorization successful

**Table 1.** STA re-authorization successful event

Event	STA re-authorization successful
Event Type	staReAuthSuccess
Event Code	1557
Severity	Informational

Event	STA re-authorization successful
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.

Parent topic: [STA Interface Events](#)

## System Events

Following are the events with the system log severity:

 **Note:** {produce.short.name} refers to controller.

Event	Event	Event
No LS responses	LS authentication failure	{produce.short.name} connected to LS
{produce.short.name} failed to connect to LS	{produce.short.name} received passive request	{produce.short.name} sent controller information report
{produce.short.name} received management request	{produce.short.name} sent AP info by venue report	{produce.short.name} sent associated client report
{produce.short.name} forwarded calibration request to AP	{produce.short.name} forwarded calibration request to AP	{produce.short.name} forwarded footfall request to AP

Event	Event	Event
{produce.short.name} received unrecognized request	Syslog server reachable	Syslog server unreachable
Syslog server switched	System service failure	Generate AP config for plane load rebalance succeeded
Generate AP config for plane load rebalance failed	FTP transfer	FTP transfer error
CSV export FTP transfer	CSV export FTP transfer error	CSV export FTP transfer maximum retry
CSV export disk threshold exceeded	CSV export disk max capacity reached	CSV export disk threshold back to normal
File upload	Email sent successfully	Email sent failed
SMS sent successfully	SMS sent failed	Process restart
Service unavailable	Keepalive failure	Resource unavailable
HIP started	HIP stopped	Standby HIP restarted
HIP cache cleaned	All data planes in the zone affinity profile are disconnected	CALEA UE Matched
Diameter peer transport failure	Diameter CER error	Diameter CER success
Diameter invalid version	Diameter peer add successful	ZD AP migrating
ZD AP migrated	ZD AP rejected	ZD AP migration failed
Database error	Recover cassandra error	Process initiated
PMIPv6 unavailable	Memory allocation failed	Process stopped
SZ login fail	SZ login	SZ logout

Event	Event	Event
Password expiration	Admin account lockout	Admin session expired
Disable inactive admins	Two factor auth failed	Unconfirmed program detection
Admin account lockout after failed attempts	Discontinuous time change	Mesh network connectivity lost

Parent topic: [Events Types](#)

## No LS responses

**Table 1.** 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.

Parent topic: [System Events](#)

## LS authentication failure

**Table 1.** 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.

Parent topic: [System Events](#)

## {produce.short.name} connected to LS

**Table 1.** {produce.short.name} connected to LS event

Event	{produce.short.name} connected to LS
Event Type	scgLBSConnectSuccess
Event Code	723
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] connected to LS: url=[{url}], port=[{port}]

Event	{produce.short.name} connected to LS
Description	This event occurs when the controller successfully connects to the location based service.

Parent topic: [System Events](#)

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

**Table 1.** {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.

Parent topic: [System Events](#)

## {produce.short.name} received passive request

**Table 1.** {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.

Parent topic: [System Events](#)

## {produce.short.name} sent controller information report

**Table 1.** {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"=""

Event	{produce.short.name} sent controller information report
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.

Parent topic: [System Events](#)

## {produce.short.name} received management request

**Table 1.** {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.

Parent topic: [System Events](#)

## {produce.short.name} sent AP info by venue report

**Table 1.** {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.

Parent topic: [System Events](#)

## {produce.short.name} sent query venues report

**Table 1.** {produce.short.name} sent query venues report event

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

Event	{produce.short.name} sent query venues report
Description	This event occurs when the controller sends the query venue report.

Parent topic: [System Events](#)

## {produce.short.name} sent associated client report

**Table 1.** {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.

Parent topic: [System Events](#)

## {produce.short.name} forwarded calibration request to AP

**Table 1.** {produce.short.name} forwarded calibration request to AP event

Event	{produce.short.name} forwarded calibration request to AP
Event Type	scgLBSFwdPassiveCalReq

Event	{produce.short.name} forwarded calibration request to AP
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.

Parent topic: [System Events](#)

## {produce.short.name} forwarded footfall request to AP

**Table 1.** {produce.short.name} forwarded footfall request to AP event

Event	{produce.short.name} forwarded footfall request to AP
Event Type	scgLBSFwdPassiveFFReq
Event Code	733
Severity	Informational
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "SCGMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] forward Passive Footfall Request to [{apName}&&apMac]: venue=

Event	{produce.short.name} forwarded footfall request to AP
	{{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.

Parent topic: [System Events](#)

## {produce.short.name} received unrecognized request

**Table 1.** {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.

Parent topic: [System Events](#)

## Syslog server reachable

**Table 1.** 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.

Parent topic: [System Events](#)

## Syslog server unreachable

**Table 1.** Syslog server unreachable event

Event	Syslog server unreachable
Event Type	syslogServerUnreachable
Event Code	751
Severity	Major
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is unreachable on {produce.short.name}.

Event	Syslog server unreachable
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.

Parent topic: [System Events](#)

## Syslog server switched

**Table 1.** 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.

Parent topic: [System Events](#)

## System service failure

**Table 1.** System service failure event

Event	System service failure
Event Type	systemservicefailure
Event Code	753
Severity	Critical
Attribute	"sysService"="", "hostName"="".
Displayed on the web interface	Service [sysService] on node [hostName] failed and respawning
Description	This event occurs when the service is not available.

Parent topic: [System Events](#)

## Generate AP config for plane load rebalance succeeded

**Table 1.** 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 rebalancing succeeded.

Event	Generate AP config for plane load rebalance succeeded
Description	This event occurs when the user executes the load of data plane for re-balancing and generates a new AP configuration successfully.

Parent topic: [System Events](#)

## Generate AP config for plane load rebalance failed

**Table 1.** Generate AP config for plane load rebalance failed event

Event	Generate AP config for plane load rebalance failed
Event Type	planeLoadingRebalancingFailed
Event Code	771
Severity	Informational
Attribute	
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing failed.
Description	This event occurs when the user executes the load of data plane for re-balancing and generation of a new AP configuration fails.

Parent topic: [System Events](#)

## FTP transfer

**Table 1.** FTP transfer event

Event	FTP transfer
Event Type	ftpTransfer

Event	FTP transfer
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.

Parent topic: [System Events](#)

## FTP transfer error

**Table 1.** 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.

Parent topic: [System Events](#)

## CSV export FTP transfer

**Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.xxx.xxx"
Displayed on the web interface	CSV export file [{filename}] transferred on control plane [{nodeName}-C] to FTP server [{ip}:{portID}]successfully.
Description	This event occurs when the CSV file is successfully sent to a remote server.

Parent topic: [System Events](#)

## CSV export FTP transfer error

**Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** 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.

Event	CSV export FTP transfer error
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.

Parent topic: [System Events](#)

## CSV export FTP transfer maximum retry


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.xxxx.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.

Parent topic: [System Events](#)

## CSV export disk threshold exceeded

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** CSV export disk threshold exceeded event

Event	CSV export disk threshold exceeded
Event Type	csvDiskThreshholdExceeded
Event Code	975

Event	CSV export disk threshold exceeded
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.

Parent topic: [System Events](#)

## CSV export disk max capacity reached


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [System Events](#)

## CSV export disk threshold back to normal

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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:xx", "currentUsedPercent"="xx: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.

Parent topic: [System Events](#)

## File upload

**Table 1.** 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.

Parent topic: [System Events](#)

## Email sent successfully

**Table 1.** Email sent successfully event

Event	Email sent successfully
Event Type	mailSendSuccess
Event Code	981
Severity	Informational
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUID" D"="xxxxx"
Displayed on the web interface	[[srcProcess]] sent email to [[receiver]] successfully.
Description	This event occurs when system sends mail successfully.

Parent topic: [System Events](#)

## Email sent failed

**Table 1.** 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.

Event	Email sent failed
Description	This event occurs when the system fails to send the mail.

Parent topic: [System Events](#)

## SMS sent successfully

**Table 1.** 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", "tenantUID"="xxxxx"
Displayed on the web interface	[[srcProcess]] sent short message to [[receiver]] successfully.
Description	This event occurs when system sends the short message successfully.

Parent topic: [System Events](#)

## SMS sent failed

**Table 1.** SMS sent failed event

Event	SMS sent failed
Event Type	smsSendFailed

Event	SMS sent failed
Event Code	984
Severity	Warning
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "reason"="xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	[[srcProcess]] sent short message to [[receiver]] failed, reason: [[reason]].
Description	This event occurs when system fails to send the short message.

Parent topic: [System Events](#)

## Process restart

**Table 1.** 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]]

Event	Process restart
Description	This event occurs when any process crashes and restarts.

Parent topic: [System Events](#)

## Service unavailable

**Table 1.** 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.

Parent topic: [System Events](#)

## Keepalive failure

**Table 1.** Keepalive failure event

Event	Keepalive failure
Event Type	keepAliveFailure

Event	Keepalive failure
Event Code	1003
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="nc", "realm"="NA",  "processName"="aut", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[[srcProcess]] on {produce.short.name} [[SCGMgmtIp]] restarted [[processName]] process.
Description	This event occurs when the <b>mon/nc</b> restarts the process due to a keep alive failure.

Parent topic: [System Events](#)

## Resource unavailable


**Table 1.** 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]]

Event	Resource unavailable
Description	This event is generated due to unavailability of any other system resource, such as memcached.

Parent topic: [System Events](#)

## HIP started


 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [System Events](#)

## HIP stopped


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** HIP stopped event

Event	HIP stopped
Event Type	hipStopped
Event Code	1015
Severity	Informational
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	[[srcProcess]] process stopped HIP on {produce.short.name} [[SCGMgmtIp]]
Description	This event occurs when HIP is stopped.

Parent topic: [System Events](#)

## Standby HIP restarted

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** 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"

Event	Standby HIP restarted
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.

Parent topic: [System Events](#)

## HIP cache cleaned

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [System Events](#)

## All data planes in the zone affinity profile are disconnected

### Note:

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**Table 1.** 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.

Parent topic: [System Events](#)

## CALEA UE Matched


**Table 1.** CALEA UE Matched event

Event	CALEA UE Matched
Event Type	dpCaleaUeInterimMatched
Event Code	1268
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	CALEA matches client [{clientMac}] on WLAN [{ssid}   authType]} from AP [{apName}&&apMac}]. TxBytes[{txBytes}], RxBytes[{rxBytes]}.

Event	CALEA UE Matched
Description	This event occurs when the data plane CALEA user equipment and client matches.

Parent topic: [System Events](#)

## Diameter peer transport failure


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Diameter peer transport failure event

Event	Diameter peer transport failure
Event Type	diaPeerTransportFailure
Event Code	1403
Severity	Major
Attribute	<pre>"ctrlBladeMac"="aa:bb:cc:dd:ee:ff","mvnold"="839f87c6-d116-497e-afce-aa8157abd30c", "srcProcess"="&lt;Application Name&gt;","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"</pre>
Displayed on the web interface	<pre>[[srcProcess]] Failed to read from peer [[peerName]] Transport Realm [[peerRealmName]] on {produce.short.name} [[SCGMgmtIp]]</pre>
Description	This event occurs when the transport with the peer is down and the stack fails to read the data.

Parent topic: [System Events](#)

## Diameter CER error


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Diameter CER error event

Event	Diameter CER error
Event Type	diaCERError
Event Code	1404
Severity	Critical
Attribute	<pre> "ctrlBladeMac"="aa:bb:cc:dd:ee:ff ","mvnold"="839f87c6-d116-497e-afce- aa8157abd30c", "srcProcess"="&lt;Application Name&gt;","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" </pre>
Displayed on the web interface	<pre> [{{srcProcess}}] Failed to decode CER from Peer [{{peerName}}] Realm [{{peerRealmName}}] on [produce.short.name] [{{SCGMgmtIp}}] </pre>
Description	This event occurs when the diameter stack fails to decode the capabilities exchange request (CER) received from peer.

Parent topic: [System Events](#)

## Diameter CER success

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** Diameter CER success event

Event	Diameter CER success
Event Type	diaCERSuccess
Event Code	1405

Event	Diameter CER success
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.

Parent topic: [System Events](#)

## Diameter invalid version

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** Diameter invalid version event

Event	Diameter invalid version
Event Type	dialInvalidVer
Event Code	1406
Severity	Warning
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"="839f87c6-d116-497e-afce-aa8157abd30c", "src Process"="<Application Name>","realm"="ruckus.com","originHost" =

Event	Diameter invalid version
	"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.

Parent topic: [System Events](#)

## Diameter peer add successful

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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","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" = "Peer addition successful"

Event	Diameter peer add 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.

Parent topic: [System Events](#)

## ZD AP migrating

**Table 1.** ZD AP migrating event

Event	ZD AP migrating
Event Type	zdAPMigrating
Event Code	2001
Severity	Informational
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="ZF7962", "firmware"="3.0.0.0.0"
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.

Parent topic: [System Events](#)

## ZD AP migrated

**Table 1.** 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.

Parent topic: [System Events](#)

## ZD AP rejected

**Table 1.** 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"

Event	ZD AP rejected
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.

Parent topic: [System Events](#)

## ZD AP migration failed

**Table 1.** ZD AP migration failed event

Event	ZD AP migration failed
Event Type	zdAPMigrationFailed
Event Code	2004
Severity	Major
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="ZF7962", "firmware"="3.0.0.0.0"
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is failed to upgrade with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when the Zone Director AP fails to upgrade with the controller AP firmware image.

Parent topic: [System Events](#)


## Database error

**Table 1.** 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.

Parent topic: [System Events](#)

## Recover cassandra error

 **Note:** This event is supported on the SmartZone 300 controllers only. This event is not applicable for vSZ-H.


**Table 1.** Recover cassandra error event

Event	Recover cassandra error
Event Type	recoverCassandraError
Event Code	3011
Severity	Informational
Attribute	"nodeName"="xxx",reason="recovery reason"

Event	Recover cassandra error
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.

Parent topic: [System Events](#)

## Process initiated


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Process initiated event

Event	Process initiated
Event Type	processInit
Event Code	5001
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process got re-started on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when PMIPv6 process crashes and restarts.

Parent topic: [System Events](#)

## PMIPv6 unavailable


 **Note:** This event is not applicable for vSZ-H.

**Table 1.** 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.

Parent topic: [System Events](#)

## Memory allocation failed

 **Note:** This event is not applicable for vSZ-H.


**Table 1.** 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"

Event	Memory allocation failed
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.

Parent topic: [System Events](#)

## Process stopped

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Process stopped event

Event	Process stopped
Event Type	processStop
Event Code	5100
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2",
Displayed on the web interface	PMIPv6 process stop on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the PMIPv6 process stops

Parent topic: [System Events](#)

## SZ Login Fail

**Table 1.** SZ login fail event

Event	SZ login fail
Event Type	szLoginFail
Event Code	8007
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on failed from [{ip}].
Description	Administrator logged on failed SZ.

Parent topic: [System Events](#)

## SZ Login

**Table 1.** SZ login event

Event	SZ login
Event Type	szLogin
Event Code	8008
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on from [{ip}].
Description	Administrator logged on SZ.

Parent topic: [System Events](#)

## SZ Logout

**Table 1.** SZ logout event

Event	SZ logout
Event Type	szLogout
Event Code	8009
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged off from [{ip}].
Description	Administrator logged off SZ.

Parent topic: [System Events](#)

## Password expiration

**Table 1.** 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.

Parent topic: [System Events](#)

## Admin account logout

**Table 1.** Admin account logout event

Event	Admin account logout
Event Type	Admin account logout
Event Code	8011
Severity	Warning
Attribute	User Account Name User IP Address Lock Duration Time
Displayed on the web interface	Administrative account [User Account Name] has been locked out because of repeated login failures from [User IP Address], wait for [Lock Duration Time] minutes to re-login.
Description	This event occurs when the account is locked.

Parent topic: [System Events](#)

## Admin session expired

**Table 1.** Admin session expired event

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

Event	Admin session expired
Displayed on the web interface	Administrative account [{userName}] login session has timed out.
Description	This event occurs when the session is timed out due to inactivity or because of absolute session timeout.

Parent topic: [System Events](#)

## Disable inactive admins

**Table 1.** 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.

Parent topic: [System Events](#)

## Two factor auth failed

**Table 1.** Two factor auth failed event

Event	Two factor auth failed
Event Type	TwoFactorAuthFailed

Event	Two factor auth failed
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.

Parent topic: [System Events](#)

## Unconfirmed program detection

**Table 1.** Unconfirmed program detection event

Event	Unconfirmed program detection
Event Type	Unconfirmed Program Detection
Event Code	1019
Severity	Warning
Attribute	"nodeName"="xxx", "status"="xxxxx"
Displayed on the web interface	Detect unconfirmed program on control plane [{nodeName}]. [{status}]
Description	This event occurs when an unconfirmed program is detected.

Parent topic: [System Events](#)

## Admin account lockout after failed attempts

**Table 1.** Admin account lockout after failed attempts

Event	Admin account lockout after failed attempts
Event Type	Admin account lockout after failed attempts
Event Code	8016
Severity	Warning
Attribute	User account name, User IP address
Displayed on the web interface	Administrative account [User account name] is locked out because of repeated login failure from [User IP Address]
Description	This event occurs when the user account is locked on failed attempts

Parent topic: [System Events](#)

## Discontinuous time change

**Table 1.** Discontinuous time change

Event	Discontinuous time change
Event Type	Discontinuous time change
Event Code	99301
Severity	Warning
Attribute	FromTime, ToTime, NTP Server, SZ IP
Displayed on the web interface	The discontinuous time of the controller is changed from [ Fromtime] to [Totime], server: [NTP Server], IP: [SZ IP]

Event	Discontinuous time change
Description	This event occurs when the discontinuous time of the controller changes to more than a minute

Parent topic: [System Events](#)

## Mesh network connectivity lost

**Table 1.** Mesh network connectivity lost event

Event	Mesh network connectivity lost
Event Type	meshConnectivityFailed
Event Code	9116
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", currIface = "xxxxx", "apName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] Mesh network connectivity lost on [{currIface}]
Description	This event occurs when mesh network connectivity is lost.

Parent topic: [System Events](#)

## Failure of Key Generation

**Table 1.** Failure of Key Generation

Event	Failure of Key Generation
Event Type	keyGenFail
Event Code	99100

Event	Failure of Key Generation
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Failure of Key generation. Reason : [{reason}] failed
Description	This event occurs when Smart Zone key generation is failed.

Parent topic: [System Events](#)

## Failure of IPsec

**Table 1.** Failure of IPsec Event

Event	Failure of IPsec
Event Type	IPSecFailure
Event Code	99101
Severity	Major
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63","reason"="Root CA is expired"
Displayed on the web interface	Failure of IP Sec. Reason : [{reason}] failed
Description	This event occurs when Smart Zone IPsec is failed.

Parent topic: [System Events](#)

## Failure Certificate

**Table 1.** Failure Certificate Event

Event	Failure Certificate
Event Type	FailureCertificate
Event Code	99102
Severity	Major
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63","reason"="Root CA is expired"
Displayed on the web interface	Failure of Certificate Reason : {{reason}} failed
Description	This event occurs when Smart Zone server certificate validation is failed.

Parent topic: [System Events](#)

## IPsec KE is Up

**Table 1.** IPsec IKE is Up Event

Event	IPsec IKE is Up
Event Type	IPSecIKEup
Event Code	99103
Severity	Informational
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63","srcProcess"="strongswan","SCGMgmtIp"="10.206.66.223","reason"="System IPsec IKE is up"
Displayed on the web interface	IPsec IKE is Up. Reason : {{reason}} failed

Event	IPsec IKE is Up
Description	This event occurs when Smart Zone IPsec IKE is up.

Parent topic: [System Events](#)

## IPsec IKE is Down

**Table 1.** IPsec IKE is Down Event

Event	IPsec IKE is Down
Event Type	IPSecIKEDown
Event Code	99104
Severity	Critical
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63", "srcProcess"="strongswan", "SCGMgmtIp"="10.206.66.223", "reason"="System IPsec IKE is terminated"
Displayed on the web interface	IPsec IKE is down. Reason : {{reason}} failed
Description	This event occurs when Smart Zone IPsec IKE is down.

Parent topic: [System Events](#)

## Discontinuous Time Change

**Table 1.** Discontinuous Time Change Event

Event	Discontinuous Time Change
Event Type	DiscontinuousTimeChange
Event Code	99301
Severity	Warning

Event	Discontinuous Time Change
Attribute	Discontinuous Time Change, "before"= , "after"=
Displayed on the web interface	
Description	This event occurs when the time of Smart Zone is changed discontinuously.

Parent topic: [System Events](#)

## szAuthAction

**Table 1.** szAuthAction Event

Event	szAuthAction
Event Type	szAuthAction
Event Code	99105
Severity	Informational
Attribute	"account"="XXX", "authType"="XXX", "resultCode"="XXX", "authInfo"="XXX"
Displayed on the web interface	Account [{account}] [{authType}] authentication [{resultCode}], additional information : [{authInfo}]
Description	This event occurs while authenticating by using user password or public key.

Parent topic: [System Events](#)

## Switch Events

Following are the events related to switch severity:

- [Switch critical message](#)
- [Switch alert message](#)

- Switch warning message
- Switch CPU warning threshold exceed
- Switch CPU major threshold exceed
- Switch CPU critical threshold exceed
- Switch memory warning threshold exceed
- Switch memory major threshold exceed
- Switch memory critical threshold exceed
- Switch custom warning threshold exceed
- Switch custom major threshold exceed
- Switch custom critical threshold exceed
- GetCACert Request
- Certificate signing request
- Accept certificate signing request
- Reject certificate signing request
- Pending certificate signing request
- Over Switch Max Capacity
- Switch Duplicated
- Switch Firmware Upgrade
- The Switch is Offline for 15 Minutes
- Switch Firmware Upgrade Failed
- Switch Configuration Update
- Switch Configuration Update Failed
- Switch Reboot

Parent topic: [Events Types](#)

## Switch critical message

**Table 1.** Switch critical message event

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

Parent topic: [Switch Events](#)

## Switch alert message

**Table 1.** Switch alert message event

Event	Switch alert message
Event Type	SwitchAlertMessage
Event Code	20001
Severity	Major
Description	This event occurs when there is a switch alert message.

Parent topic: [Switch Events](#)

## Switch warning message

**Table 1.** Switch warning message event

Event	Switch warning message
Event Type	SwitchWarningMessage
Event Code	20003
Severity	Warning
Description	This event occurs when there is a switch warning message.

Parent topic: [Switch Events](#)

## Switch CPU warning threshold exceed

**Table 1.** Switch CPU warning threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	warningCpuThresholdExceed
Event Code	22010
Severity	Warning
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (1% - Major Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU warning threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the warning threshold.

Parent topic: [Switch Events](#)

## Switch CPU major threshold exceed

**Table 1.** Switch CPU major threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	majorCpuThresholdExceed
Event Code	22011
Severity	Major
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU major threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the major threshold.

Parent topic: [Switch Events](#)

## Switch CPU critical threshold exceed

**Table 1.** Switch CPU critical threshold exceed event

Event	Switch CPU critical threshold exceed
Event Type	criticalCpuThresholdExceed
Event Code	22012
Severity	Critical
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Major Threshold - 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"

Event	Switch CPU critical threshold exceed
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU critical threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the critical threshold.

Parent topic: [Switch Events](#)

## Switch memory warning threshold exceed

**Table 1.** Switch memory warning threshold exceed event

Event	Switch memory warning threshold exceed
Event Type	warningMemoryThresholdExceed
Event Code	22020
Severity	Warning
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (1% - Major Threshold), switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory warning threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the warning threshold.

Parent topic: [Switch Events](#)

## Switch memory major threshold exceed

**Table 1.** Switch memory major threshold exceed event

Event	Switch memory major threshold exceed
Event Type	majorMemoryThresholdExceed
Event Code	22021
Severity	Major
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the major threshold.

Parent topic: [Switch Events](#)

## Switch memory critical threshold exceed

**Table 1.** Switch memory critical threshold exceed event

Event	Switch memory critical threshold exceed
Event Type	criticalMemoryThresholdExceed
Event Code	22022
Severity	Critical
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Major Threshold - 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"

Event	Switch memory critical threshold exceed
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory critical threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the critical threshold of 100%.

Parent topic: [Switch Events](#)

## Switch custom warning threshold exceed

**Table 1.** Switch custom warning threshold exceed event

Event	Switch custom warning threshold exceed
Event Type	hitWarningSwitchCombinedEvent
Event Code	22030
Severity	Warning
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Warning Event] {userDefinedDescription}
Description	This event occurs when the Switch custom warning event crosses the threshold.

Parent topic: [Switch Events](#)

## Switch custom major threshold exceed

**Table 1.** Switch custom major threshold exceed event

Event	Switch custom major threshold exceed
Event Type	hitMajorSwitchCombinedEvent

Event	Switch custom major threshold exceed
Event Code	22031
Severity	Major
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Major Event] {userDefinedDescription}
Description	This event occurs when the Switch custom major event crosses the threshold.

Parent topic: [Switch Events](#)

## Switch custom critical threshold exceed

**Table 1.** Switch custom critical threshold exceed event

Event	Switch custom critical threshold exceed
Event Type	hitCriticalSwitchCombinedEvent
Event Code	22032
Severity	Critical
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Critical Event] {userDefinedDescription}
Description	This event occurs when the Switch custom critical event crosses the threshold.

Parent topic: [Switch Events](#)

## GetCACert Request

**Table 1.** GetCACert Request event

Event	GetCACert Request
Event Type	getCACertRequest
Event Code	22000
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] GetCACert Request.
Description	This event occurs when there is a SCEP GetCACert Request.

Parent topic: [Switch Events](#)

## Certificate signing request

**Table 1.** Certificate signing request event

Event	Certificate signing request
Event Type	certificateSigningRequest
Event Code	22001
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Certificate Signing Request.
Description	This event occurs when there is a SCEP Certificate Signing Request.

Parent topic: [Switch Events](#)

## Accept certificate signing request

**Table 1.** Accept certificate signing request event

Event	Accept certificate signing request
Event Type	acceptCertificateSigningRequest
Event Code	22002
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Accept Certificate Signing Request.
Description	This event occurs when there is a SCEP Accept Certificate Signing Request.

Parent topic: [Switch Events](#)

## Reject certificate signing request

**Table 1.** Reject certificate signing request event

Event	Reject certificate signing request
Event Type	rejectCertificateSigningRequest
Event Code	22003
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Reject Certificate Signing Request.

Event	Reject certificate signing request
Description	This event occurs when there is a SCEP Reject Certificate Signing Request.

Parent topic: [Switch Events](#)

## Pending certificate signing request

**Table 1.** Pending certificate signing request event

Event	Pending certificate signing request
Event Type	pendingCertificateSigningRequest
Event Code	22004
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Pending Certificate Signing Request.
Description	This event occurs when there is a SCEP Pending Certificate Signing Request.

Parent topic: [Switch Events](#)

## Switch is Offline for 15 Minutes

**Table 1.** Switch is Offline for 15 Minutes event

Event	Switch is Offline for 15 Minutes
Event Type	SwitchOffline+B688
Event Code	21000

Event	Switch is Offline for 15 Minutes
Severity	Warning
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} offline for more than 15 minutes
Description	This event occurs when the switch is offline over 15 minutes

Parent topic: [Switch Events](#)

## Over Switch Max Capacity

**Table 1.** Over Switch Max Capacity event

Event	Over Switch Max Capacity
Event Type	OverSwitchMaxCapacity
Event Code	21001
Severity	Critical
Displayed on the web interface	The volume of switches is over system capacity.
Description	This event occurs when the volumn of switches is over system capacity

Parent topic: [Switch Events](#)

## Switch Duplicated

**Table 1.** Switch Duplicated event

Event	Switch Duplicated
Event Type	SwitchDuplicated
Event Code	21002
Severity	Warning
Attributes	"switchSerialNumber"="x",switchName = "x", "switchMac"="aa:bb:cc:dd:ee:ff", "duplicatedSwitchSerialNumber"="x", "duplicatedSwitchName"="x"
Displayed on the web interface	<p>{{switchSerialNumber}} / {{switchName}}</p> <p>A duplicated switch mac address from ({{duplicatedSwitchSerialNumber}}/ {{duplicatedSwitchName}}) is coming while existing one ({{switchMac}}) is online.</p>
Description	This event occurs when duplicated switches are detected.

Parent topic: [Switch Events](#)

## Switch Firmware Upgrade

**Table 1.** Switch Firmware Upgrade event

Event	Switch Firmware Upgrade
Event Type	SwitchFirmwareUpgrade
Event Code	22041
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"

Event	Switch Firmware Upgrade
Displayed on the web interface	{{switchSerialNumber}} / {{switchName}} Switch firmware upgraded
Description	This event occurs when the switch firmware is upgraded.

Parent topic: [Switch Events](#)

## Switch Firmware Upgrade Failed

**Table 1.** Switch Firmware Upgrade Failed event

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

Parent topic: [Switch Events](#)

## Switch Configuration Update

**Table 1.** Switch Configuration Update event

Event	Switch Configuration Update
Event Type	SwitchConfigurationUpdate

Event	Switch Configuration Update
Event Code	22051
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[[switchSerialNumber] / {switchName}] switch configuration update
Description	This event occurs when the switch configuration is updated.

Parent topic: [Switch Events](#)

## Switch Configuration Update Failed

**Table 1.** Switch Configuration Update Failed event

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

Parent topic: [Switch Events](#)

## Switch Reboot

**Table 1.** Switch Reboot event

Event	Switch Reboot
Event Type	SwitchReboot
Event Code	22061
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[[switchSerialNumber] / {switchName}] offline for more than 15 minutes
Description	This event occurs when the Switch re-booted by the controller.

Parent topic: [Switch Events](#)

## Switch Delete

**Table 1.** Switch Delete Event

Event	Switch Delete
Event Type	switchDeleteByController
Event Code	22071
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch was deleted by the controller.
Description	This event occurs when the switch was deleted by the controller.

Parent topic: [Switch Events](#)

## Switch Disconnected from the Controller

**Table 1.** Switch Disconnected from the Controller Event

Event	Switch Disconnected from the Controller
Event Type	switchDisconnectFromController
Event Code	22081
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch disconnected from the controller.
Description	This event occurs when the switch is disconnected from the controller.

Parent topic: [Switch Events](#)

## Switch is Connected to the Controller

**Table 1.** Switch is Connected to the Controller Event

Event	Switch is Connected to the Controller
Event Type	switchConnectToController
Event Code	22082
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch is connected to the controller.

Event	Switch is Connected to the Controller
Description	This event occurs when the switch is connected to the controller.

Parent topic: [Switch Events](#)

## Switch Discovered by the Controller

**Table 1.** Switch Discovered by the Controller Event

Event	Switch Discovered by the Controller
Event Type	switchDiscoverByController
Event Code	22091
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch discovered by the controller.
Description	This event occurs when the switch is discovered by the controller.

Parent topic: [Switch Events](#)

## scheduleZoneFirmwareUpgrade

**Table 1.** scheduleZoneFirmwareUpgrade event

Event	scheduleZoneFirmwareUpgrade
Event Type	scheduleZoneFirmwareUpgrade
Event Code	195

Event	scheduleZoneFirmwareUpgrade
Severity	Major
Attributes	"failedNumber"="number" "notAvailableNumber"="number" "name"="XXX"
Displayed on the web interface	[{{failedNumber}}] zone(s) upgrade failed and [{{notAvailableNumber}}] zone(s) not available in schedule upgrade task [{{name}}]
Description	This event occurs when the [{{failedNumber}}] zone(s) upgrade failed and [{{notAvailableNumber}}] zone(s) not available in schedule upgrade task [{{name}}]

Parent topic: [Switch Events](#)

## Threshold Events

Following are the events related to threshold system set:

- [CPU threshold exceeded](#)
- [Memory threshold exceeded](#)
- [Disk usage threshold exceeded](#)
- [CPU threshold back to normal](#)
- [Memory threshold back to normal](#)
- [Disk threshold back to normal](#)
- [License threshold exceeded](#)
- [The drop of client count threshold exceeded](#)
- [Rate limit threshold surpassed](#)
- [Rate limit threshold restored](#)
- [Rate limit for TOR surpassed](#)
- [The number of users exceed its limit](#)

- [The number of devices exceeded its limit](#)
- [Over AP maximum capacity](#)
- [Over Device Maximum Capacity](#)
- [Device Capacity Threshold Back to Normal](#)

Parent topic: [Events Types](#)

## CPU threshold exceeded

**Table 1.** 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.

Parent topic: [Threshold Events](#)

## Memory threshold exceeded

**Table 1.** 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.

Parent topic: [Threshold Events](#)

## Disk usage threshold exceeded

**Table 1.** 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"

Event	Disk usage threshold exceeded
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.

Parent topic: [Threshold Events](#)

## CPU threshold back to normal

**Table 1.** 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.

Parent topic: [Threshold Events](#)

## Memory threshold back to normal

**Table 1.** 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.

Parent topic: [Threshold Events](#)

## Disk threshold back to normal

**Table 1.** Disk threshold back to normal event

Event	Disk threshold back to normal
Event Type	diskUsageThresholdBackToNormal
Event Code	955
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk threshold [{perc}%] got back to normal on control plane [{nodeName}-C].

Event	Disk threshold back to normal
Description	This event occurs when the disk usage comes back to normal.

Parent topic: [Threshold Events](#)

## License threshold exceeded

**Table 1.** 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.

Parent topic: [Threshold Events](#)

## The drop of client count threshold exceeded

**Table 1.** The drop of client count threshold exceeded event

Event	The drop of client count threshold exceeded
Event Type	clientCountDropThresholdExceeded
Event Code	956

Event	The drop of client count threshold exceeded
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%.

Parent topic: [Threshold Events](#)

## Rate limit threshold surpassed

**Table 1.** 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" "AAAServerType"="Auth/ Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is surpassed. The threshold limit for this event is dependent on the maximum outstanding request

Event	Rate limit threshold surpassed
	(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.

Parent topic: [Threshold Events](#)

## Rate limit threshold restored

**Table 1.** Rate limit threshold restored event

Event	Rate limit threshold restored
Event Type	rateLimitThresholdRestored
Event Code	1301
Severity	Informational
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" "AAAServerType"="Auth/ Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold restored for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is restored. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total

Event	Rate limit threshold restored
	outstanding requests for this server is lesser or equal to 700.

Parent topic: [Threshold Events](#)

## Rate limit for TOR surpassed

**Table 1.** Rate limit for TOR surpassed event

Event	Rate limit for TOR surpassed
Event Type	rateLimitMORSurpassed
Event Code	1302
Severity	Critical
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" "AAAServerType"="Auth/ Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This event occurs when the rate limit for maximum outstanding requests (MOR) is surpassed. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds 1000.

Event	Rate limit for TOR surpassed
Auto Clearance	This event triggers the alarm1302, which is auto cleared by the event code 1301.

Parent topic: [Threshold Events](#)

## The number of users exceed its limit

**Table 1.** 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.

Parent topic: [Threshold Events](#)

## The number of devices exceeded its limit

**Table 1.** The number of devices exceeded its limit event

Event	The number of devices exceeded its limit
Event Type	tooManyDevices
Event Code	7002

Event	The number of devices exceeded its limit
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.

Parent topic: [Threshold Events](#)

## Over AP maximum capacity

**Table 1.** Over AP maximum capacity event

Event	Over AP maximum capacity
Event Type	apCapacityReached
Event Code	962
Severity	Warning
Attribute	
Displayed on the web interface	The volume of AP is over system capacity.
Description	This event occurs when the volume of AP is over system capacity.

Parent topic: [Threshold Events](#)

## Over Device Maximum Capacity

**Table 1.** Over Device Maximum Capacity event

Event	Over Device Maximum Capacity
Event Type	connectedDeviceMaxCapacityReached
Event Code	963
Severity	Major
Attributes	"deviceType"="xx"
Displayed on the web interface	The volume of {{deviceType}} is over maximum device capacity.
Description	This event is triggered when the volume is over maximum device capacity.

Parent topic: [Threshold Events](#)

## Device Capacity Threshold Back to Normal

**Table 1.** Device Capacity Threshold Back to Normal event


Event	Device Capacity Threshold Back to Normal
Event Type	connectedDeviceThresholdBackToNormal
Event Code	964
Severity	Informational
Displayed on the web interface	The device capacity threshold back to normal
Description	This event occurs when the device capacity threshold back to normal.

Parent topic: [Threshold Events](#)

# Tunnel Events - Access Point (AP)

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

- [Data plane accepted a tunnel request](#)
- [Data plane rejected a tunnel request](#)
- [Data plane terminated a tunnel](#)
- [AP created a tunnel](#)
- [AP tunnel disconnected](#)
- [AP softGRE tunnel fails over primary to secondary](#)
- [AP softGRE tunnel fails over secondary to primary](#)
- [AP softGRE gateway reachable](#)
- [AP softGRE gateway not reachable](#)
- [Data plane set up a tunnel](#)
- [AP secure gateway association success](#)
- [AP is disconnected from secure gateway](#)
- [AP secure gateway association failure](#)

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

Parent topic: [Events Types](#)

## Data plane accepted a tunnel request

**Table 1.** Data plane accepted a tunnel request event

Event	Data plane accepted a tunnel request
Event Type	dpAcceptTunnelRequest

Event	Data plane accepted a tunnel request
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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## Data plane rejected a tunnel request

**Table 1.** 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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## Data plane terminated a tunnel

**Table 1.** 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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP created a tunnel

**Table 1.** 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",


Event	AP created a tunnel
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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP tunnel disconnected

**Table 1.** 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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP softGRE tunnel fails over primary to secondary

**Table 1.** 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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP softGRE tunnel fails over secondary to primary

**Table 1.** 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"

Event	AP softGRE tunnel fails over secondary to primary
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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP softGRE gateway reachable

**Table 1.** 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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)


## AP softGRE gateway not reachable

**Table 1.** AP softGRE gateway not reachable event

Event	AP softGRE gateway not reachable
Event Type	apSoftGREGatewayNotReachable
Event Code	614
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softGREGatewayList"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}].
Description	This event occurs when AP fails to build a soft GRE tunnel either on the primary or the secondary GRE.
Auto Clearance	This event triggers the alarm 614, which is auto cleared by the event code 613.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## Data plane set up a tunnel

 **Note:** This event is not applicable for vSZ-H.

**Table 1.** Data plane set up a tunnel event

Event	Data plane set up a tunnel
Event Type	dpSetUpTunnel
Event Code	627
Severity	Informational

Event	Data plane set up a tunnel
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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP secure gateway association success

**Table 1.** 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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP is disconnected from secure gateway

**Table 1.** AP is disconnected from secure gateway event

Event	AP is disconnected from secure gateway
Event Type	ipsecTunnelDisassociated
Event Code	661
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is disconnected from secure gateway [{ipsecGWAddress}].
Description	This event occurs when the AP is disconnected from secure gateway.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## AP secure gateway association failure


**Table 1.** 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}].

Event	AP secure gateway association failure
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.

Parent topic: [Tunnel Events - Access Point \(AP\)](#)

## 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](#)
- [DP sGRE keep alive timeout](#)
- [DP sGRE GW inactive](#)
- [DP DHCPRelay no response](#)
- [DP DHCPRelay failover](#)
- [DP sGRE new tunnel](#)
- [DP sGRE del tunnel](#)
- [DP sGRE keepalive recovery](#)
- [DP DHCPRelay response recovery](#)
- [DP sGRE GW reachable](#)
- [DP sGRE GW active](#)
- [DP sGRE GW failover](#)
- [DP switchover](#)

Parent topic: [Events Types](#)

## DP sGRE GW unreachable

**Table 1.** 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE keep alive timeout

**Table 1.** 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

Event	DP sGRE keep alive 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE GW inactive

**Table 1.** 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP DHCPRelay no response

**Table 1.** DP DHCPRelay no response event

Event	DP DHCPRelay no response
Event Type	dpDhcpRelayNoResp
Event Code	618

Event	DP DHCPRelay no response
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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP DHCPRelay failover

**Table 1.** 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE new tunnel

**Table 1.** 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE del tunnel

**Table 1.** DP sGRE del tunnel event

Event	DP sGRE del tunnel
Event Type	dpSgreDelTunnel
Event Code	621
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "greType"="L2oGRE, L3oGRE", "apIpAddress"="x.x.x.x"
Displayed on the web interface	Dataplane [{dpName}   {dpKey}] lost a [{greType}] tunnel connection to AP[{apIP}].

Event	DP sGRE del tunnel
Description	This event occurs when access tunnel is disconnected due to a timeout.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE keepalive recovery

**Table 1.** 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP DHCPRelay response recovery

**Table 1.** DP DHCPRelay response recovery event

Event	DP DHCPRelay response recovery
Event Type	dpDhcpRelayRespRecovery
Event Code	623

Event	DP DHCPRelay response recovery
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dhcplIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName   dpKey}] detected DHCP server [{dhcplIP}] is now responsive
Description	This event occurs when the DHCP server resumes answering the relay request from data plane.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE GW reachable

**Table 1.** 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
Description	This event occurs when the core gateway is reachable.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE GW active

**Table 1.** 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.

Parent topic: [Tunnel Events - Data Plane](#)

## DP sGRE GW failover

**Table 1.** 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}].

Event	DP sGRE GW failover
Description	This event occurs when the data plane switches to the other gateway due to failover threshold limit.

Parent topic: [Tunnel Events - Data Plane](#)

## DP switchover

**Table 1.** DP switchover event

Event	DP switchover
Event Type	dpSwitchover
Event Code	628
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apName"="x", "ip"="x.x.x.x"
Description	This event occurs when the data plane switchover to another cluster.

Parent topic: [Tunnel Events - Data Plane](#)

## AP Ethernet Phy Error Count

**Table 1.** AP Ethernet Phy Error Count event

Event	AP Ethernet Phy Error Count
Event Type	ethPhyError
Event Code	353
Severity	Informational

Event	AP Ethernet Phy Error Count
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "linkDs"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] ethPhyDownShift [{linkDs}].
Description	This event triggers when the ethernet PHY error count is more than the threshold value.

Parent topic: [Events Types](#)

## AP Ethernet PHY Down Shift

**Table 1.** AP Ethernet PHY Down Shift event

Event	AP Ethernet PHY Down Shift
Event Type	ethPhyDownShift
Event Code	354
Severity	Major
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "linkDs"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] ethPhyDownShift [{linkDs}].
Description	This event triggers when the ethernet PHY downshift the link speed.

Parent topic: [Events Types](#)

# AP BAND Change

[apIllegalToChange3rdRadioBand](#)

[apIllegal6gVAPCreation](#)

[ap6gWLANCfgDone](#)

Parent topic: [Events Types](#)

## apIllegalToChange3rdRadioBand

**Table 1.** apIllegalToChange3rdRadioBand event

Event	apIllegalToChange3rdRadioBand
Event Type	apIllegalToChange3rdRadioBand
Event Code	356
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "countryCode"="xxxxxx",
Displayed on the web interface	AP [{apName&&apMac}] [{countryCode}] is not supporting 6G BAND for 3rd radio.
Description	This event triggers when the BAND change for 3rd radio is not allowed due to Country Configuration

Parent topic: [AP BAND Change](#)

## apIllegal6gVAPCreation

**Table 1.** apIllegal6gVAPCreation event

Event	apIllegal6gVAPCreation
Event Type	apIllegal6gVAPCreation

Event	apIllegal6gVAPCreation
Event Code	357
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] failed to create 3rd Radio VAP of SSID [{ssid}]
Description	This event triggers when the 6G Radio received the WLAN's with Security is other than WPA3 and OWE

Parent topic: [AP BAND Change](#)

## ap6gWLANCfgDone

**Table 1.** ap6gWLANCfgDone event

Event	ap6gWLANCfgDone
Event Type	ap6gWLANCfgDone
Event Code	358
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] complete WLAN configuration on 3rd Radio 6G BAND
Description	This event triggers when the 6G Radio configures all the WLAN's and all the VAP's are legal

Parent topic: [AP BAND Change](#)



**Corporate Headquarters**

**CommScope • Hickory • North Carolina • 28602 • USA**

T: 1-828-324-2200

[www.commscope.com](http://www.commscope.com)