

# SmartZone 5.2.2 (LT-GD) Alarm and Event Reference Guide (SZ100/vSZ-E)

## Supporting SmartZone 5.2.2 LT GD MR2

# Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

# Contents

---

<b>Preface</b> .....	<b>19</b>
Contacting RUCKUS Customer Services and Support.....	19
What Support Do I Need?.....	19
Open a Case.....	19
Self-Service Resources.....	20
Document Feedback.....	20
RUCKUS Product Documentation Resources.....	20
Online Training Resources.....	20
Document Conventions.....	21
Notes, Cautions, and Safety Warnings.....	21
Command Syntax Conventions.....	21
<b>About This Guide</b> .....	<b>23</b>
Introduction.....	23
New in This Document.....	23
Terminology.....	23
<b>Alarm and Event Management</b> .....	<b>25</b>
Overview.....	25
Alarm and Event Management.....	25
Event Categories.....	25
Event Attributes.....	26
Generation of Alarm and Event.....	26
<b>Alarm Types</b> .....	<b>29</b>
Introduction.....	29
Accounting Alarms.....	29
Accounting server not reachable.....	29
AP Authentication Alarms.....	30
RADIUS server unreachable.....	30
LDAP server unreachable.....	31
AD server unreachable.....	31
WeChat ESP authentication server unreachable.....	31
WeChat ESP authentication server unresolvable.....	32
WeChat ESP DNAT server unreachable.....	32
WeChat ESP DNAT server unresolvable.....	33
AP Communication Alarms.....	33
AP rejected.....	33
AP configuration update failed.....	34
AP swap model mismatched.....	34
AP pre-provision model mismatched.....	35
AP firmware update failed.....	35
AP WLAN oversubscribed.....	35
AP LBS Alarms.....	36
No LS responses.....	36
LS authentication failure.....	36
AP failed to connect to LS.....	37
AP State Change Alarms.....	37

AP rebooted by system.....	38
AP disconnected.....	38
AP deleted.....	38
AP cable modem interface down.....	39
AP DHCP service failure.....	39
AP NAT failure.....	39
AP DHCP/NAT DWPDP Ethernet port configuration override.....	40
SZ DHCP/NAT DWPDP Ethernet port configuration override.....	40
SIM removal.....	41
AP System Anomaly.....	41
Authentication Alarms.....	41
Authentication server not reachable.....	42
Authentication failed over to secondary.....	42
Authentication fallback to primary.....	42
AD/LDAP connectivity failure.....	43
Bind fails with AD/LDAP.....	43
Bind success with LDAP, but unable to find clear text password for the user.....	44
RADIUS fails to connect to AD NPS server.....	44
RADIUS fails to authenticate with AD NPS server.....	45
Fails to establish TLS tunnel with AD/LDAP.....	45
Control and Data Plane Interface Alarms.....	46
GtpManager (DP) disconnected.....	46
Cloud Alarms.....	47
Cloud Analytics Service has been Enabled.....	47
Cloud Analytics Service has been Disabled.....	47
Cloud Analytics Disconnected.....	47
Cluster Alarms.....	47
New node failed to join.....	48
Node removal failed.....	49
Node out of service.....	49
Cluster in maintenance state.....	50
Cluster backup failed.....	50
Cluster restore failed.....	51
Cluster upgrade failed.....	51
Cluster application stopped.....	52
Node bond interface down.....	52
Node physical interface down.....	53
Cluster node rebooted.....	53
Cluster node shut down.....	54
Node IP Changed.....	54
Disk usage exceed threshold.....	54
Cluster out of service.....	55
Cluster upload AP firmware failed.....	55
Cluster add AP firmware failed.....	56
Unsync NTP time.....	56
Cluster upload KSP file failed.....	56
Configuration backup failed.....	57
Configuration restore failed.....	57
AP certificate updated.....	57
Upgrade SS table failed.....	58

Over switch max capacity.....	58
AP is connected to Standby Cluster Over The Expiration Date.....	58
Cluster redundancy sync configuration failed.....	59
Cluster redundancy restoring configuration failed.....	59
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy.....	59
Not all APs rehome after timeout.....	60
External DP Connected to Standby Cluster after Rehome Timeout.....	60
Certificate is about to Expire.....	60
Certificate is already Expired.....	61
Configuration Alarms.....	61
Zone configuration preparation failed.....	61
AP configuration generation failed.....	62
End-of-life AP model detected.....	62
VLAN configuration mismatch on non DHCP/NAT WLAN.....	63
VLAN configuration mismatch on DHCP/NAT WLAN.....	63
Data Plane Alarms.....	63
Data plane configuration update failed.....	64
Data plane disconnected.....	64
Data plane physical interface down.....	65
Data plane process restarted.....	65
Data plane license is not enough.....	65
Data plane upgrade failed.....	66
Data plane of data center side fails to connect to the CALEA server.....	66
Data plane fails to connects to the other data plane.....	67
Data Plane DHCP IP Pool usage rate is 100 percent.....	67
Data Streaming Alarms.....	68
Connecting Failure to a Data Streaming Profile.....	68
IPMI Alarms.....	68
ipmiThempBB.....	68
ipmiThempP.....	69
ipmiFan.....	69
ipmiFanStatus.....	69
Licensing Interface Alarms.....	70
License going to expire.....	70
Insufficient license capacity.....	70
Data plane DHCP IP license insufficient.....	71
Data plane NAT session license insufficient.....	71
Insufficient license capacity .....	72
SCI Alarms.....	72
Connect to SCI failure.....	72
SCI has been disabled.....	73
SCI and FTP have been disabled.....	73
System Alarms.....	73
No LS responses.....	74
LS authentication failure.....	74
{produce.short.name} failed to connect to LS.....	75
Syslog server unreachable.....	75
CSV export FTP maximum retry.....	75
CSV export disk threshold exceeded.....	76
CSV export disk max capacity reached.....	76

Process restart.....	76
Service unavailable.....	77
Keepalive failure.....	77
Resource unavailable.....	78
The last one data plane is disconnected zone affinity profile.....	78
Unconfirmed program detection.....	78
Switch Alarms.....	79
Power supply failure.....	80
Fan failure.....	80
Module insertion.....	80
Module removal.....	81
Temperature above threshold warning.....	81
Stack member unit failure.....	81
PoE power allocation failure.....	82
DHCP_Snooping: DHCP offer dropped message.....	82
Port put into error disable state.....	82
Switch offline.....	83
Switch duplicated.....	83
Reject certificate signing request.....	83
Pending certificate signing request.....	84
Switch CPU major threshold exceed .....	84
Switch CPU critical threshold exceed .....	84
Switch memory major threshold exceed .....	85
Switch memory critical threshold exceed .....	85
Switch custom major threshold exceed .....	85
Switch custom critical threshold exceed .....	86
Switch Firmware Upgrade Failed.....	86
Switch Configuration Update Failed.....	86
Threshold Alarms.....	86
CPU threshold exceeded.....	87
Memory threshold exceeded.....	87
Disk usage threshold exceeded.....	88
The drop of client count threshold exceeded.....	88
License threshold exceeded.....	89
HDD Health Degradation.....	89
Rate limit for TOR surpassed.....	89
The number of users exceeded its limit.....	90
The number of devices exceeded its limit.....	90
Over AP maximum capacity.....	91
Over Device maximum capacity.....	91
Tunnel Alarms - Access Point.....	91
AP softGRE gateway not reachable.....	91
AP is disconnected from secure gateway.....	92
AP secure gateway association failure.....	92
<b>Events Types.....</b>	<b>93</b>
Accounting Events.....	93
Accounting server not reachable.....	93
AP accounting response while invalid config.....	94
AP account message drop while no accounting start message.....	94
Unauthorized COA/DM message dropped.....	95

AP Communication Events.....	95
AP discovery succeeded.....	95
AP managed.....	96
AP rejected.....	96
AP firmware updated.....	96
AP firmware update failed.....	97
Updating AP firmware.....	97
Updating AP configuration.....	97
AP configuration updated.....	97
AP configuration update failed.....	98
AP pre-provision model mismatched.....	98
AP swap model mismatched.....	98
AP WLAN oversubscribed.....	99
AP illegal to change country code.....	99
AP configuration get failed.....	99
Rogue AP.....	100
Rogue AP disappeared.....	100
Classified Rogue AP.....	100
AP image signing failed.....	101
Jamming attack.....	101
Rogue client.....	101
Key gen fail.....	102
Key dis fail.....	102
Key dis fail GTK.....	102
wpaendec fail.....	102
IPsecsec fail.....	103
Fw manual initiation.....	103
AP Management TSF data.....	103
AP TSF failure.....	104
AP Self tests.....	104
Firmware initiation update.....	104
SSH initiation.....	105
SSH termination.....	105
SSH failure.....	105
TLS initiation.....	106
TLS termination.....	106
TLS failure.....	106
IP sec initiation.....	107
IP sec termination.....	107
IP sec failure.....	107
AP LBS Events.....	107
No LS responses.....	108
LS authentication failure.....	108
AP connected to LS.....	108
AP failed to connect to LS.....	109
AP started location service.....	109
AP stopped location service.....	109
AP received passive calibration request.....	109
AP received passive footfall request.....	110
AP received unrecognized request.....	110

AP Mesh Events.....	110
EMAP downlink connected to MAP.....	111
EMAP downlink disconnected from MAP.....	111
EMAP uplink connected to MAP.....	111
EMAP uplink disconnected from MAP.....	112
MAP disconnected.....	112
MAP downlink connected.....	112
MAP downlink connected to EMAP.....	112
MAP downlink disconnected from EMAP.....	113
RAP downlink connected to MAP.....	113
MAP uplink connected to EMAP.....	113
MAP uplink disconnected from EMAP.....	114
MAP uplink connected to RAP.....	114
MAP uplink connected to MAP.....	114
Mesh state updated to MAP.....	114
Mesh state updated to MAP no channel.....	115
Mesh state updated to RAP.....	115
Mesh state update to RAP no channel.....	115
MAP downlink connected to MAP.....	116
MAP downlink disconnected from MAP.....	116
RAP downlink disconnected from MAP.....	116
AP State Change Events.....	117
AP rebooted by user.....	117
AP rebooted by system.....	118
AP disconnected.....	118
AP IP address updated.....	118
AP reset to factory default.....	118
AP channel updated.....	119
AP country code updated.....	119
AP channel updated because dynamic frequency selection (DFS) detected a radar.....	119
AP change control plane.....	120
AP connected.....	120
AP deleted.....	120
AP heartbeat lost.....	121
AP tagged as critical.....	121
AP cable modem interface down.....	121
AP brownout.....	121
AP cable modem power-cycled by user.....	122
AP smart monitor turn off WLAN.....	122
AP client load balancing limit reached.....	122
AP client load balancing limit recovered.....	123
AP WLAN state changed.....	123
AP capacity reached.....	123
AP capacity recovered.....	124
AP cable modem interface up.....	124
AP cable modem soft-rebooted by user.....	124
AP cable modem set to factory default by user.....	125
AP health high latency flag.....	125
AP health low capacity flag.....	125
AP health high connection failure flag.....	126



AP health high client count flag.....	126
AP health high latency clear.....	126
AP health low capacity clear.....	127
AP health high connection failure clear.....	127
AP health high client count clear.....	127
Primary DHCP AP is down.....	128
Primary DHCP AP is up.....	128
Secondary DHCP AP is down.....	128
Secondary DHCP AP is up.....	129
Primary or secondary DHCP AP detects 90% of the configured total IPs.....	129
Both primary and secondary DHCP server APs are down.....	129
AP NAT gateway IP failover detected for particular VLAN pool.....	129
AP NAT gateway IP fall back detected for particular VLAN pool.....	130
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.....	130
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.....	131
AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down.....	131
AP health high airtime utilization flag.....	131
AP health high airtime utilization clear.....	132
AP cluster failover.....	132
AP cluster rehome.....	132
AP MAC OUI violation.....	133
Backhaul switched to primary.....	133
Backhaul switched to secondary.....	133
LTE network connectivity lost.....	134
Ethernet network connectivity lost.....	134
LTE DHCP timeout.....	134
Ethernet link down.....	134
Ethernet link up.....	135
SIM switch.....	135
Remote host blacklisted.....	135
SIM removal.....	136
LTE network registration status.....	136
LTE connection status.....	136
AP System Anomaly.....	136
Mesh network connectivity lost.....	137
AP Authentication Events.....	137
Radius server reachable.....	138
Radius server unreachable.....	138
LDAP server reachable.....	138
LDAP server unreachable.....	139
AD server reachable.....	139
AD server unreachable.....	139
Wechat ESP authentication server reachable.....	140
WeChat ESP authentication server unreachable.....	140
WeChat ESP authentication server resolvable.....	140
WeChat ESP authentication server unresolvable.....	141
WeChat ESP DNAT server reachable.....	141
WeChat ESP DNAT server unreachable.....	141

WeChat ESP DNAT server resolvable.....	142
WeChat ESP DNAT server unresolvable.....	142
Authentication Attempts.....	143
Authentication Unsuccessful.....	143
Authentication Re-attempt.....	143
Authentication 8021.....	143
AP Local Session Timeout.....	144
AP Remote Session Timeout.....	144
AP Interactive Session Termination.....	144
AP USB Events.....	145
AP USB software package downloaded.....	145
AP USB software package download failed.....	145
Authentication Events.....	145
Authentication server not reachable.....	146
Authentication failed over to secondary.....	146
Authentication fallback to primary.....	146
AD/LDAP connected successfully.....	147
AD/LDAP connectivity failure.....	147
Bind fails with AD/LDAP.....	147
Bind success with LDAP, but unable to find clear text password for the user.....	148
RADIUS fails to connect to AD NPS server.....	148
RADIUS fails to authenticate with AD NPS server.....	148
Successfully established the TLS tunnel with AD/LDAP.....	149
Fails to establish TLS tunnel with AD/LDAP.....	149
TLS Establishment Failed between SZ and external AAA Server.....	149
Authorization Events.....	150
DM received from AAA.....	150
DM NACK sent to AAA.....	151
DM sent to NAS.....	151
DM NACK received from NAS.....	151
CoA received from AAA.....	152
CoA NACK sent to AAA.....	152
CoA sent NAS.....	152
CoA NAK received NAS.....	153
CoA authorize only access reject.....	153
CoA RWSG MWSG notification failure.....	153
Control and Data Plane Interface Events.....	154
DP connected.....	154
GtpManager (DP) disconnected.....	154
Session updated at DP.....	155
Session update at DP failed.....	155
Session deleted at DP.....	155
Session delete at DP failed.....	156
C2d configuration failed.....	156
Client Events.....	156
Client authentication failed.....	157
Client joined.....	158
Client failed to join.....	158
Client disconnected.....	158
Client connection timed out.....	159

Client authorization successfully.....	159
Client authorization failed.....	159
Client session expired.....	160
Client roaming.....	160
Client logged out.....	160
Client roaming disconnected.....	161
Client blocked.....	161
Client grace period .....	162
Onboarding registration succeeded .....	162
Onboarding registration failed .....	162
Remediation succeeded .....	163
Remediation failed .....	163
Force DHCP disconnected .....	163
WDS device joined .....	164
WDS device left.....	164
Client is blocked because of barring UE rule.....	164
Client is unblocked by barring UE rule.....	165
Start CALEA mirroring client.....	165
Stop CALEA mirroring client.....	165
Wired client joined.....	165
Wired client failed to join.....	166
Wired client disconnected.....	166
Wired client authorization successfully.....	166
Wired client session expired.....	167
Application identified.....	167
Application denied.....	167
URL filtering server unreachable.....	168
URL filtering server reachable.....	168
Packet spoofing detected.....	168
Packet spoofing detected.....	169
Packet spoofing detected.....	169
Packet spoofing detected.....	169
Cloud Events.....	170
Cloud Services Enabled.....	170
Cloud Services Disabled.....	170
Cloud Analytics Enabled.....	170
Cloud Analytics Disabled.....	171
Cloud Services Token Refreshed.....	171
Cloud Analytics Token Renewed.....	171
Cloud Analytics Disconnected.....	172
Cluster Events.....	172
Cluster created successfully.....	173
New node joined successfully.....	173
New node failed to join.....	173
Node removal completed.....	174
Node removal failed.....	174
Node out of service.....	174
Cluster in maintenance state.....	174
Cluster back in service.....	175
Cluster backup completed.....	175

Cluster backup failed.....	175
Cluster restore completed.....	176
Cluster restore failed.....	176
Cluster node upgrade completed.....	176
Entire cluster upgraded successfully.....	177
Cluster upgrade failed.....	177
Cluster application stopped.....	177
Cluster application started.....	177
Cluster backup started.....	178
Cluster upgrade started.....	178
Cluster leader changed.....	178
Node bond interface down.....	179
Node bond interface up.....	179
Node IP address changed.....	179
Node physical interface down.....	179
Node physical interface up.....	180
Cluster node rebooted.....	180
NTP time synchronized.....	180
Cluster node shutdown.....	181
Cluster upload started.....	181
Cluster upload completed.....	181
Cluster upload failed.....	182
SSH tunnel switched.....	182
Cluster remove node started.....	182
Node back in service.....	182
Resync NTP time.....	183
Disk usage exceed threshold.....	183
Cluster out of service.....	183
Initiated moving APs in node to a new cluster.....	184
Cluster upload vSZ-D firmware started.....	184
Cluster upload vSZ-D firmware completed.....	184
Cluster upload vSZ-D firmware failed.....	185
Cluster upload AP firmware started.....	185
Cluster upload AP firmware completed.....	185
Cluster upload AP firmware failed.....	185
Cluster add AP firmware started.....	186
Cluster add AP firmware completed.....	186
Cluster add AP firmware failed.....	186
Cluster name is changed.....	187
Unsync NTP Time.....	187
Cluster upload KSP file started.....	187
Cluster upload KSP file completed.....	188
Cluster upload KSP file failed.....	188
NTP unreachable server.....	188
Configuration backup started.....	188
Configuration backup succeeded.....	189
Configuration backup failed.....	189
Configuration restore succeeded.....	189
Configuration restore failed.....	190
AP Certificate Expired.....	190

AP Certificate Updated.....	190
Configuration restore started.....	190
Upgrade SSTable failed.....	191
Reindex elastic search finished.....	191
Initiated APs contact APR.....	191
All nodes back in service.....	192
Not management service ready.....	192
Management service ready.....	192
Configuration sync failed.....	192
Node IPv6 address added.....	193
Node IPv6 address deleted.....	193
AP is connected to standby cluster over the expiration date.....	193
Sync Configuration Failed for Cluster Redundancy.....	194
Standby Cluster Failed to Restore a Configuration for Cluster Redundancy.....	194
Standby Cluster Back to Monitoring Mode for Cluster Redundancy.....	194
Standby Cluster Restored a Configuration Success for Cluster Redundancy.....	194
AP Connected to Standby Cluster after Rehome Timeout.....	195
External DP Connected to Standby Cluster after Rehome Timeout.....	195
Sync Configuration started for Cluster Redundancy.....	195
Sync Configuration Success for Cluster Redundancy.....	196
Standby Cluster Restores a Configuration for Cluster Redundancy.....	196
Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy.....	196
Certificate is about to Expire.....	196
Certificate is already Expired.....	197
Result of Renew Certificate.....	197
Configuration Events.....	197
Configuration updated.....	198
Configuration update failed.....	198
Configuration receive failed.....	198
Incorrect flat file configuration.....	199
Zone configuration preparation failed.....	199
AP configuration generation failed.....	199
End-of-life AP model detected.....	200
VLAN configuration mismatch on non-DHCP/NAT WLAN.....	200
VLAN configuration mismatch on a DHCP/NAT WLAN.....	200
Datablade Events.....	201
DP integrity test failed.....	201
DP CLI enable failed.....	201
DP re-authentication.....	202
DP password min length updated.....	202
DP password changed.....	202
DP enable password changed.....	203
DP https authentication failed.....	203
DP certificate uploaded.....	203
DP Scg FQDN updated.....	203
DP initial upgrade.....	204
DP discontinuous time change NTP server DP Ntp time sync.....	204
DP user login.....	204
DP user login failed.....	205
DP user logout.....	205

DP account locked.....	205
DP session idle updated.....	205
DP session idle terminated.....	206
DP SSH tunnel failed.....	206
DP https connection failed.....	206
DP IPsec tunnel create failed.....	207
Data Plane Events.....	207
Data plane discovered.....	208
Data plane discovery failed.....	208
Data plane configuration updated.....	208
Data plane configuration update failed.....	208
Data plane rebooted.....	209
Data plane heartbeat lost.....	209
Data plane IP address updated.....	209
Data plane updated to a new control plane.....	210
Data plane status update failed.....	210
Data plane statistics update failed.....	210
Data plane connected.....	211
Data plane disconnected.....	211
Data plane physical interface down.....	211
Data plane physical interface up.....	211
Data plane packet pool is under low water mark.....	212
Data plane packet pool is under critical low water mark.....	212
Data plane packet pool is above high water mark.....	212
Data plane core dead.....	213
Data plane process restarted.....	213
Data plane discovery succeeded.....	213
Data plane managed.....	214
Data plane deleted.....	214
Data plane license is not enough.....	214
Data plane upgrade started.....	215
Data plane upgrading.....	215
Data plane upgrade succeeded.....	215
Data plane upgrade failed.....	215
Data Plane Upgrade Failed Due to Corrupted RPM.....	216
Data plane of data center side successfully connects to the CALEA server.....	216
Data plane of data center side fails to connect to the CALEA server.....	216
Data plane successfully connects to the other data plane.....	217
Data plane fails to connect to the other data plane.....	217
Data plane disconnects to the other data plane.....	218
Start CALEA mirroring client in data plane.....	218
Stop CALEA mirroring client in data plane.....	218
Data plane DHCP IP pool usage rate is 100 percent.....	219
Data plane DHCP IP pool usage rate is 80 percent.....	219
Data plane NAT session capacity usage rate is 80 percent.....	219
Data plane NAT session capacity usage rate is 100 percent.....	220
Data plane DHCP IP capacity usage rate is 80 percent.....	220
Data plane DHCP IP capacity usage rate is 100 percent.....	220
dplpmiThempBB.....	221
dplpmiThempP.....	221

dplpmiFan.....	222
dplpmiREThempBB.....	222
dplpmiREThempP.....	222
dplpmiREFan.....	223
Data plane backup success.....	223
Data plane backup failed.....	223
Data plane restore success.....	223
Data plane restore failed.....	224
Remote Administration Start.....	224
Remote Administration Stop.....	224
dplpmiThempIOH.....	225
dplpmiPsStatus.....	225
dplpmiREThempMemP.....	225
dplpmiPsStatus.....	225
dplpmiREThempMemP.....	226
dplpmiRePsStatus.....	226
dpSSDHealthDegrade.....	226
Data Plane Upgrade Failed Due to Corrupted RPM.....	227
Data Streaming Event.....	227
Connected to Data a Streaming Endpoint.....	227
Disconnected to Data a Streaming Endpoint.....	227
Connected to Data a Streaming Endpoint Failure.....	228
IPMI Events.....	228
ipmiThempBB.....	228
ipmiThempP.....	229
ipmiFan.....	229
ipmiFanStatus.....	229
ipmiREThempBB.....	230
ipmiREThempP.....	230
ipmiREFan.....	230
ipmiREFanStatus.....	230
Licensing Interface Events.....	231
License sync succeeded.....	231
License sync failed.....	232
License import succeeded.....	232
License import failed.....	232
License data changed.....	232
License going to expire.....	233
Insufficient license capacity.....	233
Data plane DHCP IP license insufficient.....	233
Data plane NAT session license insufficient.....	234
AP number limit exceeded.....	234
Insufficient license capacity.....	235
Data plane DHCP IP capacity license has been removed.....	235
Data plane NAT session capacity license has been removed.....	235
Insufficient license capacity.....	236
Session Events.....	236
Delete all sessions.....	236
System Events.....	236
No LS responses.....	237

LS authentication failure.....	237
{produce.short.name} connected to LS.....	238
{produce.short.name} failed to connect to LS.....	238
{produce.short.name} received passive request.....	238
{produce.short.name} sent controller information report.....	238
{produce.short.name} received management request.....	239
{produce.short.name} sent AP info by venue report.....	239
{produce.short.name} sent query venues report.....	239
{produce.short.name} sent associated client report.....	240
{produce.short.name} forwarded calibration request to AP.....	240
{produce.short.name} forwarded footfall request to AP.....	240
{produce.short.name} received unrecognized request.....	241
Syslog server reachable.....	241
Syslog server unreachable.....	241
Syslog server switched.....	241
System service failure.....	242
Generate AP config for plane load rebalance succeeded.....	242
Generate AP config for plane load rebalance failed.....	242
FTP transfer.....	243
FTP transfer error.....	243
File upload.....	243
Email sent successfully.....	244
Email sent failed.....	244
SMS sent successfully.....	244
SMS sent failed.....	244
Process restart.....	245
Service unavailable.....	245
Keepalive failure.....	245
Resource unavailable.....	246
Unconfirmed program detection.....	246
All data planes in the zone affinity profile are disconnected.....	246
CALEA UE Matched.....	247
ZD AP migrating.....	247
ZD AP migrated.....	247
ZD AP rejected.....	248
ZD AP migration failed.....	248
Database error.....	248
Database error.....	248
SZ Login Fail.....	249
SZ Login.....	249
SZ Logout.....	249
Password expiration.....	250
Admin account lockout.....	250
Admin session expired.....	250
Disable inactive admins.....	251
Two factor auth failed.....	251
Admin account lockout after failed attempts.....	251
Discontinuous time change.....	251
Connected to Data a Streaming Endpoint.....	252
Disconnected to Data a Streaming Endpoint.....	252



Connected to Data a Streaming Endpoint Failure.....	252
Failure of Key Generation.....	253
Failure Certificate.....	253
Failure of IPsec.....	253
IPsec KE is Up.....	253
IPsec IKE is Down.....	254
Switch Events.....	254
Switch critical message.....	255
Switch alert message.....	255
Switch warning message.....	255
Switch CPU warning threshold exceed.....	256
Switch CPU major threshold exceed.....	256
Switch CPU critical threshold exceed.....	256
Switch memory warning threshold exceed.....	256
Switch memory major threshold exceed.....	257
Switch memory critical threshold exceed.....	257
Switch custom warning threshold exceed.....	257
Switch custom major threshold exceed.....	258
Switch custom critical threshold exceed.....	258
GetCACert Request.....	258
Certificate signing request.....	259
Accept certificate signing request.....	259
Reject certificate signing request.....	259
Pending certificate signing request.....	259
Over Switch Max Capacity.....	260
Switch Duplicated.....	260
Switch is Offline for 15 Minutes.....	260
Switch Firmware Upgrade.....	261
Switch Firmware Upgrade Failed.....	261
Switch Configuration Update.....	261
Switch Configuration Update Failed.....	261
Switch Reboot.....	262
Switch Delete.....	262
Switch Disconnected from the Controller.....	262
Switch is Connected to the Controller.....	263
Switch Discovered by the Controller.....	263
Threshold Events.....	263
CPU threshold exceeded.....	264
Memory threshold exceeded.....	264
Disk usage threshold exceeded.....	264
CPU threshold back to normal.....	265
Memory threshold back to normal.....	265
Disk threshold back to normal.....	265
The drop of client count threshold exceeded.....	265
License threshold exceeded.....	266
HDD health degradation.....	266
Rate limit threshold surpassed.....	266
Rate limit threshold restored.....	267
Rate limit for TOR surpassed.....	267
The number of users exceed its limit.....	268

The number of devices exceeded its limit.....	268
Over AP maximum capacity.....	268
Over Device Maximum Capacity.....	268
Device Capacity Threshold Back to Normal.....	269
Tunnel Events - Access Point (AP).....	269
Data plane accepted a tunnel request.....	270
Data plane rejected a tunnel request.....	270
Data plane terminated a tunnel.....	270
AP created a tunnel.....	271
AP tunnel disconnected.....	271
AP SoftGRE tunnel fails over primary to secondary.....	271
AP SoftGRE tunnel fails over secondary to primary.....	272
AP SoftGRE gateway reachable.....	272
AP SoftGRE gateway not reachable.....	272
Data plane set up a tunnel.....	273
AP secure gateway association success.....	273
AP is disconnected from secure gateway.....	273
AP secure gateway association failure.....	273
Tunnel Events - Data Plane.....	274
DP sGRE GW unreachable.....	274
DP sGRE keep alive timeout.....	275
DP sGRE GW inactive.....	275
DP DHCPRelay no response.....	275
DP DHCPRelay failover.....	275
DP sGRE new tunnel.....	276
DP sGRE keepalive recovery.....	276
DP DHCPRelay response recovery.....	276
DP sGRE GW reachable.....	277
DP sGRE GW active.....	277
AP Ethernet PHY Down Shift.....	277
AP Ethernet Phy Error Count.....	278

# Preface

---

• Contacting RUCKUS Customer Services and Support.....	19
• Document Feedback.....	20
• RUCKUS Product Documentation Resources.....	20
• Online Training Resources.....	20
• Document Conventions.....	21
• Command Syntax Conventions.....	21

## 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.commscope.com/ruckus> and select **Support**.

### What Support Do I Need?

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

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

### Open a Case

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

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

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

## Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/>
- 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.commscope.com/ruckus>.

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

## Notes, Cautions, and Safety Warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

## Command Syntax Conventions

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

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



# About This Guide

- Introduction..... 23
- New in This Document..... 23
- Terminology..... 23

## Introduction

This *SmartZone Alarm and Event Reference Guide* describes the various types of alarms and events that SmartZone 100 (SZ100) and Virtual SmartZone-Essentials (vSZ-E) (collectively referred to as “the controller” throughout this guide) generates. For each alarm and event this guide provides the code, type, attributes, and description.

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

### NOTE

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

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

## New in This Document

TABLE 2 Summary of Enhancements in SmartZone Release 5.2.2 (June 2022)

Revision Number	Description	Location	Publication Date
A	Event code 554	Refer to <a href="#">Data Plane Upgrade Failed Due to Corrupted RPM</a> on page 216	June 2022

## Terminology

Table 3 lists the terms used in this guide.

TABLE 3 Terms used

Term	Description
AAA	Authentication, Authorization, and Accounting
AP	Access Point
APN	Access Point Name
CDR	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.
CLB	Client Load Balance
CNN	Configuration Change Notifier
CNR	Configuration Notification Receiver

## About This Guide

### Terminology

**TABLE 3** Terms used (continued)

Term	Description
CoA	Change of Authorization
Controller	Refers to either SZ100 or vSZ-E as the case may be.
CPE	Customer-Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DM	Dynamic Multipoint
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EMAP	Ethernet Mesh AP
EPS	Evolved Packet System
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunneling Protocol
GTPv1-U	GTP version 1, user plane
GTPv2-C	GTP version 2, control plane
HIP	Host Identity Protocol
MAP	Mobile Application Part
MOR	Maximum Outstanding Request
MTU	Maximum Transmission Unit
MWSG	Metro Wireless Security Gateway
NAS	Network Access Server
NTP	Network Time Protocol)
OUI	Organization Unique ID
PDP	Packet Data Protocol
produce.short.name	Refers to either SZ100 or vSZ-E
RAC	Radio Access Controller
RAP	Root Access Point
RSSI	Received Signal Strength Indicator
SSID	Service Set Identifier (SSID)
TCP	Transmission Control Protocol
TEID	Tunnel End Point Identifier
UE	User Equipment
UI	The SmartZone Web User Interface
USB	Universal Serial Bus
WDS	Wireless Distribution System



# Alarm and Event Management

---

- [Overview](#)..... 25
- [Alarm and Event Management](#)..... 25

## Overview

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

### NOTE

Refer to [About This Guide](#) on page 23 for the conventions used in this guide.

## Alarm and Event Management

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

- [Event Categories](#) on page 25
- [Event Attributes](#) on page 26
- [Generation of Alarm and Event](#) on page 26

## 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 controller web interface. This is because it reduces the performance of the system since its large in numbers. Enabling display of these events on the controller web interface is possible through CLI but it is not recommended.

## Event Attributes

An event always includes the following attributes:

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

## Generation of Alarm and Event

The following are the steps of how the controller generates alarm and event.

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:
    - 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 **Monitor > Alarms**
    - Date and Time
    - Code
    - Alarm Type
    - Severity
    - Status
    - Activity
    - Acknowledged on
    - Cleared By
    - Cleared On
    - Comments
  - d. On an alarm generation, the controller web interface **Monitor > Alarms** provides the following information as seen in Figure 1.

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 off the filter. Click on the gear icon to set the filters. A text box appears where you can enter the severity, status and start and end date and time. Click OK when done.

- 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 and 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 Alarms** 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 filters. 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
2017/01/24 16:...	302	AP rebooted by system	Major	Outstanding	AP [INDIA-AP-H510@1C:B9:C4:23:03...	N/A	N/A
2017/01/26 15:...	302	AP rebooted by system	Major	Outstanding	AP [R710-215@D4:68:4D:1A:6B:20] r...	N/A	N/A
2017/01/25 16:...	303	AP disconnected	Major	Outstanding	AP [INDIA-AP-H510@1C:B9:C4:23:03...	N/A	N/A
2017/01/25 16:...	303	AP disconnected	Major	Outstanding	AP [C110@F0:3E:90:3F:7F:40] disco...	N/A	N/A
2017/01/24 21:...	803	Node out of service	Critical	Outstanding	Node [set-2] in cluster [set-1] is out ...	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
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
2017/01/26 15:...	1601	Authentication server not reachable	Major	Outstanding	Authentication Server [172.19.13.10...	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

9 tota

2. Event - On an event generation:

- The controller collects, receives, and maintains the raw events from the managed entities (control plane, data plane and access points). These raw events are kept in the controller database, and are automatically purged.
- The controller allows users to enable/disable certain event types from the managed entities.
  - Disabled events are filtered at the source whenever possible to minimize resources for processing events
  - Threshold events are triggered at the source whenever possible.
- The controller provides an **events** log window as seen in Figure 2) for users to visualize and analyze the events. Users are able to perform various operations on the events, such as filtration, aggregation and counting. To view the below event information in the controller web interface navigate to **Events & Alarms > Events**.
  - Date and Time
  - Code
  - Type
  - Severity
  - Activity

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

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

Users are able to perform various operations on the events, such as filtration, aggregation and counting. The **Filter** button is deactivated by default. Click this button if you want to turn off the filter. Click on the gear icon to set the filters. 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:6B: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:6B:20] heartbeat lost.
2017/01/30 17:20:30	314	AP heartbeat lost	Informational	AP [T710@F0:3E:90:1B:A7:90] heartbeat lost.

**NOTE**

Refer to [Alarm Types](#) on page 29 and [Events Types](#) on page 93 for the list of alarms and events that the controller generates.

**NOTE**

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

**NOTE**

Refer to Administrator Guide for Viewing of Alarms and Events.

# Alarm Types

- Introduction..... 29
- Accounting Alarms..... 29
- AP Authentication Alarms..... 30
- AP Communication Alarms..... 33
- AP LBS Alarms..... 36
- AP State Change Alarms..... 37
- Authentication Alarms..... 41
- Control and Data Plane Interface Alarms..... 46
- Cloud Alarms..... 47
- Cluster Alarms..... 47
- Configuration Alarms..... 61
- Data Plane Alarms..... 63
- Data Streaming Alarms..... 68
- IPMI Alarms..... 68
- Licensing Interface Alarms..... 70
- SCI Alarms..... 72
- System Alarms..... 73
- Switch Alarms..... 79
- Threshold Alarms..... 86
- Tunnel Alarms - Access Point..... 91

## Introduction

This chapter provides information on the various types of alarms that the controller 100 generates. Alarms are a subset of the events defined. Categories are inherited from the event.

## Accounting Alarms

Following are the alarms related to accounting.

- [Accounting server not reachable](#) on page 29

## Accounting server not reachable

**TABLE 4** Accounting server not reachable alarm

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

## Alarm Types

### AP Authentication Alarms

**TABLE 4 Accounting server not reachable alarm (continued)**

Alarm	Accounting server not reachable
Attribute	"mvsold"=12, "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd", "realm"="wlan.3gppnetwork.org" "radProxyIp"="7.7.7.7", "accSrvrIp"="30.30.30.30" " {produce.short.name}"="2.2.2.2"
Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered when the accounting server cannot be reached.
Recommended Actions	Manual intervention is required. Check the web interface for the SZ connection to the AAA interface. Also, check if the RADIUS server can reach the AAA server interface.

## AP Authentication Alarms

Following are the alarms related to AP authentication.

- [RADIUS server unreachable](#) on page 30
- [LDAP server unreachable](#) on page 31
- [AD server unreachable](#) on page 31
- [WeChat ESP authentication server unreachable](#) on page 31
- [WeChat ESP authentication server unresolvable](#) on page 32
- [WeChat ESP DNAT server unreachable](#) on page 32
- [WeChat ESP DNAT server unresolvable](#) on page 33

## RADIUS server unreachable

**TABLE 5 RADIUS server unreachable alarm**

Alarm	RADIUS server unreachable
Alarm Type	radiusServerUnreachable
Alarm Code	2102
Severity	Major
Aggregation Policy	From the event code 2102 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ip"="17.0.0.12", "fwVersion"="3.2.0.0.x", "model"="ZF798 2", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2101.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach radius server [{ip}].
Description	This alarm is triggered when AP is unable to reach RADIUS server.
Recommended Actions	Check the network connectivity between AP and RADIUS server.

## LDAP server unreachable

TABLE 6 LDAP server unreachable alarm

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

## AD server unreachable

TABLE 7 AD server unreachable alarm

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

## WeChat ESP authentication server unreachable

TABLE 8 WeChat ESP authentication server unreachable alarm

Alarm	WeChat ESP authentication server unreachable
Alarm Type	espAuthServerUnreachable
Alarm Code	2152
Severity	Major
Aggregation Policy	From the event code 2152 an alarm is raised for every event. A single event triggers a single alarm.

## Alarm Types

### AP Authentication Alarms

**TABLE 8 WeChat ESP authentication server unreachable alarm (continued)**

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

## WeChat ESP authentication server unresolvable

**TABLE 9 WeChat ESP authentication server unresolvable alarm**

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

## WeChat ESP DNAT server unreachable

**TABLE 10 WeChat ESP DNAT server unreachable alarm**

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



**TABLE 10 WeChat ESP DNAT server unreachable alarm (continued)**

Alarm	WeChat ESP DNAT server unreachable
Description	This alarm is triggered when the AP is unable to reach WeChat ESP DNAT server.
Recommended Actions	Check the network connectivity between controller web interface and WeChat ESP DNAT server.

## WeChat ESP DNAT server unresolvable

**TABLE 11 WeChat ESP DNAT server unresolvable alarm**

Alarm	WeChat ESP DNAT server unresolvable
Alarm Type	espDNATServerUnresolvable
Alarm Code	2164
Severity	Major
Aggregation Policy	From the event code 2164 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dn"="www.test.com", "profileId"="1", "fwVersion"="3.2.0 0.x", "model"="ZF7982", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2163.
Displayed on the web interface	AP [{apName&&apMac}] is unable to resolve WeChat ESP DNAT server domain name [{dn}] to IP
Description	This alarm is triggered when the AP is unable to resolve WeChat ESP DNAT server domain name.
Recommended Actions	Check the DNS server configuration settings in the controller web interface.

## AP Communication Alarms

Following are the alarms related to access point communications.

- [AP rejected](#) on page 33
- [AP configuration update failed](#) on page 34
- [AP swap model mismatched](#) on page 34
- [AP pre-provision model mismatched](#) on page 35
- [AP firmware update failed](#) on page 35
- [AP WLAN oversubscribed](#) on page 35

### AP rejected

**TABLE 12 AP rejected alarm**

Alarm	AP rejected
Alarm Type	apStatusRejected
Alarm Code	101
Severity	Minor

## Alarm Types

### AP Communication Alarms

**TABLE 12 AP rejected alarm (continued)**

Alarm	AP rejected
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 by the controller.
Recommended Actions	Check if the number of licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses.

## AP configuration update failed

**TABLE 13 AP configuration update failed alarm**

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

## AP swap model mismatched

**TABLE 14 AP swap model mismatched alarm**

Alarm	AP swap model mismatched
Alarm Type	apModelDiffWithSwapOutAP
Alarm Code	104
Severity	Major
Aggregation Policy	From the event code 113 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx " "configModel"="xxx.xxx.xxx.xxx", "model"="xxx.xxx.xxx.xxx
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from swap configuration model [{configModel}].
Description	This alarm is triggered when the AP model differs from the swapped configuration model.
Recommended Actions	If the model is incorrect delete and rejoin the AP.

## AP pre-provision model mismatched

TABLE 15 AP pre-provision model mismatched alarm

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

## AP firmware update failed

TABLE 16 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 on the controller.
Recommended Actions	Retrieve the AP support text. Reboot the AP and trigger another configuration change for upgrading the AP. If it fails revert to the previous zone firmware.

## AP WLAN oversubscribed

TABLE 17 AP WLAN oversubscribed alarm

Alarm	AP WLAN oversubscribed
Alarm Type	apWlanOversubscribed
Alarm Code	108
Severity	Major
Aggregation Policy	From the event code 114 an alarm is raised for every event. A single event triggers a single alarm.

TABLE 17 AP WLAN oversubscribed alarm (continued)

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

## AP LBS Alarms

Following are the alarms related to AP Location Based Service.

- [No LS responses](#) on page 36
- [LS authentication failure](#) on page 36
- [AP failed to connect to LS](#) on page 37

## No LS responses

TABLE 18 No LS responses alarm

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

## LS authentication failure

TABLE 19 LS authentication failure alarm

Alarm	LS authentication failure
Alarm Type	apLBSAuthFailed
Alarm Code	702
Severity	Major

**TABLE 19 LS authentication failure alarm (continued)**

Alarm	LS authentication failure
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 web interface	AP [{apName&&apMac}] LBS authentication failed: url=[{url}], port=[{port}]
Description	This alarm is triggered due to the authentication failure on connecting to the location based service.
Recommended Actions	The password needs to be corrected in the LBS service page.

## AP failed to connect to LS

**TABLE 20 AP failed to connect to LS alarm**

Alarm	AP failed to connect to LS
Alarm Type	apLBSCoconnectFailed
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 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 name system (DNS) configuration is incorrect. It is recommended to check all the three possible error codes 701, 702 and 704.

## AP State Change Alarms

Following are the alarms related to access point state changes.

- [AP rebooted by system](#) on page 38
- [AP disconnected](#) on page 38
- [AP deleted](#) on page 38
- [AP cable modem interface down](#) on page 39
- [AP DHCP service failure](#) on page 39
- [AP NAT failure](#) on page 39
- [AP DHCP/NAT DWPDP Ethernet port configuration override](#) on page 40
- [SZ DHCP/NAT DWPDP Ethernet port configuration override](#) on page 40
- [SIM removal](#) on page 41

## Alarm Types

### AP State Change Alarms

## AP rebooted by system

TABLE 21 AP rebooted by system alarm

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

## AP disconnected

TABLE 22 AP disconnected alarm

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

## AP deleted

TABLE 23 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

TABLE 23 AP deleted alarm (continued)

Alarm	AP deleted
Description	This alarm is triggered when the AP is deleted.
Recommended Actions	This is a user action and to confirm check the user audit.

## AP cable modem interface down

TABLE 24 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.

## AP DHCP service failure

TABLE 25 AP DHCP service failure alarm

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

## AP NAT failure

TABLE 26 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

## Alarm Types

### AP State Change Alarms

**TABLE 26 AP NAT failure alarm (continued)**

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

## AP DHCP/NAT DWPD Ethernet port configuration override

**TABLE 27 AP DHCP/NAT DWPD Ethernet port configuration override alarm**

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

## SZ DHCP/NAT DWPD Ethernet port configuration override

**TABLE 28 SZ DHCP/NAT DWPD Ethernet port configuration override alarm**

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



## SIM removal

TABLE 29 SIM removal alarm

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

## AP System Anomaly

TABLE 30 AP System Anomaly alarm

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

## Authentication Alarms

The following are the alarms related to authentication.

- [Authentication server not reachable](#) on page 42
- [Authentication failed over to secondary](#) on page 42
- [Authentication fallback to primary](#) on page 42
- [AD/LDAP connectivity failure](#) on page 43
- [Bind fails with AD/LDAP](#) on page 43
- [Bind success with LDAP, but unable to find clear text password for the user](#) on page 44
- [RADIUS fails to connect to AD NPS server](#) on page 44
- [RADIUS fails to authenticate with AD NPS server](#) on page 45
- [Fails to establish TLS tunnel with AD/LDAP](#) on page 45

## Authentication server not reachable

TABLE 31 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	"mynoid"=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" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered when the authentication fails since the primary or secondary servers are not reachable.
Recommended Actions	Manual intervention is required. Check the web interface for the interface from the controller to AAA server. Also check if the AAA server can be reached from the RADIUS server. Ensure that the AAA server is UP.

## Authentication failed over to secondary

TABLE 32 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	"mynoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", srcProcess="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SZMgmtIp"="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} [{SZMgmtIp}]
Description	This alarm is triggered when the secondary RADIUS server is available after the primary server becomes zombie or dead.
Recommended Actions	No operator action is required.

## Authentication fallback to primary

TABLE 33 Authentication fallback to primary alarm

Alarm	Authentication fallback to primary
Alarm Type	authFallbackToPrimary
Alarm Code	1652
Severity	Major
Aggregation Policy	From the event code 1652 an alarm is raised for every event. A single event triggers a single alarm.

**TABLE 33 Authentication fallback to primary alarm (continued)**

Alarm	Authentication fallback to primary
Attribute	"mvsold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SZMgmtIp"="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} [[SZMgmtIp]]
Description	This alarm is triggered when automatic fallback is enable. Consequently, the authentication failover to secondary server occurs and the revival timer for the primary server expires, and the requests falls back to the primary server.
Recommended Actions	No action is required.

## AD/LDAP connectivity failure

**TABLE 34 AD/LDAP connectivity failure alarm**

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

## Bind fails with AD/LDAP

**TABLE 35 Bind fails with AD/LDAP alarm**

Alarm	Bind fails with AD/LDAP
Alarm Type	racADLDAPBindFail
Alarm Code	1753
Severity	Major
Aggregation Policy	From the event code 1753 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvsold"=12, "srcProcess"="RAC", "authSrvrIp"= "1.1.1.1", "username"="testuser"  "SZMgmtIp"="2.2.2.2", "desc"="Bind to AD/LDAP fails"

## Alarm Types

### Authentication Alarms

**TABLE 35 Bind fails with AD/LDAP alarm (continued)**

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

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

**TABLE 36 Bind success with LDAP, but unable to find clear text password for the user alarm**

Alarm	Bind success with LDAP, but unable to find clear text password for the user
Alarm Type	racLDAPFailToFindPassword
Alarm Code	1754
Severity	Major
Aggregation Policy	From the event code 1754 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrlp"="1.1.1.1", "username"="testuser"  "SZMgmtIp"="2.2.2.2", "desc"="Fail to find password"
Displayed on the web interface	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12  "srcProcess"="RAC", "authSrvrlp"="1.1.1.1", "username"="testuser"  "SZMgmtIp"="2.2.2.2", "desc"="Fail to find password"]
Description	This alarm is triggered when binding is successful with LDAP server using root credentials but it is unable to retrieve the clear text password for the user.
Recommended Actions	Verify whether the given username and clear text password are configured in the LDAP server.

## RADIUS fails to connect to AD NPS server

**TABLE 37 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", "authSrvrlp"="1.1.1.1", "username"="testuser"  "SZMgmtIp"="2.2.2.2", "desc"="Fails to connect to AD NPS server"

**TABLE 37 RADIUS fails to connect to AD NPS server alarm (continued)**

Alarm	RADIUS fails to connect to AD NPS server
Displayed on the web interface	{{srcProcess}} Fails to connect to AD NPS{{authSrvrIp}} from {produce.short.name} {{SZMgmtIp}}
Description	This alarm is triggered RADIUS server fails to connect to AD NPS server.
Recommended Actions	<ul style="list-style-type: none"> <li>• Verify if the configured NPS server instance is up and running (Network Policy Server)</li> <li>• Verify if the NPS server instance is communicating on the standard RADIUS port 1812</li> <li>• Ensure that Windows server where AD/NPS server is provisioned can be reached from the controller web interface</li> </ul>

## RADIUS fails to authenticate with AD NPS server

**TABLE 38 RADIUS fails to authenticate with AD NPS server alarm**

Alarm	RADIUS fails to authenticate with AD NPS server
Alarm Type	racADNPSFailToAuthenticate
Alarm Code	1756
Severity	Major
Aggregation Policy	From the event code 1756 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SZMgmtIp"="2.2.2.2", "desc"="Fails to authenticate with AD NPS"
Displayed on the web interface	{{srcProcess}} Fails to authenticate AD NPS{{authSrvrIp}} on {produce.short.name} {{SZMgmtIp}} for User{{userName}}
Description	This alarm is triggered when RADIUS server fails to authenticate with 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>

## Fails to establish TLS tunnel with AD/LDAP

**TABLE 39 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.

## Alarm Types

### Control and Data Plane Interface Alarms

**TABLE 39** Fails to establish TLS tunnel with AD/LDAP alarm (continued)

Alarm	Fails to establish TLS tunnel with AD/LDAP
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnoid"=12 "srcProcess"="RAC", "authSrvrIp" = "1.1.1.1" "authSrvrPort"="636", "SCGMgmtIp"="2.2.2.2" "desc"=" Fail to establish TLS Tunnel with LDAP/AD"
Displayed on the web interface	[[srcProcess]] Fails to authenticate AD NPS[[authSrvrIp]] on SCG[[SCGMgmtIp]] for User[[userName]]
Description	This alarm is triggered when TLS connection between the controller and AD/LDAP fails.

## Control and Data Plane Interface Alarms

### NOTE

This section is not applicable for vSZ-E.

Following alarm relates to control and data plane.

- [GtpManager \(DP\) disconnected](#) on page 46

## GtpManager (DP) disconnected

**TABLE 40** 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" "SZMgmtIp"="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} [[SZMgmtIp]]
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 Events</a> on page 154 event 1201.

## Cloud Alarms

### Cloud Analytics Service has been Enabled

**TABLE 41** Cloud Analytics Service has been Enabled Alarm

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

### Cloud Analytics Service has been Disabled

**TABLE 42** Cloud Analytics Service has been Disabled Alarm

Alarm	Cloud Analytics Service has been Disabled
Alarm Type	cloudAnalyticsDisabled
Alarm Code	4504
Severity	Major
Attribute	
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This alarm occurs when Smart Zone successfully disables cloud analytics service.

### Cloud Analytics Disconnected

**TABLE 43** Cloud Analytics Disconnected Alarm

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

## Cluster Alarms

Following are alarms related to cluster:

- [New node failed to join](#) on page 48

## Alarm Types

### Cluster Alarms

- [Node removal failed](#) on page 49
- [Node out of service](#) on page 49
- [Cluster in maintenance state](#) on page 50
- [Cluster backup failed](#) on page 50
- [Cluster restore failed](#) on page 51
- [Cluster upgrade failed](#) on page 51
- [Cluster application stopped](#) on page 52
- [Node bond interface down](#) on page 52
- [Node physical interface down](#) on page 53
- [Cluster node rebooted](#) on page 53
- [Cluster node shut down](#) on page 54
- [Disk usage exceed threshold](#) on page 54
- [Cluster out of service](#) on page 55
- [Cluster upload AP firmware failed](#) on page 55
- [Cluster add AP firmware failed](#) on page 56
- [Unsync NTP time](#) on page 56
- [Cluster upload KSP file failed](#) on page 56
- [Configuration backup failed](#) on page 57
- [Configuration restore failed](#) on page 57
- [AP certificate updated](#) on page 57
- [Upgrade SS table failed](#) on page 58
- [Over switch max capacity](#) on page 58

## New node failed to join

**TABLE 44** 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 {{{nodeName}}} failed to join cluster {{{clusterName}}}
Description	This alarm is triggered when a node fails to join a cluster session. The controller web Interface displays the error message.



TABLE 44 New node failed to join alarm (continued)

Alarm	New node failed to join
Recommended Actions	<p>When the operation fails, the user can run the <b>join process</b>. If it continues to fail, please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration &gt;&gt; Diagnostics &gt;&gt; Application Logs &amp; Status. Possible causes are:</p> <ul style="list-style-type: none"> <li>• The joining node is unable to complete the syncing of data in time. This could be due to the existing node performing compaction/repair etc.</li> <li>• The communication between the nodes may be broken. This could cause the operation to timeout such as IP address change or due to other events, which affects the network. Usually, it does not last for a long period of time.</li> </ul>

## Node removal failed

TABLE 45 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	<p>"clusterName"="xxx", "nodeName"="xxx",</p> <p>"nodeMac"=" xx:xx:xx:xx:xx:xx"</p>
Displayed on the web interface	Node [{nodeName}] failed to remove from cluster [{clusterName}].
Description	This alarm is triggered when it is unable to remove a node from the cluster.
Recommended Actions	In general, this alarm should rarely occur. If it occurs, restore to the previous backup file. Please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status.

## Node out of service

TABLE 46 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	<p>"clusterName"="xxx", "nodeName"="xxx",</p> <p>"nodeMac"=" xx:xx:xx:xx:xx:xx"</p>
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service. Reason:[{reason}].

## Alarm Types

### Cluster Alarms

**TABLE 46 Node out of service alarm (continued)**

Alarm	Node out of service
Description	This alarm is triggered when a node is out of service.
Recommended Actions	The operator/user needs to check the application/interface state.

## Cluster in maintenance state

**TABLE 47 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> <p>For any other cause, please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration &gt; Diagnostics &gt; Application Logs &amp; Status.</p>

## Cluster backup failed

**TABLE 48 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.

**TABLE 48 Cluster backup failed alarm (continued)**

Alarm	Cluster backup failed
Recommended Actions	<p>Check the disk usage. Try restoring the communication between nodes for a few more times. If the backup continues to fail or if you encounter Python script errors, please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration &gt; Diagnostics &gt; Application Logs &amp; Status. Possible causes:</p> <ul style="list-style-type: none"> <li>• Insufficient disk space.</li> <li>• Communication between nodes may be broken.</li> <li>• Errors due to the underlying Python script.</li> </ul>

## Cluster restore failed

**TABLE 49 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	<p>Try a few more times. If the backup restore continues failing, please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration &gt; Diagnostics &gt; Application Logs &amp; Status.</p> <p>The possible cause could be that the command for all nodes in the cluster failed. This could be due to a broken communication link between the nodes.</p>

## Cluster upgrade failed

**TABLE 50 Cluster upgrade failed alarm**

Alarm	Cluster upgrade failed
Alarm Type	upgradeClusterFailed
Alarm Code	807
Severity	Major
Aggregation Policy	From the event code 815 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 814.
Attribute	<p>"clusterName"="xxx", "nodeName"="xxx",</p> <p>"nodeMac"=" xx:xx:xx:xx:xx:xx", "fromVersion"="x.x",</p> <p>"toVersion"="x.x"</p>
Displayed on the web interface	Cluster [{{clusterName}}] could not be upgraded from [{{fromVersion}}] to [{{toVersion}}]. Reason:{{reason}}.

**TABLE 50 Cluster upgrade failed alarm (continued)**

Alarm	Cluster upgrade failed
Description	This alarm is triggered when a version upgrade of a cluster fails.
Recommended Actions	<p>Check the disk usage. Try restoring the communication between nodes for a few times. If the backup continues to fail or if you encounter Python script errors, please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to <b>Administration &gt; Diagnostics &gt; Application Logs &amp; Status</b>. Possible causes:</p> <ul style="list-style-type: none"> <li>• Insufficient disk space.</li> <li>• Communication between nodes might be broken.</li> <li>• Errors due to the underlying Python script.</li> </ul>

## Cluster application stopped

**TABLE 51 Cluster application stopped alarm**

Alarm	Cluster application stopped
Alarm Type	clusterAppStop
Alarm Code	808
Severity	Critical
Aggregation Policy	From the event code 816 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 817.
Attribute	"appName"="xxxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Application [{appName}] on node [{nodeName}] stopped
Description	This alarm is triggered when the application on a node stops.
Recommended Actions	This could happen to any application for various reasons. Please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status.

## Node bond interface down

**TABLE 52 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.

**TABLE 52 Node bond interface down alarm (continued)**

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 is broken. Please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status.

## Node physical interface down

**TABLE 53 Node physical interface down alarm**

Alarm	Node physical interface down
Alarm Type	nodePhyInterfaceDown
Alarm Code	810
Severity	Critical
Aggregation Policy	From the event code 824 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 825.
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Physical network interface {{networkInterface   ifName}} on node {{nodeName}} is down.
Description	This alarm is triggered when the physical interface of a node is down.
Recommended Actions	Check if the network cables of both the physical interfaces are broken. Alternatively, check if the physical interfaces for this bond interface is broken. Please send the complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration >> Diagnostics >> Application Logs & Status.

## Cluster node rebooted

**TABLE 54 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 complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration >> Diagnostics >> Application Logs & Status.

## Cluster node shut down

TABLE 55 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 "
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 complete log files to RUCKUS support. Download the system log file by logging to the controller system. Navigate to Administration >> Diagnostics >> Application Logs & Status.

## Node IP Changed

TABLE 56 Node IP Changed alarm

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

## Disk usage exceed threshold

TABLE 57 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"

**TABLE 57 Disk usage exceed threshold alarm (continued)**

Alarm	Disk usage exceed threshold
Displayed on the web interface	The disk usage of node {{nodeName}} is over {status}%.
Description	This alarm is triggered when the disk usage has reached the threshold limit.The disk usage percentage can be configured from 60% to 90%.
Recommended Actions	It is recommended that the user moves the backup files to the file transfer protocol (FTP) server and deletes the moved backup files.

## Cluster out of service

**TABLE 58 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 cluster is out of service.
Recommended Actions	It is recommended that the operator/user checks the out of service node to locate the reason.

## Cluster upload AP firmware failed

**TABLE 59 Cluster upload AP firmware failed alarm**

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

## Cluster add AP firmware failed

TABLE 60 Cluster add AP firmware failed alarm

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

## Unsync NTP time

TABLE 61 Unsync NTP time alarm

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

## Cluster upload KSP file failed

TABLE 62 Cluster upload KSP file failed alarm

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



## Configuration backup failed

TABLE 63 Configuration backup failed alarm

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

## Configuration restore failed

TABLE 64 Configuration restore failed alarm

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

## AP certificate updated

TABLE 65 AP certificate updated alarm

Alarm	AP certificate updated
Alarm Type	apCertificateExpire
Alarm Code	865
Severity	Critical
Aggregation Policy	From the event code 865 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 866.
Attribute	"count"="XXX"
Displayed on the web interface	{{count}} APs need to update their certificates.

TABLE 65 AP certificate updated alarm (continued)

Alarm	AP certificate updated
Description	This alarm is triggered when the AP certificate is not valid.
Recommended Actions	AP certificates need to be refreshed. Navigate to Administration > AP Certificate Replacement page to verify and follow the certificate refresh process.

## Upgrade SS table failed

TABLE 66 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.

## Over switch max capacity

TABLE 67 Over switch max capacity alarm

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

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

TABLE 68 AP is connected to standby cluster over the expiration date alarm

Alarm	AP Certificate Expired
Alarm Type	ApConnectedToStandbyClusterOverTheExpirationDate
Alarm Code	188
Severity	Critical
Attribute	apMac="xx:xx:xx:xx:xx:xx", days="xx"
Displayed on the web interface	The AP[{apMac}] is connected to standby cluster over [{days}] days, please move it to active cluster to avoid service interruption

**TABLE 68** AP is connected to standby cluster over the expiration date alarm (continued)

Alarm	AP Certificate Expired
Description	This alarm occurs when a AP is connected to standby cluster over the expiration date.

## 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 69** Cluster redundancy sync configuration failed alarm

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

## Cluster redundancy restoring configuration failed

**NOTE**

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

**TABLE 70** Cluster redundancy restoring configuration failed alarm

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

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

**TABLE 71** 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

**TABLE 71 Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy alarm (continued)**

Alarm	Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy
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.

## 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 72 Not all APs rehome after timeout alarm**

Alarm	Not all APs rehome after timeout
Alarm Type	clusterRedundancyApRehomeIncomplete
Alarm Code	881
Severity	Major
Aggregation Policy	From the event code 881 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"count"="xxx"
Displayed on the web interface	Standby cluster still has [[count]] AP connected.
Description	This alarm is triggered when the AP is still connected to the standby cluster.

## External DP Connected to Standby Cluster after Rehome Timeout

**TABLE 73 External DP Connected to Standby Cluster after Rehome Timeout alarm**

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

## Certificate is about to Expire

**TABLE 74 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.

**TABLE 74 Certificate is about to Expire alarm (continued)**

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.

## Certificate is already Expired

**TABLE 75 Certificate is already Expired alarm**

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

## Configuration Alarms

Following are the alarms related to configuration.

- [Zone configuration preparation failed](#) on page 61
- [AP configuration generation failed](#) on page 62
- [End-of-life AP model detected](#) on page 62
- [VLAN configuration mismatch on non DHCP/NAT WLAN](#) on page 63
- [VLAN configuration mismatch on DHCP/NAT WLAN](#) on page 63

## Zone configuration preparation failed

**TABLE 76 Zone configuration preparation failed alarm**

Alarm	Zone configuration preparation failed
Alarm Type	zoneCfgPrepareFailed
Alarm Code	1021
Severity	Major

## Alarm Types

### Configuration Alarms

**TABLE 76 Zone configuration preparation failed alarm (continued)**

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

## AP configuration generation failed

**TABLE 77 AP configuration generation failed alarm**

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

## End-of-life AP model detected

**TABLE 78 End-of-life AP model detected alarm**

Alarm	End-of-life AP model detected
Alarm Type	cfgGenSkippedDueToEolAp
Alarm Code	1023
Severity	Major
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "model"="R300,T300"
Displayed on the web interface	Detected usage of end-of-life ap model(s)[{model}] while generating configuration for AP(s) under zone[{zoneName}]
Description	This alarm is triggered when the controller detects the AP model's end-of-life under a certain zone.

**TABLE 78 End-of-life AP model detected alarm (continued)**

Alarm	End-of-life AP model detected
Recommended Actions	<p>These obsoleted APs occupies licensed AP space. Disconnect these unsupported AP models from the given zone by:</p> <ul style="list-style-type: none"> <li>Reset the APs to a factory setting using the AP command line</li> </ul> <p>Delete these APs through the <b>controller Web Interface &gt; Configuration AP List</b></p>

## VLAN configuration mismatch on non DHCP/NAT WLAN

**TABLE 79 VLAN configuration mismatch on non DHCP/NAT WLAN alarm**

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

## VLAN configuration mismatch on DHCP/NAT WLAN

**TABLE 80 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.

# Data Plane Alarms

Following are the alarms related to data plane.

- [Data plane configuration update failed](#) on page 64

## Alarm Types

### Data Plane Alarms

- [Data plane disconnected](#) on page 64
- [Data plane physical interface down](#) on page 65
- [Data plane process restarted](#) on page 65
- [Data plane license is not enough](#) on page 65
- [Data plane upgrade failed](#) on page 66

## Data plane configuration update failed

**TABLE 81** 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.

## Data plane disconnected

**TABLE 82** 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 the status to the control plane.
Recommended Actions	Check if the communicator is still alive and if the cluster interface is working.



## Data plane physical interface down

TABLE 83 Data plane physical interface down alarm

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

## Data plane process restarted

TABLE 84 Data plane process restarted alarm

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

## Data plane license is not enough

**NOTE**

Alarm 538 is applicable only for vSZ-E.

TABLE 85 Data plane license is not enough alarm

Alarm	Data plane license is not enough
Alarm Type	dpLicenseInsufficient
Alarm Code	538
Severity	Major
Aggregation Policy	From the event code 538 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"count"=<delete-vdp-count>

## Alarm Types

### Data Plane Alarms

**TABLE 85 Data plane license is not enough alarm (continued)**

Alarm	Data plane license is not enough
Displayed on the web interface	DP license is not enough, [{count}] instance of DP will be deleted.
Description	This alarm is triggered when the number of data plane licenses are insufficient.
Recommended Actions	Check if the number of data plane licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses and synchronize the licenses.

## Data plane upgrade failed

### NOTE

Alarm 553 is applicable only for vSZ-E

**TABLE 86 Data plane upgrade failed alarm**

Alarm	Data plane upgrade failed
Alarm Type	dpLicenseInsufficient
Alarm Code	553
Severity	Major
Aggregation Policy	From the event code 553 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpKey"="xx:xx:xx:xx:xx: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. <b>Note:</b> Debug file includes the upgrade log file. The operator can get the debug log from vSZ web interface or through vSZ-D CLI.</p> <p>The operator can use the following vSZ-D CLI commands to:</p> <ul style="list-style-type: none"><li>• View the previous upgrade status and reason in case of a failure - ruckus# show upgrade-state / ruckus# show upgrade-history</li><li>• Save the debug file for viewing - ruckus(debug)# save-log</li><li>• Check the connection status between vSZ and vSZ-D - ruckus# show status</li><li>• Check the current vSZ-D software version - ruckus# show version</li></ul> <p><b>Note:</b> Refer to the vSZ-D CLI Reference Guide for details on the CLI commands mentioned above.</p>

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

**TABLE 87 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

**TABLE 87** Data plane of data center side fails to connect to the CALEA server alarm  
(continued)

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

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

**TABLE 88** Data plane fails to connects to the other data plane alarm

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

## Data Plane DHCP IP Pool usage rate is 100 percent

**TABLE 89** Data plane DHCP IP pool usage rate is 100 percent alarm

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

# Data Streaming Alarms

[Connecting Failure to a Data Streaming Profile](#) on page 68

## Connecting Failure to a Data Streaming Profile

**TABLE 90** 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.

## IPMI Alarms

### NOTE

This section is not applicable for vSZ-E.

Following are the alarms related to IPMIs.

- [ipmiThempBB](#) on page 68
- [ipmiThempP](#) on page 69
- [ipmiFan](#) on page 69
- [ipmiFanStatus](#) on page 69

## ipmiThempBB

**TABLE 91** ipmiThempBB alarm

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

TABLE 91 ipmiThempBB alarm (continued)

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

## ipmiThempP

TABLE 92 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"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the reading surpasses threshold value is $\leq 55^{\circ}$ 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.

## ipmiFan

TABLE 93 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"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's fan module status is shown.
Recommended Actions	Replace the fan module.

## ipmiFanStatus

TABLE 94 ipmiFanStatus alarm

Alarm	ipmiFanStatus
Alarm Type	ipmiFanStatus
Alarm Code	912

## Alarm Types

### Licensing Interface Alarms

**TABLE 94 ipmiFanStatus alarm (continued)**

Alarm	ipmiFanStatus
Severity	Major
Aggregation Policy	From the event code 912 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 937.
Attribute	"id"="x", "status"="xxxx", "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.

## Licensing Interface Alarms

The following are the alarms related to licensing:

- [License going to expire](#) on page 70
- [Insufficient license capacity](#) on page 70
- [Data plane DHCP IP license insufficient](#) on page 71
- [Data plane NAT session license insufficient](#) on page 71
- [Insufficient license capacity](#) on page 72

### License going to expire

**TABLE 95 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.

### Insufficient license capacity

**TABLE 96 Insufficient license capacity alarm**

Alarm	Insufficient license capacity
Alarm Type	apConnectionTerminatedDueToInsufficientLicense

**TABLE 96 Insufficient license capacity alarm (continued)**

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

## Data plane DHCP IP license insufficient

**TABLE 97 Data plane DHCP IP license insufficient alarm**

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

## Data plane NAT session license insufficient

**TABLE 98 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", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This alarm occurs when Data Plane NAT session license insufficient. ( total [{{totalLicenseCnt}}, consumed [{{consumedLicenseCnt}}, available [{{availableLicenseCnt}}] )

**TABLE 98 Data plane NAT session license insufficient alarm (continued)**

Alarm	Data plane NAT session license insufficient
Description	This alarm is triggered when the data plane NAT server license is insufficient.

## Insufficient license capacity

**TABLE 99 Insufficient license capacity alarm**

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

## SCI Alarms

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

- [Connect to SCI failure](#) on page 72
- [SCI has been disabled](#) on page 73
- [SCI and FTP have been disabled](#) on page 73

## Connect to SCI failure

**TABLE 100 Connect to SCI failure alarm**

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



## SCI has been disabled

TABLE 101 SCI has been disabled alarm

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

## SCI and FTP have been disabled

TABLE 102 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.

## System Alarms

### NOTE

{produce.short.name} refers to SZ or vSZ-E.

Following are the alarms with the system log severity:

- [No LS responses](#) on page 74
- [LS authentication failure](#) on page 74
- [{produce.short.name} failed to connect to LS](#) on page 75
- [Syslog server unreachable](#) on page 75
- [CSV export FTP maximum retry](#) on page 75
- [CSV export disk threshold exceeded](#) on page 76

## Alarm Types

### System Alarms

- [CSV export disk max capacity reached](#) on page 76
- [Process restart](#) on page 76
- [Service unavailable](#) on page 77
- [Keepalive failure](#) on page 77
- [Resource unavailable](#) on page 78
- [The last one data plane is disconnected zone affinity profile](#) on page 78
- [Unconfirmed program detection](#) on page 78

## No LS responses

**TABLE 103** 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	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] 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 the location server is working properly.

## LS authentication failure

**TABLE 104** 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	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] authentication failed: url={{url}}, port={{port}}
Description	This alarm is triggered due to the authentication failure on connecting to the location based service.
Recommended Actions	Check the location server password.

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

TABLE 105 {produce.short.name} failed to connect to LSalarm

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	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] connection failed to LS: url=[{url}], port=[{port}]
Description	This alarm is triggered when the controller fails to connect to the location based service.
Recommended Actions	Check the location service configuration. Also check the network connectivity between the controller and location server.

## Syslog server unreachable

TABLE 106 Syslog server unreachable alarm

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

## CSV export FTP maximum retry

TABLE 107 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.

**TABLE 107 CSV export FTP maximum retry alarm (continued)**

Alarm	CSV export FTP maximum retry
Attribute	"nodeName"="xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx", "portID"="xx:xx:xx:xx:xx", "filename"="xxx.xxx.xxx.xxx"
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV file fails to transfer after a maximum of five (5) retries.

## CSV export disk threshold exceeded

**TABLE 108 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", "threshold"="xx:xx:xx:xx:xx", "availableDiskSize"="xx:xx:xx:xx:xx"
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV report size exceeds 80% of its capacity.
Recommended Actions	

## CSV export disk max capacity reached

**TABLE 109 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", "allocatedDiskSize"="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	

## Process restart

**TABLE 110 Process restart alarm**

Alarm	Process restart
Alarm Type	processRestart

**TABLE 110 Process restart alarm (continued)**

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

## Service unavailable

**TABLE 111 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", " {produce.short.name}MgmtIp"="2.2.2.2"
Displayed on the web interface	[[processName]] process is not stable on {produce.short.name} [[SZMgmtIp]]
Description	This alarm is triggered when the process repeatedly restarts and is unstable.
Recommended Actions	A manual intervention is required. Download the process log file from the controller web Interface to find the cause of the error.

## Keepalive failure

**TABLE 112 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", " {produce.short.name}MgmtIp"="2.2.2.2"
Displayed on the web interface	[[srcProcess]] on Smart Zone [[SZMgmtIp]] restarted [[processName]] process

TABLE 112 Keepalive failure alarm (continued)

Alarm	Keepalive failure
Description	This alarm is triggered when the <b>mon/nc</b> restarts the process due to a keep alive failure.
Recommended Actions	Download the process log file from the controller web Interface to locate the cause of the error.

## Resource unavailable

TABLE 113 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", " {produce.short.name}MgmtIp"="3.3.3.3", "cause"="xx"
Displayed on the web interface	System resource {{cause}} not available in {{srcProcess}} process at {produce.short.name} {{SZMgmtIp}}
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.

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

TABLE 114 The last one data plane is disconnected zone affinity profile alarm

Alarm	The last one data plane is disconnected zone affinity profile
Alarm Type	zoneAffinityLastDpDisconnected
Alarm Code	1267
Severity	Informational
Aggregation Policy	From the event code 1267 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"dpName="xxxxxxx", "dpKey"="xx:xx:xx:xx:xx:xx", "zoneAffinityProfileId"="xxxxxxx"
Displayed on the web interface	The Last one Data Plane[{{dpName}}&{{dpKey}}] is disconnected Zone Affinity profile[{{zoneAffinityProfileId}}].
Description	This alarm is logged when the last data plane is disconnected from the zone affinity.
Recommended Actions	

## Unconfirmed program detection

TABLE 115 Unconfirmed program detection alarm

Alarm	Unconfirmed program detection
Alarm Type	Unconfirmed Program Detection

**TABLE 115 Unconfirmed program detection alarm (continued)**

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

## Switch Alarms

Following are the alarms related to switch severity:

- [Power supply failure](#) on page 80
- [Fan failure](#) on page 80
- [Module insertion](#) on page 80
- [Module removal](#) on page 81
- [Temperature above threshold warning](#) on page 81
- [Stack member unit failure](#) on page 81
- [PoE power allocation failure](#) on page 82
- [DHCP\\_Snooping: DHCP offer dropped message](#) on page 82
- [Port put into error disable state](#) on page 82
- [Switch offline](#) on page 83
- [Switch duplicated](#) on page 83
- [Reject certificate signing request](#) on page 83
- [Pending certificate signing request](#) on page 84
- [Switch CPU major threshold exceed](#) on page 84
- [Switch CPU critical threshold exceed](#) on page 84
- [Switch memory major threshold exceed](#) on page 85
- [Switch memory critical threshold exceed](#) on page 85
- [Switch custom major threshold exceed](#) on page 85
- [Switch custom critical threshold exceed](#) on page 86
- [Switch Firmware Upgrade Failed](#) on page 86
- [Switch Configuration Update Failed](#) on page 86

## Power supply failure

TABLE 116 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.
Recommended Actions	Check the status of Switch power supply.

## Fan failure

TABLE 117 Fan failure alarm

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

## Module insertion

TABLE 118 Module insertion alarm

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



## Module removal

TABLE 119 Module removal alarm

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

## Temperature above threshold warning

TABLE 120 Temperature above threshold warning alarm

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

## Stack member unit failure

TABLE 121 Stack member unit failure alarm

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

## PoE power allocation failure

TABLE 122 PoE power allocation failure alarm

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

## DHCP\_Snooping: DHCP offer dropped message

TABLE 123 DHCP\_Snooping: DHCP offer dropped message alarm

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

## Port put into error disable state

TABLE 124 Port put into error disable state alarm

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

## Switch offline

TABLE 125 Switch offline alarm

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

## Switch duplicated

TABLE 126 Switch duplicated alarm

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

## Reject certificate signing request

TABLE 127 Reject certificate signing request alarm

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

## Pending certificate signing request

TABLE 128 Pending certificate signing request alarm

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

## Switch CPU major threshold exceed

TABLE 129 Switch CPU major threshold exceed alarm

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

## Switch CPU critical threshold exceed

TABLE 130 Switch CPU critical threshold exceed alarm

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

## Switch memory major threshold exceed

TABLE 131 Switch memory major threshold exceed alarm

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

## Switch memory critical threshold exceed

TABLE 132 Switch memory critical threshold exceed alarm

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

## Switch custom major threshold exceed

TABLE 133 Switch custom major threshold exceed alarm

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

## Switch custom critical threshold exceed

TABLE 134 Switch custom critical threshold exceed alarm

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

## Switch Firmware Upgrade Failed

TABLE 135 Switch Firmware Upgrade Failed alarm

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

## Switch Configuration Update Failed

TABLE 136 Switch Configuration Update Failed alarm

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

## Threshold Alarms

Following are the alarms related to threshold system set:

- [CPU threshold exceeded](#) on page 87
- [Memory threshold exceeded](#) on page 87

- [Disk usage threshold exceeded](#) on page 88
- [The drop of client count threshold exceeded](#) on page 88
- [License threshold exceeded](#) on page 89
- [HDD Health Degradation](#) on page 89
- [Rate limit for TOR surpassed](#) on page 89
- [The number of users exceeded its limit](#) on page 90
- [The number of devices exceeded its limit](#) on page 90
- [Over AP maximum capacity](#) on page 91

## CPU threshold exceeded

TABLE 137 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", "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 usage percentage threshold can be configured as 60% to 90%.
Recommended Actions	<p>Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to RUCKUS support.</p> <p>Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.</p>

## Memory threshold exceeded

TABLE 138 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", "perc"="XX"
Displayed on the web interface	Memory threshold [{{perc}}%] exceeded on control plane [{{nodeName}}-C].

**TABLE 138 Memory threshold exceeded alarm (continued)**

Alarm	Memory threshold exceeded
Description	This alarm is triggered when the memory usage exceeds the threshold limit. The disk threshold value for SZ100 is 85% and 90% for vSZ-E.
Recommended Actions	<p>Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to RUCKUS support.</p> <p>Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.</p>

## Disk usage threshold exceeded

**TABLE 139 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", "perc"="XX"
Displayed on the web interface	Disk usage threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the disk usage exceeds the threshold limit. The disk threshold value is 80%.
Recommended Actions	Check the backup files for disk usage. Each backup file may occupy a large disk space based on the database size. If there are multiple backup files/versions in the controller, it is recommended to delete the older backup files to free disk usage. If the problem persists, please take a screen shot and send it to RUCKUS support.

## The drop of client count threshold exceeded

**TABLE 140 The drop of client count threshold exceeded alarm**

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



## License threshold exceeded

TABLE 141 License threshold exceeded alarm

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

## HDD Health Degradation

**NOTE**

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

TABLE 142 HDD Health Degradation Alarm

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

## Rate limit for TOR surpassed

TABLE 143 Rate limit for TOR surpassed alarm

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

**TABLE 143 Rate limit for TOR surpassed alarm (continued)**

Alarm	Rate limit for TOR surpassed
Auto Clearance	The alarm code is auto cleared with the event code 1301.
Attribute	"mvnold"="12", "wlanId"="1", "zoneId"="10", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd",  "UserName"="abc@xyz.com, "realm"="wlan.3gppnetwor"  "SZMgmtIp"="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 alarm is triggered when maximum outstanding requests (MOR) is surpassed.
Recommended Actions	Download the SM log file from the controller web Interface to check the error cause.

## The number of users exceeded its limit

**TABLE 144 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	This alarm has no attributes.
Displayed on the web interface	The number of users exceeds the specified limit
Description	This alarm is triggered when the number of users exceeds the specified limit.
Recommended Actions	No action is required.

## The number of devices exceeded its limit

**TABLE 145 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	This alarm has no attributes.
Displayed on the web interface	Displayed on the web interface. The number of devices exceeded its limit
Description	This alarm is triggered the number of devices exceeds the specified limit.
Recommended Actions	No action is required.

## Over AP maximum capacity

TABLE 146 Over AP maximum capacity alarm

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

## Over Device maximum capacity

TABLE 147 Over Device maximum capacity alarm

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

## Tunnel Alarms - Access Point

Following are the alarms related to tunnel.

- [AP softGRE gateway not reachable](#) on page 91
- [AP is disconnected from secure gateway](#) on page 92
- [AP secure gateway association failure](#) on page 92

## AP softGRE gateway not reachable

TABLE 148 AP softGRE gateway not reachable alarm

Alarm	AP softGRE gateway not reachable
Alarm Type	apSoftGREGatewayNotReachable
Alarm Code	614
Severity	Major
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"

## Alarm Types

### Tunnel Alarms - Access Point

**TABLE 148 AP softGRE gateway not reachable alarm (continued)**

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

## AP is disconnected from secure gateway

**TABLE 149 AP is disconnected from secure gateway alarm**

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

## AP secure gateway association failure

**TABLE 150 AP secure gateway association failure alarm**

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

# Events Types

- Accounting Events..... 93
- AP Communication Events..... 95
- AP LBS Events..... 107
- AP Mesh Events..... 110
- AP State Change Events..... 117
- AP Authentication Events..... 137
- AP USB Events..... 145
- Authentication Events..... 145
- Authorization Events..... 150
- Control and Data Plane Interface Events..... 154
- Client Events..... 156
- Cloud Events..... 170
- Cluster Events..... 172
- Configuration Events..... 197
- Datablade Events..... 201
- Data Plane Events..... 207
- Data Streaming Event..... 227
- IPMI Events..... 228
- Licensing Interface Events..... 231
- Session Events..... 236
- System Events..... 236
- Switch Events..... 254
- Threshold Events..... 263
- Tunnel Events - Access Point (AP)..... 269
- Tunnel Events - Data Plane..... 274
- AP Ethernet PHY Down Shift..... 277
- AP Ethernet Phy Error Count..... 278

## Accounting Events

Following are the events related to accounting.

- [Accounting server not reachable](#) on page 93
- [AP accounting response while invalid config](#) on page 94
- [AP account message drop while no accounting start message](#) on page 94
- [Unauthorized COA/DM message dropped](#) on page 95

## Accounting server not reachable

**TABLE 151** Accounting server not reachable event

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

## Events Types

### Accounting Events

**TABLE 151 Accounting server not reachable event (continued)**

Event	Accounting server not reachable
Attribute	"mvnold"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "accSrvrIp"="30.30.30.30" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}].
Description	This event occurs when the controller is unable to connect to either the primary or secondary accounting server.

## AP accounting response while invalid config

**TABLE 152 AP accounting response while invalid config event**

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

## AP account message drop while no accounting start message

**TABLE 153 AP account message drop while no accounting start message event**

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

## Unauthorized COA/DM message dropped

TABLE 154 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", "radSrvrlp"="7.7.7.7","SZMgmtIp"="2.2.2.2"
Displayed on the web interface	{{srcProcess}} Dropped CoA/DM Packet received from AAA {{radSrvrlp}} on {{produce.short.name}} {{SZMgmtIp}}, with username {{userName}}. Received message from unauthorized AAA
Description	This event occurs when the controller receives a change of authorization (CoA) or dynamic multipoint (DM) messages from an unauthorized AAA server.

## AP 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.

<a href="#">AP discovery succeeded</a> on page 95	<a href="#">AP managed</a> on page 96	<a href="#">AP rejected</a> on page 96
<a href="#">AP firmware updated</a> on page 96	<a href="#">AP firmware update failed</a> on page 97	<a href="#">Updating AP firmware</a> on page 97
<a href="#">Updating AP configuration</a> on page 97	<a href="#">AP configuration updated</a> on page 97	<a href="#">AP configuration update failed</a> on page 98
<a href="#">AP pre-provision model mismatched</a> on page 98	<a href="#">AP swap model mismatched</a> on page 98	<a href="#">AP WLAN oversubscribed</a> on page 99
<a href="#">AP illegal to change country code</a> on page 99	<a href="#">AP configuration get failed</a> on page 99	<a href="#">Rogue AP</a> on page 100
<a href="#">Rogue AP disappeared</a> on page 100	<a href="#">Classified Rogue AP</a> on page 100	<a href="#">AP image signing failed</a> on page 101
<a href="#">Jamming attack</a> on page 101	<a href="#">Rogue client</a> on page 101	<a href="#">Key gen fail</a> on page 102
<a href="#">Key dis fail</a> on page 102	<a href="#">Key dis fail GTK</a> on page 102	<a href="#">wpaenc fail</a> on page 102
<a href="#">IPsec fail</a> on page 103	<a href="#">Fw manual initiation</a> on page 103	<a href="#">AP Management TSF data</a> on page 103
<a href="#">AP TSF failure</a> on page 104	<a href="#">AP Self tests</a> on page 104	<a href="#">Firmware initiation update</a> on page 104
<a href="#">SSH initiation</a> on page 105	<a href="#">SSH failure</a> on page 105	<a href="#">SSH termination</a> on page 105
<a href="#">TLS initiation</a> on page 106	<a href="#">TLS termination</a> on page 106	<a href="#">TLS failure</a> on page 106
<a href="#">IP sec initiation</a> on page 107	<a href="#">IP sec termination</a> on page 107	<a href="#">IP sec failure</a> on page 107

## AP discovery succeeded

TABLE 155 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"

## Events Types

### AP Communication Events

**TABLE 155 AP discovery succeeded event (continued)**

Event	AP discovery succeeded
Displayed on the web interface	AP [{apName&&apMac}] sent a discovery request to {produce.short.name} [{wsgIP}]
Description	This event occurs when the AP sends a discovery request to the {produce.short.name} successfully.

## AP managed

**TABLE 156 AP managed event**

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

## AP rejected

**TABLE 157 AP rejected event**

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

## AP firmware updated

**TABLE 158 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"="3.2.0.0.539", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{apName&&apMac}] updated its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP successfully updates the firmware details to the controller.



## AP firmware update failed

TABLE 159 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"="3.2.0.0.x", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{{apName&&apMac}}] failed to update its firmware from [{{fromVersion}}] to [{{toVersion}}].
Description	This event occurs when the AP fails to update the firmware details to the controller.
Auto Clearance	This event triggers the alarm 107, which is auto cleared by the event code 106.

## Updating AP firmware

TABLE 160 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"="3.2.0.0.x", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{{apName&&apMac}}] firmware is being updated from [{{fromVersion}}] to [{{toVersion}}].
Description	This event occurs when AP updates its firmware.

## Updating AP configuration

TABLE 161 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 the AP updates its configuration.

## AP configuration updated

TABLE 162 AP configuration updated event

Event	AP configuration updated
Event Type	apConfUpdated

## Events Types

### AP Communication Events

**TABLE 162 AP configuration updated event (continued)**

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

## AP configuration update failed

**TABLE 163 AP configuration update failed event**

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

## AP pre-provision model mismatched

**TABLE 164 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"="xxx.xxx.xxx.xxx" "model"="R700"
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from per-provision configuration model [configModel]
Description	This event occurs when the AP model differs from the configuration model.

## AP swap model mismatched

**TABLE 165 AP swap model mismatched event**

Event	AP swap model mismatched
Event Type	apModelDiffWithSwapOutAP
Event Code	113
Severity	Major

**TABLE 165 AP swap model mismatched event (continued)**

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

## AP WLAN oversubscribed

**TABLE 166 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 wlangs. Only maximum wlan number of the AP can be deployed
Description	This event occurs when the AP exceeds the maximum capacity for deploying all WLANs.

## AP illegal to change country code

**TABLE 167 AP illegal to change country code event**

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

## AP configuration get failed

**TABLE 168 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}].

## Events Types

### AP Communication Events

**TABLE 168 AP configuration get failed event (continued)**

Event	AP configuration get failed
Description	This event occurs when the AP fails to get the configuration.

## Rogue AP

**TABLE 169 Rogue AP event**

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

## Rogue AP disappeared

**TABLE 170 Rogue AP disappeared event**

Event	Rogue AP disappeared
Event Type	maliciousRogueAPTimeout
Event Code	185
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Malicious rogue [{{rogueMac}}] detected by [{{apName&&apMac}}] goes away.
Description	This event occurs when the rogue AP disappears.

## Classified Rogue AP

**TABLE 171 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"="xxxxxxxx", "channel"="xx", "rogueType"="xxxx", "roguePolicyName"="xxxx", "rogueRuleName"="xxxx"
Displayed on the web interface	AP [{{apName&&apMac}}] has detected a rogue AP rogue AP[{{rogueMac}}] with SSID[{{ssid}}] on channel[{{channel}}] classified as [{{rogueType}}] because of rogue classification policy (policy[{{roguePolicyName}}], rule[{{rogueRuleName}}]).
Description	This event occurs when the AP detects a rogue AP(malicious/known) that is classified by configurable rogue policy and its rules.

## AP image signing failed

TABLE 172 AP image signing failed event

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

## Jamming attack

TABLE 173 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"="xxxx" "roguePolicyName"="xxxx" "rogueRuleName"="xxxx"
Displayed on the web interface	A jamming rogue AP[rogueMac] with SSID[ssid] is detected by [apName&&apMac] on channel[channel].
Description	This event occurs when an AP detects a radio jamming attack.

## Rogue client

TABLE 174 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.

## Events Types

### AP Communication Events

## Key gen fail

TABLE 175 Key gen fail event

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

## Key dis fail

TABLE 176 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.

## Key dis fail GTK

TABLE 177 Key dis fail GTK event

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

## wpaendec fail

TABLE 178 WpaEnDec fail event

Event	WpaEnDec fail
Event Type	wpaEnDecFail
Event Code	99003
Severity	Critical

**TABLE 178 WpaEnDec fail event (continued)**

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

## IPsecSes fail

**TABLE 179 IPsecSes fail event**

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

## Fw manual initiation

**TABLE 180 Fw manual initiation event**

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

## AP Management TSF data

**TABLE 181 AP Management TSF data event**

Event	AP Management TSF data
Event Type	APMGMNTTSFdata
Event Code	99010

## Events Types

### AP Communication Events

**TABLE 181 AP Management TSF data event (continued)**

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

## AP TSF failure

**TABLE 182 AP TSF failure event**

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

## AP Self tests

**TABLE 183 AP Self tests event**

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

## Firmware initiation update

**TABLE 184 Firmware initiation update event**

Event	Firmware initiation update
Event Type	FwInitiationUpdate
Event Code	99013
Severity	Informational



**TABLE 184** Firmware initiation update event (continued)

Event	Firmware initiation update
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.

## SSH initiation

**TABLE 185** 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.

## SSH termination

**TABLE 186** 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}].
Description	This event occurs whenever there is exit from established SSH session

## SSH failure

**TABLE 187** 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"

## Events Types

### AP Communication Events

**TABLE 187 SSH failure event (continued)**

Event	SSH failure
Displayed on the web interface	There SSH session initiation with failed authentication, AP: [{apMac}].
Description	This event occurs whenever there SSH session initiation with failed authentication.

## TLS initiation

**TABLE 188 TLS initiation event**

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

## TLS termination

**TABLE 189 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.

## TLS failure

**TABLE 190 TLS failure event**

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

## IP sec initiation

TABLE 191 IP sec initiation event

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

## IP sec termination

TABLE 192 IP sec termination event

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

## IP sec failure

TABLE 193 IP sec failure event

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

## AP LBS Events

Following are the events related to AP Location Based Service.

- [No LS responses](#) on page 108
- [LS authentication failure](#) on page 108
- [AP connected to LS](#) on page 108
- [AP failed to connect to LS](#) on page 109

**Events Types**  
AP LBS Events

- [AP started location service](#) on page 109
- [AP stopped location service](#) on page 109
- [AP received passive calibration request](#) on page 109
- [AP received passive footfall request](#) on page 110
- [AP received unrecognized request](#) on page 110

## No LS responses

**TABLE 194** No LS responses event

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

## LS authentication failure

**TABLE 195** LS authentication failure event

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

## AP connected to LS

**TABLE 196** AP connected to LS event

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

## AP failed to connect to LS

TABLE 197 AP failed to connect to LS event

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

## AP started location service

TABLE 198 AP started location service event

Event	AP started location service
Event Type	apLBSStartLocationService
Event Code	705
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "venue"=""
Displayed on the web interface	AP [{{apName&&apMac}} Start Ruckus Location Service: venue= [{{venue}}], band= [{{band}}]
Description	This event occurs when the AP starts to get the location data.

## AP stopped location service

TABLE 199 AP stopped location service event

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

## AP received passive calibration request

TABLE 200 AP received passive calibration request event

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

**TABLE 200 AP received passive calibration request event (continued)**

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

## AP received passive footfall request

**TABLE 201 AP received passive footfall request event**

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

## AP received unrecognized request

**TABLE 202 AP received unrecognized request event**

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

## AP Mesh Events

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

<a href="#">EMAP downlink connected to MAP on page 111</a>	<a href="#">EMAP downlink disconnected from MAP on page 111</a>	<a href="#">EMAP uplink connected to MAP on page 111</a>
<a href="#">EMAP uplink disconnected from MAP on page 112</a>	<a href="#">MAP disconnected on page 112</a>	<a href="#">MAP downlink connected on page 112</a>
<a href="#">MAP downlink connected to EMAP on page 112</a>	<a href="#">MAP downlink disconnected from EMAP on page 113</a>	<a href="#">RAP downlink connected to MAP on page 113</a>
<a href="#">MAP uplink connected to EMAP on page 113</a>	<a href="#">MAP uplink disconnected from EMAP on page 114</a>	<a href="#">MAP uplink connected to RAP on page 114</a>
<a href="#">MAP uplink connected to MAP on page 114</a>	<a href="#">Mesh state updated to MAP on page 114</a>	<a href="#">Mesh state updated to MAP no channel on page 115</a>

Mesh state updated to RAP on page 115	Mesh state update to RAP no channel on page 115	MAP downlink connected to MAP on page 116
MAP downlink disconnected from MAP on page 116	RAP downlink disconnected from MAP on page 116	

## EMAP downlink connected to MAP

TABLE 203 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 the mobile application part (MAP) to Ethernet Mesh AP (EMAP) connection is successful.

## EMAP downlink disconnected from MAP

TABLE 204 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 the MAP disconnects from EMAP.

## EMAP uplink connected to MAP

TABLE 205 EMAP uplink connected to MAP event

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

## EMAP uplink disconnected from MAP

TABLE 206 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 the EMAP uplink disconnects from MAP.

## MAP disconnected

TABLE 207 MAP disconnected event

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

## MAP downlink connected

TABLE 208 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 the MAP downlink connects to the AP.

## MAP downlink connected to EMAP

TABLE 209 MAP downlink connected to EMAP event

Event	MAP downlink connected to EMAP
Event Type	mapDlinkConnectWithMap
Event Code	413
Severity	Informational



**TABLE 209 MAP downlink connected to EMAP event (continued)**

Event	MAP downlink connected to EMAP
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 the MAP accepts the connection from Ethernet Mesh AP.

## MAP downlink disconnected from EMAP

**TABLE 210 MAP downlink disconnected from EMAP event**

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

## RAP downlink connected to MAP

**TABLE 211 RAP downlink connected to MAP event**

Event	RAP downlink connected to MAP
Event Type	rmapDlinkConnectWithMap
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 the MAP connection.

## MAP uplink connected to EMAP

**TABLE 212 MAP uplink connected to EMAP event**

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

## MAP uplink disconnected from EMAP

TABLE 213 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 the MAP disconnects from EMAP.

## MAP uplink connected to RAP

TABLE 214 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 the MAP connects to RAP with RSSI (across links).

## MAP uplink connected to MAP

TABLE 215 MAP uplink connected to MAP event

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

## Mesh state updated to MAP

TABLE 216 Mesh state updated to MAP event

Event	Mesh state updated to MAP
Event Type	meshStateUpdateToMap

**TABLE 216 Mesh state updated to MAP event (continued)**

Event	Mesh state updated to MAP
Event Code	421
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "mapMac"="xx:xx:xx:xx:xx:xx", "numHop"="x", "channel"="xx",  "downlinkState"="xx", "radio"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] uplinks to [{mapName&&mapMac}] across [{numHop}] hops on channel [{channel}] at [{radio}] with downlink [{downlinkState}]
Description	This event occurs when the AP is set to MAP uplinks across hops on channel radio (with downlink).

## Mesh state updated to MAP no channel

**TABLE 217 Mesh state updated to MAP no channel event**

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

## Mesh state updated to RAP

**TABLE 218 Mesh state updated to RAP event**

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

## Mesh state update to RAP no channel

**TABLE 219 Mesh state update to RAP no channel event**

Event	Mesh state update to RAP no channel
Event Type	meshStateUpdateToRapNoChannel

**TABLE 219** Mesh state update to RAP no channel event (continued)

Event	Mesh state update to RAP no channel
Event Code	424
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "downlinkState"="xx"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] with downlink [{downlinkState}]
Description	This event occurs when the AP is set to downlink.

## MAP downlink connected to MAP

**TABLE 220** MAP downlink connected to MAP event

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

## MAP downlink disconnected from MAP

**TABLE 221** MAP downlink disconnected from MAP event

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

## RAP downlink disconnected from MAP

**TABLE 222** RAP downlink disconnected from MAP event

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

## AP State Change Events

Following are the events related to access point state changes.

AP rebooted by user on page 117	AP rebooted by system on page 118	AP disconnected on page 118
AP IP address updated on page 118	AP reset to factory default on page 118	AP channel updated on page 119
AP country code updated on page 119	AP channel updated because dynamic frequency selection (DFS) detected a radar on page 119	AP change control plane on page 120
AP connected on page 120	AP deleted on page 120	AP heartbeat lost on page 121
AP tagged as critical on page 121	AP cable modem interface down on page 121	AP brownout on page 121
AP cable modem power-cycled by user on page 122	AP smart monitor turn off WLAN on page 122	AP client load balancing limit reached on page 122
AP client load balancing limit recovered on page 123	AP WLAN state changed on page 123	AP capacity reached on page 123
AP capacity recovered on page 124	AP cable modem interface up on page 124	AP cable modem soft-rebooted by user on page 124
AP cable modem set to factory default by user on page 125	AP health high latency flag on page 125	AP health low capacity flag on page 125
AP health high connection failure flag on page 126	AP health high client count flag on page 126	AP health high latency clear on page 126
AP health low capacity clear on page 127	AP health high connection failure clear on page 127	AP health high client count clear on page 127
Primary DHCP AP is down on page 128	Primary DHCP AP is up on page 128	Secondary DHCP AP is down on page 128
Secondary DHCP AP is up on page 129	Primary or secondary DHCP AP detects 90% of the configured total IPs on page 129	Both primary and secondary DHCP server APs are down on page 129
AP NAT gateway IP failover detected for particular VLAN pool on page 129	AP NAT gateway IP fall back detected for particular VLAN pool on page 130	NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool on page 130
NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up on page 131	AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down on page 131	AP health high airtime utilization flag on page 131
AP health high airtime utilization clear on page 132	AP cluster failover on page 132	AP cluster rehome on page 132
AP MAC OUI violation on page 133	Backhaul switched to primary on page 133	Backhaul switched to secondary on page 133
LTE network connectivity lost on page 134	Ethernet network connectivity lost on page 134	LTE DHCP timeout on page 134
Ethernet link down on page 134	Ethernet link up on page 135	SIM switch on page 135
Remote host blacklisted on page 135	SIM removal on page 136	LTE network registration status on page 136
LTE connection status on page 136	AP System Anomaly on page 136	Mesh network connectivity lost on page 137

## AP rebooted by user

TABLE 223 AP rebooted by user event

Event	AP rebooted by user
Event Type	apRebootByUser
Event Code	301
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "reason"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] rebooted because of [{reason}]
Description	This event occurs when AP reboots.

## Events Types

### AP State Change Events

## AP rebooted by system

TABLE 224 AP rebooted by system event

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

## AP disconnected

TABLE 225 AP disconnected event

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

## AP IP address updated

TABLE 226 AP IP address updated event

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

## AP reset to factory default

TABLE 227 AP reset to factory default event

Event	AP reset to factory default
Event Type	apFactoryReset
Event Code	305

**TABLE 227 AP reset to factory default event (continued)**

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

## AP channel updated

**TABLE 228 AP channel updated event**

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

## AP country code updated

**TABLE 229 AP country code updated event**

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

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

**TABLE 230 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

## Events Types

### AP State Change Events

**TABLE 230 AP channel updated because dynamic frequency selection (DFS) detected a radar event (continued)**

Event	AP channel updated because dynamic frequency selection (DFS) detected a radar
Description	This event occurs when the AP detects a radar burst on the radio and the channel moves to a non-occupancy mode.

## AP change control plane

**TABLE 231 AP change control plane event**

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

## AP connected

**TABLE 232 AP connected event**

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

## AP deleted

**TABLE 233 AP deleted event**

Event	AP deleted
Event Type	apDeleted (detected on the server)
Event Code	313
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	AP [{apName&&apMac}] deleted
Description	This event occurs when the AP is deleted on the server side.



## AP heartbeat lost

TABLE 234 AP heartbeat lost event

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

## AP tagged as critical

TABLE 235 AP tagged as critical event

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

## AP cable modem interface down

TABLE 236 AP cable modem interface down event

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

## AP brownout

TABLE 237 AP brownout event

Event	AP brownout
Event Type	apBrownout
Event Code	317

## Events Types

### AP State Change Events

**TABLE 237 AP brownout event (continued)**

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

## AP cable modem power-cycled by user

**TABLE 238 AP cable modem power-cycled by user event**

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

## AP smart monitor turn off WLAN

**TABLE 239 AP smart monitor turn off WLAN event**

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

## AP client load balancing limit reached

**TABLE 240 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]]

**TABLE 240 AP client load balancing limit reached event (continued)**

Event	AP client load balancing limit reached
Description	This event occurs when the AP reaches the client loading balance (CLB) limit. The adjacent threshold limit value is 50 for 2.4GHz radio and 43 for 5GHz radio.

## AP client load balancing limit recovered

**TABLE 241 AP client load balancing limit recovered event**

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

## AP WLAN state changed

**TABLE 242 AP WLAN state changed event**

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

## AP capacity reached

**TABLE 243 AP capacity reached event**

Event	AP capacity reached
Event Type	apCapacityReached
Event Code	323
Severity	Warning
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.

## Events Types

### AP State Change Events

**TABLE 243 AP capacity reached event (continued)**

Event	AP capacity reached
Description	This event occurs when an AP rejects a client due to the threshold limit reached by the client.

## AP capacity recovered

**TABLE 244 AP capacity recovered event**

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

## AP cable modem interface up

**TABLE 245 AP cable modem interface up event**

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

## AP cable modem soft-rebooted by user

**TABLE 246 AP cable modem soft-rebooted by user event**

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

## AP cable modem set to factory default by user

TABLE 247 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 CLI command.

## AP health high latency flag

TABLE 248 AP health high latency flag event

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

## AP health low capacity flag

TABLE 249 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.

## Events Types

### AP State Change Events

## AP health high connection failure flag

TABLE 250 AP health high connection failure flag event

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

## AP health high client count flag

TABLE 251 AP health high client count flag event

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

## AP health high latency clear

TABLE 252 AP health high latency clear event

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

## AP health low capacity clear

TABLE 253 AP health low capacity clear event

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

## AP health high connection failure clear

TABLE 254 AP health high connection failure clear event

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

## AP health high client count clear

TABLE 255 AP health high client count clear event

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

## Events Types

### AP State Change Events

## Primary DHCP AP is down

TABLE 256 Primary DHCP AP is down event

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

## Primary DHCP AP is up

TABLE 257 Primary DHCP AP is up event

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

## Secondary DHCP AP is down

TABLE 258 Secondary DHCP AP is down event

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



## Secondary DHCP AP is up

TABLE 259 Secondary DHCP AP is up event

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

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

TABLE 260 Primary or secondary DHCP AP detects 90% of the configured total IPs event

Event	Primary or secondary DHCP AP detects 90% of the configured total IPs
Event Type	apDHCIPIPPoolMaxThresholdReached
Event Code	340
Severity	Warning
Attribute	"zoneName"="ZoneName", "poolId"="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.

## Both primary and secondary DHCP server APs are down

TABLE 261 Both primary and secondary DHCP server APs are down event

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

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

TABLE 262 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

## Events Types

### AP State Change Events

**TABLE 262 AP NAT gateway IP failover detected for particular VLAN pool event (continued)**

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

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

**TABLE 263 AP NAT gateway IP fall back detected for particular VLAN pool event**

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

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

**TABLE 264 NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool event**

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

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

**TABLE 265 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"
Displayed on the web interface	NAT VLAN capacity restored detected by DHCP NAT AP [{apMac}] one of the NAT gateway IPs [{natGatewayIP}] is now up, out of three (3) consecutive NAT gateway IPs which were down. The NAT traffic for affected clients is restored back.
Description	This event occurs when the AP detects at least one of the three (3) consecutive gateway APs IPs that had failed is now UP.

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

**TABLE 266 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", "apMac2"="xx:xx:xx:xx:xx", "apMac3"="xx:xx:xx:xx:xx"
Displayed on the web interface	NAT failure detected by SZ since three (3) consecutive NAT gateway IPs are down AP1=[{apMac1}] AP2=[{apMac2}] AP3=[{apMac3}] (All consecutive NAT APs are down in case of less than 3 NAT Gateway APs configured). The NAT traffic for some of the clients may get affected for the respective VLANs.
Description	This event occurs when the controller detects three (3) consecutive failures of NAT server APs.

## AP health high airtime utilization flag

**TABLE 267 AP health high airtime utilization flag event**

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

## Events Types

### AP State Change Events

**TABLE 267 AP health high airtime utilization flag event (continued)**

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

## AP health high airtime utilization clear

**TABLE 268 AP health high airtime utilization clear event**

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

## AP cluster failover

**TABLE 269 AP cluster failover event**

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

## AP cluster rehome

**TABLE 270 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].

**TABLE 270 AP cluster rehome event (continued)**

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

## AP MAC OUI violation

**TABLE 271 AP MAC OUI violation**

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

## Backhaul switched to primary

**TABLE 272 Backhaul switched to primary event**

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

## Backhaul switched to secondary

**TABLE 273 Backhaul switched to secondary event**

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

## Events Types

### AP State Change Events

## LTE network connectivity lost

TABLE 274 LTE network connectivity lost event

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

## Ethernet network connectivity lost

TABLE 275 Ethernet network connectivity lost vent

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

## LTE DHCP timeout

TABLE 276 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.

## Ethernet link down

TABLE 277 Ethernet link down event

Event	Ethernet link down
Event Type	ethernetLinkDown
Event Code	9105
Severity	Informational

**TABLE 277 Ethernet link down event (continued)**

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

## Ethernet link up

**TABLE 278 Ethernet link up event**

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

## SIM switch

**TABLE 279 SIM switch event**

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

## Remote host blacklisted

**TABLE 280 Remote host blacklisted event**

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

## Events Types

### AP State Change Events

## SIM removal

TABLE 281 SIM removal event

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

## LTE network registration status

TABLE 282 LTE network registration status event

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

## LTE connection status

TABLE 283 LTE connection status event

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

## AP System Anomaly

TABLE 284 AP System Anomaly event

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



**TABLE 284 AP System Anomaly event (continued)**

Event	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 event is triggered when AP /writable partition is mounted as Read-Only

## Mesh network connectivity lost

**TABLE 285 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", currlface = "xxxxx", "apName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] Mesh network connectivity lost on [{currlface}]
Description	This event occurs when mesh network connectivity is lost.

## AP Authentication Events

Following are the events related to AP authentication.

- [Radius server reachable](#) on page 138
- [Radius server unreachable](#) on page 138
- [LDAP server reachable](#) on page 138
- [LDAP server unreachable](#) on page 139
- [AD server reachable](#) on page 139
- [AD server unreachable](#) on page 139
- [Wechat ESP authentication server reachable](#) on page 140
- [WeChat ESP authentication server unreachable](#) on page 140
- [WeChat ESP authentication server resolvable](#) on page 140
- [WeChat ESP authentication server unresolvable](#) on page 141
- [WeChat ESP DNAT server reachable](#) on page 141
- [WeChat ESP DNAT server unreachable](#) on page 141
- [WeChat ESP DNAT server resolvable](#) on page 142
- [WeChat ESP DNAT server unresolvable](#) on page 142
- [Authentication Attempts](#) on page 143
- [Authentication Unsuccessful](#) on page 143
- [Authentication Re-attempt](#) on page 143
- [Authentication 8021](#) on page 143
- [AP Local Session Timeout](#) on page 144

## Events Types

### AP Authentication Events

- [AP Remote Session Timeout](#) on page 144
- [AP Interactive Session Termination](#) on page 144

## Radius server reachable

TABLE 286 Radius server reachable event

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

## Radius server unreachable

TABLE 287 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 AP is unable to reach the RADIUS server.
Auto Clearance	This event triggers the alarm 2102, which is auto cleared by the event code 2101.

## LDAP server reachable

TABLE 288 LDAP server reachable event

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

**TABLE 288 LDAP server reachable event (continued)**

Event	LDAP server reachable
Description	This event occurs when the AP is able to reach the lightweight directory access protocol (LDAP) server successfully.

## LDAP server unreachable

**TABLE 289 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 the AP is unable to reach the LDAP server.
Auto Clearance	This event triggers the alarm 2122, which is auto cleared by the event code 2121.

## AD server reachable

**TABLE 290 AD server reachable event**

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

## AD server unreachable

**TABLE 291 AD server unreachable event**

Event	AD server unreachable
Event Type	adServerUnreachable
Event Code	2142
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""

## Events Types

### AP Authentication Events

**TABLE 291 AD server unreachable event (continued)**

Event	AD server unreachable
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].
Description	This event occurs when AP is unable able to reach the active directory.
Auto Clearance	This event triggers the alarm 2142, which is auto cleared by the event code 2141.

## Wechat ESP authentication server reachable

**TABLE 292 Wechat ESP authentication server reachable event**

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

## WeChat ESP authentication server unreachable

**TABLE 293 WeChat ESP authentication server unreachable event**

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

## WeChat ESP authentication server resolvable

**TABLE 294 WeChat ESP authentication server resolvable event**

Event	WeChat ESP authentication server resolvable
Event Type	espAuthServerResolvable
Event Code	2153
Severity	Informational

**TABLE 294 WeChat ESP authentication server resolvable event (continued)**

Event	WeChat ESP authentication 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 authentication server domain name [{dn}] to [{ip}] successfully.
Description	This event occurs when AP successfully resolves WeChat ESP authentication server domain name.

## WeChat ESP authentication server unresolvable

**TABLE 295 WeChat ESP authentication server unresolvable event**

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

## WeChat ESP DNAT server reachable

**TABLE 296 WeChat ESP DNAT server reachable event**

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

## WeChat ESP DNAT server unreachable

**TABLE 297 WeChat ESP DNAT server unreachable event**

Event	WeChat ESP DNAT server unreachable
Event Type	espDNATServerUnreachable

## Events Types

### AP Authentication Events

**TABLE 297 WeChat ESP DNAT server unreachable event (continued)**

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

## WeChat ESP DNAT server resolvable

**TABLE 298 WeChat ESP DNAT server resolvable event**

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

## WeChat ESP DNAT server unresolvable

**TABLE 299 WeChat ESP DNAT server unresolvable event**

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

## Authentication Attempts

TABLE 300 Authentication attempt event

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

## Authentication Unsuccessful

TABLE 301 Authentication unsuccessful event

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

## Authentication Re-attempt

TABLE 302 Authentication re-attempt event

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

## Authentication 8021

TABLE 303 Authentication 8021 client event

Event	Authentication Unsuccessful
Event Type	auth8021xClient
Event Code	99008

## Events Types

### AP Authentication Events

**TABLE 303 Authentication 8021 client event (continued)**

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

## AP Local Session Timeout

**TABLE 304 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.
Description	This event occurs when local AP session terminates due to session timeout.

## AP Remote Session Timeout

**TABLE 305 AP Remote session timeout event**

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

## AP Interactive Session Termination

**TABLE 306 AP Interactive Session Termination event**

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



## AP USB Events

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

- [AP USB software package downloaded](#) on page 145
- [AP USB software package download failed](#) on page 145

### AP USB software package downloaded

TABLE 307 AP USB software package downloaded event

Event	AP USB software package downloaded
Event Type	apUsbSoftwarePackageDownloaded
Event Code	370
Severity	Informational
Attribute	"apMac="xx:xx:xx:xx:xx:xx", "usbSoftwareName="19d2-fff5(v1.0)"
Displayed on the web interface	AP [{apName&&apMac}] downloaded USB software package [{usbSoftwareName}] successfully.
Description	This event occurs when AP successfully downloads its USB software package.

### AP USB software package download failed

TABLE 308 AP USB software package download failed event

Event	AP USB software package download failed
Event Type	apUsbSoftwarePackageDownloadFailed
Event Code	371
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx", usbSoftwareName="19d2-fff5(v1.0)"
Displayed on the web interface	AP [{apName&&apMac}] failed to download USB software package [{usbSoftwareName}]
Description	This event occurs when the AP fails to download its USB software package.

## Authentication Events

The following are the events related to authentication.

- [Authentication server not reachable](#) on page 146
- [Authentication failed over to secondary](#) on page 146
- [Authentication fallback to primary](#) on page 146
- [AD/LDAP connected successfully](#) on page 147
- [AD/LDAP connectivity failure](#) on page 147
- [Bind fails with AD/LDAP](#) on page 147
- [Bind success with LDAP, but unable to find clear text password for the user](#) on page 148
- [RADIUS fails to connect to AD NPS server](#) on page 148
- [RADIUS fails to authenticate with AD NPS server](#) on page 148

## Events Types

### Authentication Events

- [Successfully established the TLS tunnel with AD/LDAP](#) on page 149
- [Fails to establish TLS tunnel with AD/LDAP](#) on page 149
- [TLS Establishment Failed between SZ and external AAA Server](#) on page 149

## Authentication server not reachable

TABLE 309 Authentication server not reachable event

Event	Authentication server not reachable
Event Type	authSrvrNotReachable
Event Code	1601
Severity	Major
Attribute	"mynoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "authSrvrIp"="20.20.20.20" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the authentication fails since the primary or secondary servers is not reachable.

## Authentication failed over to secondary

TABLE 310 Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651
Severity	Major
Attribute	"mynoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SZMgmtIp"="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} [{SZMgmtIp}]
Description	This event occurs when the secondary authentication RADIUS server is available after the primary server becomes zombie or dead.

## Authentication fallback to primary

TABLE 311 Authentication fallback to primary event

Event	Authentication fallback to primary
Event Type	authFallbackToPrimary
Event Code	1652
Severity	Major
Attribute	"mynoid"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SZMgmtIp"="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} [{SZMgmtIp}]

**TABLE 311 Authentication fallback to primary event (continued)**

Event	Authentication fallback to primary
Description	This event occurs when the automatic fallback is enabled. The authentication failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.

## AD/LDAP connected successfully

**TABLE 312 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" "SZMgmtIp"="2.2.2.2", "desc"="Successful connection to AD/LDAP"
Displayed on the web interface	[[srcProcess]] Connect to AD/LDAP[[authSrvrIp]] successfully from SCG[[SZMgmtIp]]
Description	This event occurs when RADIUS connection to AD/LDAP server is successful.

## AD/LDAP connectivity failure

**TABLE 313 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", "SZMgmtIp"="2.2.2.2" "desc"="Connection to AD/LDAP fails"
Displayed on the web interface	[[srcProcess]] Connect to AD/LDAP[[authSrvrIp]] fails from SCG[[SZMgmtIp]]
Description	This event occurs when RADIUS fails to connect to AD/LDAP server.

## Bind fails with AD/LDAP

**TABLE 314 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" "SZMgmtIp"="2.2.2.2", "desc"="Bind to AD/LDAP fails"

## Events Types

### Authentication Events

**TABLE 314 Bind fails with AD/LDAP event (continued)**

Event	Bind fails with AD/LDAP
Displayed on the web interface	[[srcProcess]] Bind to AD/LDAP[[authSrvrIp]] fails from SCG[[SZMgmtIp]] for User[[userName]]
Description	This event occurs when RADIUS binding fails to AD/LDAP server.

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

**TABLE 315 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"  "SZMgmtIp"="2.2.2.2", "desc"= "Fail to find password"
Displayed on the web interface	[[srcProcess]] failed to find password from LDAP [[authSrvrIp]] for SCG[[SZMgmtIp]] for User[[userName]]
Description	This event occurs when binding is successful with LDAP using root credential but is unable to retrieve the clear text password for the user.

## RADIUS fails to connect to AD NPS server

**TABLE 316 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"  "SZMgmtIp"="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[[SZMgmtIp]]
Description	This event occurs when RADIUS fails to connect to AD NPS server.

## RADIUS fails to authenticate with AD NPS server

**TABLE 317 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

**TABLE 317 RADIUS fails to authenticate with AD NPS server event (continued)**

Event	RADIUS fails to authenticate with AD NPS server
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="RAC", "authSrvrIp"="1.1.1.1", "username"="testuser"  "SZMgmtIp"="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 [[SZMgmtIp]] for User[[userName]]
Description	This event occurs when RADIUS fails to authenticate with AD NPS server.

## Successfully established the TLS tunnel with AD/LDAP

**TABLE 318 Successfully established the TLS tunnel with AD/LDAP event**

Event	Successfully established the TLS tunnel with AD/LDAP
Event Type	racADNPSFailToAuthenticate
Event Code	1761
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12, "srcProcess"="radiusd", "authSrvrIp"="1.1.1.1", "authSrvrPort"="636" "SCGMgmtIp"="2.2.2.2", "desc"="Successfully established TLS Tunnel with LDAP/AD"
Displayed on the web interface	[[srcProcess]] Established the TLS connection with AD/LDAP[[authSrvrIp]] successfully from SCG[[SCGMgmtIp]]
Description	This event occurs when the TLS connection between the controller and AD/LDAP is successfully established.

## Fails to establish TLS tunnel with AD/LDAP

**TABLE 319 Fails to establish TLS tunnel with AD/LDAP event**

Event	Fails to establish TLS tunnel with AD/LDAP
Event Type	racADLDAPTLSFailed
Event Code	1762
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "mvnold"=12 "srcProcess"="radiusd", "authSrvrIp"="1.1.1.1" "authSrvrPort"="636", "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish TLS Tunnel with LDAP/AD"
Displayed on the web interface	[[srcProcess]] Establishes the TLS connection with AD/LDAP[[authSrvrIp]] fails from SCG[[SCGMgmtIp]]
Description	This event occurs when the TLS connection between the controller and AD/LDAP fails.
Auto Clearance	This event triggers the alarm 1762, which is auto cleared by the event code 1761.

## TLS Establishment Failed between SZ and external AAA Server

**TABLE 320 TLS Establishment Failed between SZ and external AAA Server event**

Event	TLS Establishment Failed between SZ and external AAA Server
Event Type	racTLSEstablishmentFailedBetweenSZandExternalAAAServer
Event Code	1763

**TABLE 320 TLS Establishment Failed between SZ and external AAA Server event (continued)**

Event	TLS Establishment Failed between SZ and external AAA Server
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish "
Displayed on the web interface	[[srcProcess]] Establishes the TLS connection fails between SZ and external AAA Server from SCG[[SCGMgmtIp]]
Description	This event is triggered when TLS connection between the controller and AD/LDAP fails.

## Authorization Events

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

- [DM received from AAA](#) on page 150
- [DM NACK sent to AAA](#) on page 151
- [DM sent to NAS](#) on page 151
- [DM NACK received from NAS](#) on page 151
- [CoA received from AAA](#) on page 152
- [CoA NACK sent to AAA](#) on page 152
- [CoA sent NAS](#) on page 152
- [CoA NAK received NAS](#) on page 153
- [CoA authorize only access reject](#) on page 153
- [CoA RWSG MWMSG notification failure](#) on page 153

## DM received from AAA

**TABLE 321 DM received from AAA event**

Event	DM received from AAA
Event Type	dmRcvdAAA
Event Code	1641
Severity	Debug
Attribute	"mynold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSvrIp"="7.7.7.7" "rmtRadSvrIp"="40.40.40.40" "{produce.short.name}MgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM received by RAC [[radSvrIp]] from AAA [[rmtRadSvrIp]] for [[userName]]
Description	This event occurs when the radio access controller (RAC) receives a disconnected message from the AAA server.

## DM NACK sent to AAA

TABLE 322 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" "radSrvrlp"="7.7.7.7" "rmtRadSrvrlp"="40.40.40.40" "SZMgmtlp"="2.2.2.2"
Displayed on the web interface	RADIUS DM NACK sent by RAC [{radSrvrlp}] to AAA [{rmtRadSrvrlp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected not acknowledged message to the AAA server.

## DM sent to NAS

TABLE 323 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" "radSrvrlp"="7.7.7.7" "naslp"="40.40.40.40" "SZMgmtlp"="2.2.2.2"
Displayed on the web interface	RADIUS DM sent to NAS [{rmtRadSrvrlp}] by RAC [{radSrvrlp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected message to the network access server [proxy of received disconnected message or the disconnected message as initiated by the controller].

## DM NACK received from NAS

TABLE 324 DM NACK received from NAS event

Event	DM NACK received from NAS
Event Type	dmNackRcvdNAS
Event Code	1644
Severity	Debug
Attribute	"mvnold"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrlp"="7.7.7.7" "naslp"="40.40.40.40" "SZMgmtlp"="2.2.2.2", "cause"=""
Displayed on the web interface	RADIUS DM NACK received by RAC [{radSrvrlp}] from NAS [{naslp}] for [{userName}]
Description	This event occurs when the radio access control receives disconnect message, which is not acknowledged from the NAS server.

## CoA received from AAA

TABLE 325 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" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA received by RAC [{radSrvrIp}] from AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control receives a change of authorization message from the AAA server.

## CoA NACK sent to AAA

TABLE 326 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" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control sends a change of authorization, not acknowledged to the AAA server.

## CoA sent NAS

TABLE 327 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" "radSrvrIp"="1.1.1.1" "nasIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA requests proxied/forwarded to NAS(AP) [{nasIp]}.
Description	This event occurs when the controller forwards/proxy of change of authorization to the NAS server.



## CoA NAK received NAS

TABLE 328 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" "radSrvrlp"="1.1.1.1" "nasIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA NAK received from NAS(AP) for forwarded/proxied CoA [{radSrvrlp}]
Description	This event occurs when a change of authorization, not acknowledged is received from the NAS server.

## CoA authorize only access reject

TABLE 329 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" "userName"="abc@xyz.com" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "SZMgmtIp"="2.2.2.2" "apType" = "" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "rmtRadSrvrlp"="40.40.40.40"
Displayed on the web interface	CoA Authorize Only unsuccessful for AAA Server [rmtRadSrvrlp] for UE [ueMacAddr]
Description	This event occurs when the change of authorization is rejected.

## CoA RWSG MWSG notification failure

TABLE 330 CoA RWSG MWSG notification failure event

Event	CoA RWSG MWSG notification failure
Event Type	coaRWSGMWSGNotifFailure
Event Code	1650
Severity	Major
Attribute	mvnold=12 "wlanId"=1 "zoneId"=10 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "userName"="abc@xyz.com" "realm"="wlan.mnc080.mcc405.3gppnetwork.org" "SZMgmtIp"="2.2.2.2" "apType" = "" "ueMacAddr"="aa:bb:cc:gg:hh:ii"
Displayed on the web interface	Session Modify MWSG-RWSG Notification Failure/No response received
Description	This event occurs when the change of authorization in RADIUS /metro wireless service gateway notification fails.

# Control and Data Plane Interface Events

Following are the events related to control and data plane events.

- [DP connected](#) on page 154
- [GtpManager \(DP\) disconnected](#) on page 154
- [Session updated at DP](#) on page 155
- [Session update at DP failed](#) on page 155
- [Session deleted at DP](#) on page 155
- [Session delete at DP failed](#) on page 156
- [C2d configuration failed](#) on page 156

## DP connected

TABLE 331 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" "ctrlBladelp"="1.1.1.1" "dataBladelp"="3.3.3.3" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	The connectivity between Control plane {{ctrlBladelp}} and Data plane {{dataBladelp}} is established at {produce.short.name} {{SZMgmtIp}}
Description	This event occurs when data plane successfully completes the configuration procedure.

## GtpManager (DP) disconnected

TABLE 332 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" "ctrlBladelp"="1.1.1.1" "dataBladelp"="3.3.3.3" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	The connectivity between Control plane {{ctrlBladelp}} and Data plane {{dataBladelp}} is lost at {produce.short.name} {{SZMgmtIp}}
Description	This event occurs when either the transmission control protocol connection is lost or when the control plane is unable to complete the configuration procedure.
Auto Clearance	This event triggers the alarm 1202, which is auto cleared by the event code 1201.

## Session updated at DP

TABLE 333 Session updated at DP event

Event	Session updated at DP
Event Type	sessUpdatedAtDblade
Event Code	1205
Severity	Debug
Attribute	"mvsidn"="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" "SZMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsidn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsidn}] has been updated at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the session updates the request (C-D-SESS-UPD-REQ) successfully.

## Session update at DP failed

TABLE 334 Session update at DP failed event

Event	Session update at DP failed
Event Type	sessUpdateErrAtDblade
Event Code	1206
Severity	Debug
Attribute	"mvsidn"="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", "{produce.short.name}MgmtIp"="2.2.2.2", "ueMacAddr"="aa:bb:cc:gg:hh:ii", "ueImsi"="12345", "ueMsidn"="98787"
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsidn}] has failed to update at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the session update request fails (C-D-SESS-UPD-REQ). This is either due to a request timeout or a failed response.

## Session deleted at DP

TABLE 335 Session deleted at DP event

Event	Session deleted at DP
Event Type	sessDeletedAtDblade
Event Code	1207
Severity	Debug
Attribute	"mvsidn"="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" "SZMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsidn"="98787"

**TABLE 335 Session deleted at DP event (continued)**

Event	Session deleted at DP
Displayed on the web interface	TTG/PDG session for UE with IMSI [{{ueImsi}}] and MSISDN [{{ueMsisdn}}] has been deleted from Data plane [{{dataBladelp}}] by Control plane [{{ctrlBladelp}}] at {produce.short.name} [{{SZMgmtlp}}]
Description	This event occurs when the session deletes request (C-D-SESS-DEL-REQ) is successfully acknowledged.

## Session delete at DP failed

**TABLE 336 Session delete at DP failed event**

Event	Session delete at DP failed
Event Type	sessDeleteErrAtDblade
Event Code	1208
Severity	Debug
Attribute	"mvsidn"="12" "wlanid"="1" "zoneid"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="realm sent by UE" "ctrlBladelp"="1.1.1.1" "dataBladelp"="3.3.3.3" "SZMgmtlp"="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 [{{dataBladelp}}] by Control plane [{{ctrlBladelp}}] at {produce.short.name} [{{SZMgmtlp}}]
Description	This event occurs when the session delete request (C-D-SESS-DEL-REQ) results in a timeout or a failed response.

## C2d configuration failed

**TABLE 337 C2d configuration failed event**

Event	C2d configuration failed
Event Type	c2dCfgFailed
Event Code	1209
Severity	Warning
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "ctrlBladelp"="1.1.1.1" "dataBladelp"="3.3.3.3" "SZMgmtlp"="2.2.2.2" "cause"="<what was configured>"
Displayed on the web interface	Configuration [{{cause}}] from Control plane [{{ctrlBladelp}}] failed to apply on Data plane [{{dataBladelp}}] at {produce.short.name} [{{SZMgmtlp}}]
Description	This event occurs when the configuration request (C-D-CFG-REQ) results in a timeout or a failed response.

## Client Events

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

- [Client authentication failed](#) on page 157
- [Client joined](#) on page 158
- [Client failed to join](#) on page 158

- [Client disconnected](#) on page 158
- [Client connection timed out](#) on page 159
- [Client authorization successfully](#) on page 159
- [Client authorization failed](#) on page 159
- [Client session expired](#) on page 160
- [Client roaming](#) on page 160
- [Client logged out](#) on page 160
- [Client roaming disconnected](#) on page 161
- [Client blocked](#) on page 161
- [Client grace period](#) on page 162
- [Onboarding registration succeeded](#) on page 162
- [Onboarding registration failed](#) on page 162
- [Remediation succeeded](#) on page 163
- [Remediation failed](#) on page 163
- [Force DHCP disconnected](#) on page 163
- [WDS device joined](#) on page 164
- [WDS device left](#) on page 164
- [Client is blocked because of barring UE rule](#) on page 164
- [Client is unblocked by barring UE rule](#) on page 165
- [Start CALEA mirroring client](#) on page 165
- [Stop CALEA mirroring client](#) on page 165
- [Wired client joined](#) on page 165
- [Wired client failed to join](#) on page 166
- [Wired client disconnected](#) on page 166
- [Wired client authorization successfully](#) on page 166
- [Wired client session expired](#) on page 167
- [Application identified](#) on page 167
- [Application denied](#) on page 167
- [URL filtering server unreachable](#) on page 168
- [URL filtering server reachable](#) on page 168
- [Packet spoofing detected](#) on page 169
- [Packet spoofing detected](#) on page 168
- [Packet spoofing detected](#) on page 169
- [Packet spoofing detected](#) on page 169

## Client authentication failed

TABLE 338 Client authentication failed event

Event	Client authentication failed
Event Type	clientAuthFailure

**TABLE 338 Client authentication failed event (continued)**

Event	Client authentication failed
Event Code	201
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join WLAN [{ssid}] from AP [{apName&&apMac}] due to authentication failure.
Description	This event occurs when the client fails to join WLAN on the AP due to an authentication failure.

## Client joined

**TABLE 339 Client joined event**

Event	Client joined
Event Type	clientJoin
Event Code	202
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] joined WLAN [{ssid}] from AP [{apName&&apMac}].
Description	This event occurs when the client session joins the WLAN on AP.

## Client failed to join

**TABLE 340 Client failed to join event**

Event	Client failed to join
Event Type	clientJoinFailure
Event Code	203
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join WLAN [{ssid}] from AP [{apName&&apMac}].
Description	This event occurs when the client fails to connect to the WLAN on the AP.

## Client disconnected

**TABLE 341 Client disconnected event**

Event	Client disconnected
Event Type	clientDisconnect
Event Code	204
Severity	Informational

**TABLE 341 Client disconnected event (continued)**

Event	Client disconnected
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] disconnected from WLAN [{ssid}] on AP [{apName&&apMac}]
Description	This event occurs when the client disconnects from WLAN on AP.

## Client connection timed out

**TABLE 342 Client connection timed out event**

Event	Client connection timed out
Event Type	clientInactivityTimeout
Event Code	205
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "userId"="uuid"
Displayed on the web interface	Remediation of type [{remediationType}] failed on client [{clientIP}   clientMac] for user [{userName}].
Description	This event occurs when client disconnects from WLAN on AP due to inactivity.

## Client authorization successfully

**TABLE 343 Client authorization successfully event**

Event	Client authorization successfully
Event Type	clientAuthorization
Event Code	206
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] of WLAN [{ssid}] from AP [{apName&&apMac}] was authorized.
Description	This event occurs when the client on WLAN AP is authorized.

## Client authorization failed

**TABLE 344 Client authorization failed event**

Event	Client authorization failed
Event Type	clientAuthorizationFailure

**TABLE 344 Client authorization failed event (continued)**

Event	Client authorization failed
Event Code	207
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x" "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] of WLAN [{ssid}] from AP [{apName}&&apMac] was not authorized.
Description	This event occurs when the client on WLAN AP authorization fails.

## Client session expired

**TABLE 345 Client session expired event**

Event	Client session expired
Event Type	clientSessionExpiration
Event Code	208
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "associationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="" "userId"="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] exceeded the session time limit. Session terminated.
Description	This event occurs when the client exceeds the session time limit resulting in a session termination.

## Client roaming

**TABLE 346 Client roaming event**

Event	Client roaming
Event Type	clientRoaming
Event Code	209
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x" "userId"="uuid"
Displayed on the web interface	AP [{apName}&&apMac] radio [{toRadio}] detected client [{userName}   IP   clientMac] in WLAN [{ssid}] roam from AP [{fromApName}&&fromApMac].
Description	This event occurs when the AP radio detects a client.

## Client logged out

**TABLE 347 Client logged out event**

Event	Client logged out
Event Type	clientSessionLogout



**TABLE 347 Client logged out event (continued)**

Event	Client logged out
Event Code	210
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "assoicationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="" "userId"="uuid"
Displayed on the web interface	Client [{userName   IP   clientMac}] session logout.
Description	This event occurs when a client session is logged out.

## Client roaming disconnected

**TABLE 348 Client roaming disconnected event**

Event	Client roaming disconnected
Event Type	smartRoamDisconnect
Event Code	218
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "assoicationTime"="600", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "apName"="", "apLocation"="", "username"="", "osType"="", "radio"="", "vlanId"="", "sessionDuration"="", "txBytes"="", "rxBytes"="", "rssi"="", "receivedSignalStrength"="", "apGps"="", "hostname"="", "encryption"="", "disconnectReason"="", "bssid"="", "ni_rx_rssi_cnt"="", "ni_rx_tot_cnt"="", "ns_rx_rssi_cnt"="", "ns_rx_tot_cnt"="", "ni_tx_xput_lo_cnt"="", "ni_tx_xput_lo_dur"="", "Instantaneous rssi"="", "Xput"="", "userId"="uuid"
Displayed on the web interface	Client [{userName   IP   clientMac}] disconnected from WLAN [{ssid}] on AP [{apName&&apMac}] due to SmartRoam policy.
Description	This event occurs when the client disconnects from the WLALN due to a smart roam policy.

## Client blocked

**TABLE 349 Client blocked event**

Event	Client blocked
Event Type	clientBlockByDeviceType
Event Code	219
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "deviceType"="xxxxx", "ssid"="xxxxx", "wlanId"="xxxxx",
Displayed on the web interface	Client [{clientMac}] was recognized as [{deviceType}], and blocked by a device policy in AP [{apMac}]
Description	This event occurs when a client is blocked by a device policy.

## Client grace period

TABLE 350 Client grace period event

Event	Client grace period
Event Type	clientGracePeriod
Event Code	220
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x"
Displayed on the web interface	Client [{userName}   {clientIP}   {clientMac}] reconnects WLAN [{ssid}] on AP [{apName}&&apMac}] within grace period. No additional authentication is required.
Description	This event occurs when the when the STA interface reconnects and authorizes due to the grace period.

## Onboarding registration succeeded

TABLE 351 Onboarding registration succeeded event

Event	Onboarding registration succeeded
Event Type	onboardingRegistrationSuccess
Event Code	221
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "wlanId"="xxxxx", "userName"="xxxxx", "clientIP"="x.x.x.x", "userId"="uuid", "apLocation"="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.

## Onboarding registration failed

TABLE 352 Onboarding registration failed event

Event	On boarding 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 on boarding registration fails.

## Remediation succeeded

TABLE 353 Remediation succeeded event

Event	Remediation succeeded
Event Type	remediationSuccess
Event Code	223
Severity	Informational
Attribute	"remediationType"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "userName"="xxxxx", "userId"="uuid", "reason"="xxxxx"
Displayed on the web interface	Remediation of type [[remediationType]] finished successfully on client [[clientIP   clientMac]] for user [[userName]].
Description	This event occurs when the client remediation is successful.

## Remediation failed

TABLE 354 Remediation failed event

Event	Remediation failed
Event Type	remediationFailure
Event Code	224
Severity	Informational
Attribute	"remediationType"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "userName"="xxxxx", "userId"="uuid"
Displayed on the web interface	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 remediation fails.

## Force DHCP disconnected

TABLE 355 Force DHCP disconnected event

Event	Force DHCP disconnected
Event Type	ForceDHCPDisconnect
Event Code	225
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "bssid"="", "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 dynamic host configuration protocol (DHCP).

## WDS device joined

TABLE 356 WDS device joined event

Event	WDS device joined
Event Type	wdsDeviceJoin
Event Code	226
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "wdsDeviceMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Device [{{wdsDeviceMac}}] sends traffic via Client [{{clientMac}}] in AP [{{apName&&apMac}}].
Description	This event occurs when a subscriber device joins the network provided by a Customer-Premises Equipment (CPE) of a client associated AP through a wireless distribution system (WDS) mode.

## WDS device left

TABLE 357 WDS device left event

Event	WDS device left
Event Type	wdsDeviceLeave
Event Code	227
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "wdsDeviceMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Device [{{wdsDeviceMac}}] stops traffic via Client [{{clientMac}}] in AP [{{apName&&apMac}}].
Description	This event occurs when a subscriber device leaves the network provided by a CPE client associated to an AP through WDS.

## Client is blocked because of barring UE rule

TABLE 358 Client is blocked because of barring UE rule event

Event	Client is blocked because of barring UE rule
Event Type	clientBlockByBarringUERule
Event Code	228
Severity	Informational
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 temporally blocked by the UE barring rule.

## Client is unblocked by barring UE rule

TABLE 359 Client is unblocked by barring UE rule event

Event	Client is unblocked by barring UE rule
Event Type	clientUnblockByBarringUERule
Event Code	229
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Client [clientMac] of WLAN [{ssid}] from AP [{apName&&apMac}] was unblocked
Description	This event occurs when a client is unblocked by the UE barring rule.

## Start CALEA mirroring client

TABLE 360 Start CALEA mirroring client event

Event	Start CALEA mirroring client
Event Type	caleaMirroringStart
Event Code	230
Severity	Informational
Attribute	"userName"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Start CALEA mirroring client [{userName}   IP   clientMac] on WLAN [{ssid}] from AP [{apName&&apMac}].
Description	This event occurs when CALEA is started for mirroring the client image.

## Stop CALEA mirroring client

TABLE 361 Stop CALEA mirroring client event

Event	Stop CALEA mirroring client
Event Type	caleaMirroringStop
Event Code	231
Severity	Informational
Attribute	"userName"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "authType"="xxxxx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	Stop CALEA mirroring client [{userName}   IP   clientMac] on WLAN [{ssid}] with authentication type [{authType}] from AP [{apName&&apMac}]. TxBytes[{txBytes}], RxBytes[{rxBytes}].
Description	This event occurs when CALEA stops mirroring the client image.

## Wired client joined

TABLE 362 Wired client joined event

Event	Wired client joined
Event Type	wiredClientJoin

**TABLE 362** Wired client joined event (continued)

Event	Wired client joined
Event Code	2802
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxxx", tenantUUID="xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx", apName="xxxx", vlanId="x"
Displayed on the web interface	Client [{userName}   IP   clientMac] joined LAN [{ethPort}] from AP [{apName}&&apMac}].
Description	This event occurs when a client joins the LAN AP.

## Wired client failed to join

**TABLE 363** Wired client failed to join event

Event	Wired client failed to join
Event Type	wiredClientJoinFailure
Event Code	2803
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxxx", userName="xxxxx", userId="uuid"
Displayed on the web interface	Client [{userName}   IP   clientMac] failed to join LAN [{ethPort}] from AP [{apName}&&apMac}].
Description	This event occurs when a client fails to join the LAN AP.

## Wired client disconnected

**TABLE 364** Wired client disconnected event

Event	Wired client disconnected
Event Type	wiredClientDisconnect
Event Code	2804
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxxx", tenantUUID="xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx", apName="xxxx", vlanId="x", rxBytes="x", txFrames="x", txBytes="x", disconnectTime="x", sessionDuration="x", disconnectReason="x"
Displayed on the web interface	Client [{userName}   IP   clientMac] disconnected from LAN [{ethPort}] on AP [{apName}&&apMac}].
Description	This event occurs when a client disconnect from the LAN AP.

## Wired client authorization successfully

**TABLE 365** Wired client authorization successfully event

Event	Wired client authorization successfully
Event Type	wiredClientAuthorization
Event Code	2806

**TABLE 365** Wired client authorization successfully event (continued)

Event	Wired client authorization successfully
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="xxx", tenantUUID="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", apName="xxx", vlanId="x", 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.

## Wired client session expired

**TABLE 366** Wired client session expired event

Event	Wired client session expired
Event Type	wiredClientSessionExpiration
Event Code	2808
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx", clientMac="xx:xx:xx:xx:xx:xx", ethProfileId="xxxxx", ethPort="x", iface="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.
Description	This event occurs when a client exceeds the session time limit, which results in a session termination.

## Application identified

**TABLE 367** Application identified event

Event	Application identified
Event Type	application of user is identified
Event Code	8001
Severity	Informational
Attribute	
Displayed on the web interface	APP[{APP}] identified from AP[{apMac}] for client [{STA_MAC}] with source[{SRC_IP}: {SRC_PORT}] destination[{DST_IP}:{DST_PORT}] Proto[{PROTO}]
Description	This event occurs when the user of the application is identified.

## Application denied

**TABLE 368** Application denied event

Event	Application denied
Event Type	application of user is denied
Event Code	8002
Severity	Informational

**TABLE 368** Application denied event (continued)

Event	Application denied
Attribute	
Displayed on the web interface	APP[{{APP}}] denied from AP[{{apMac}}] for client [{{STA_MAC}}] with source[{{SRC_IP}}:{{SRC_PORT}}] destination[{{DST_IP}}:{{DST_PORT}}] Proto[{{PROTO}}]
Description	This event occurs when the application of the user is denied.

## URL filtering server unreachable

**TABLE 369** URL filtering server unreachable event

Event	URL filtering server unreachable
Event Type	urlFilteringServerUnreachable
Event Code	8003
Severity	Major
Attribute	apMac = "xx:xx:xx:xx:xx:xx", serverUrl = "xxxxxx"
Displayed on the web interface	AP [{{apMac}}] cannot reach the URL Filtering server [{{serverUrl}}].
Description	This event occurs when URL filtering server is unreachable.

## URL filtering server reachable

**TABLE 370** URL filtering server reachable event

Event	URL filtering server reachable
Event Type	urlFilteringServerReachable
Event Code	8004
Severity	Major
Attribute	apMac = "xx:xx:xx:xx:xx:xx", serverUrl = "xxxxxx"
Displayed on the web interface	AP [{{apMac}}] can reach the URL Filtering server [{{serverUrl}}].
Description	This event occurs when URL filtering server is reachable.

## Packet spoofing detected

**TABLE 371** Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWireless
Event Code	232
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "ssid"="xxxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{{desc}}] from client [{{clientMac&&clientIP}}] on WLAN [{{ssid}}] [{{networkInterface}}] from AP [{{apName&&apMac}}]
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature.



## Packet spoofing detected

TABLE 372 Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWirelessSourceMacSpoofed
Event Code	233
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "ssid"="xxxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{{desc}}], packets [{{packetDropCount}}] were dropped on WLAN [{{ssid}}] [{{networkInterface}}] from AP [{{apName&&apMac}}]
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature. It is a source MAC address spoof.

## Packet spoofing detected

TABLE 373 Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWired
Event Code	234
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{{desc}}] from client [{{clientMac&&clientIP}}] on [{{networkInterface}}] from AP [{{apName&&apMac}}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature.

## Packet spoofing detected

TABLE 374 Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWiredSourceMacSpoofed
Event Code	235
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "networkInterface" = "xxxxxx", "apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{{desc}}], packets [{{packetDropCount}}] were dropped on [{{networkInterface}}] from AP [{{apName&&apMac}}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature. It is a source MAC address spoof.

## Cloud Events

The following are the events related to Cloud Based Service.

- [Cloud Services Enabled](#) on page 170
- [Cloud Services Disabled](#) on page 170
- [Cloud Analytics Enabled](#) on page 170
- [Cloud Analytics Disabled](#) on page 171
- [Cloud Services Token Refreshed](#) on page 171
- [Cloud Analytics Token Renewed](#) on page 171

## Cloud Services Enabled

TABLE 375 Cloud services enabled event

Event	Cloud services enabled
Event Type	CloudServicesEnabled
Event Code	4501
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services have been enabled successfully.
Description	This event occurs when the controller successfully enables the Cloud Services.

## Cloud Services Disabled

TABLE 376 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.
Description	This event occurs when controller successfully disables the Cloud Services.

## Cloud Analytics Enabled

TABLE 377 Cloud analytics enabled event

Event	Cloud analytics enabled
Event Type	CloudAnalyticsEnabled
Event Code	4503
Severity	Informational
Attribute	No attribute for this event.

**TABLE 377** Cloud analytics enabled event (continued)

Event	Cloud analytics enabled
Displayed on the web interface	Cloud Analytics service has been enabled successfully.
Description	This event occurs when the controller successfully enables Cloud Analytics service.

## Cloud Analytics Disabled

**TABLE 378** Cloud analytics disabled event

Event	Cloud analytics disabled
Event Type	CloudAnalyticsDisabled
Event Code	4504
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics service has been disabled successfully.
Description	This event occurs when the controller successfully disables Cloud Analytics service.

## Cloud Services Token Refreshed

**TABLE 379** Cloud services token refreshed event

Event	Cloud services token refreshed
Event Type	CloudServicesTokenRefreshed
Event Code	4601
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services token has been refreshed successfully.
Description	This event occurs when the controller successfully refreshes the Cloud Services access token.

## Cloud Analytics Token Renewed

**TABLE 380** Cloud analytics token renewed event

Event	Cloud analytics token renewed
Event Type	cloudAnalyticsTokenRenewed
Event Code	4602
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics token has been renewed successfully.
Description	This event occurs when the controller successfully renews Cloud Analytics access token.

## Cloud Analytics Disconnected

TABLE 381 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.

## Cluster Events

Following are the events related to clusters.

<a href="#">Cluster created successfully</a> on page 173	<a href="#">New node joined successfully</a> on page 173	<a href="#">New node failed to join</a> on page 173
<a href="#">Node removal completed</a> on page 174	<a href="#">Node removal failed</a> on page 174	<a href="#">Node out of service</a> on page 174
<a href="#">Cluster in maintenance state</a> on page 174	<a href="#">Cluster back in service</a> on page 175	<a href="#">Cluster backup completed</a> on page 175
<a href="#">Cluster backup failed</a> on page 175	<a href="#">Cluster restore completed</a> on page 176	<a href="#">Cluster restore failed</a> on page 176
<a href="#">Cluster node upgrade completed</a> on page 176	<a href="#">Entire cluster upgraded successfully</a> on page 177	<a href="#">Cluster upgrade failed</a> on page 177
<a href="#">Cluster application stopped</a> on page 177	<a href="#">Cluster application started</a> on page 177	<a href="#">Cluster backup started</a> on page 178
<a href="#">Cluster upgrade started</a> on page 178	<a href="#">Cluster leader changed</a> on page 178	<a href="#">Node bond interface down</a> on page 179
<a href="#">Node bond interface up</a> on page 179	<a href="#">Node IP address changed</a> on page 179	<a href="#">Node physical interface down</a> on page 179
<a href="#">Node physical interface up</a> on page 180	<a href="#">Cluster node rebooted</a> on page 180	<a href="#">NTP time synchronized</a> on page 180
<a href="#">Cluster node shutdown</a> on page 181	<a href="#">Cluster upload started</a> on page 181	<a href="#">Cluster upload completed</a> on page 181
<a href="#">Cluster upload failed</a> on page 182	<a href="#">SSH tunnel switched</a> on page 182	<a href="#">Cluster remove node started</a> on page 182
<a href="#">Node back in service</a> on page 182	<a href="#">Resync NTP time</a> on page 183	<a href="#">Disk usage exceed threshold</a> on page 183
<a href="#">Cluster out of service</a> on page 183	<a href="#">Initiated moving APs in node to a new cluster</a> on page 184	<a href="#">Cluster upload vSZ-D firmware started</a> on page 184
<a href="#">Cluster upload vSZ-D firmware completed</a> on page 184	<a href="#">Cluster upload vSZ-D firmware failed</a> on page 185	<a href="#">Cluster upload AP firmware started</a> on page 185
<a href="#">Cluster upload AP firmware completed</a> on page 185	<a href="#">Cluster upload AP firmware failed</a> on page 185	<a href="#">Cluster add AP firmware started</a> on page 186
<a href="#">Cluster add AP firmware completed</a> on page 186	<a href="#">Cluster add AP firmware failed</a> on page 186	<a href="#">Cluster name is changed</a> on page 187
<a href="#">Unsync NTP Time</a> on page 187	<a href="#">Cluster upload KSP file started</a> on page 187	<a href="#">Cluster upload KSP file completed</a> on page 188
<a href="#">Cluster upload KSP file failed</a> on page 188	<a href="#">NTP unreachable server</a> on page 188	<a href="#">Configuration backup started</a> on page 188
<a href="#">Configuration backup succeeded</a> on page 189	<a href="#">Configuration backup failed</a> on page 189	<a href="#">Configuration restore succeeded</a> on page 189
<a href="#">Configuration restore failed</a> on page 190	<a href="#">AP Certificate Expired</a> on page 190	<a href="#">AP Certificate Updated</a> on page 190
<a href="#">Configuration restore started</a> on page 190	<a href="#">Upgrade SSTable failed</a> on page 191	<a href="#">Reindex elastic search finished</a> on page 191
<a href="#">Initiated APs contact APR</a> on page 191	<a href="#">All nodes back in service</a> on page 192	<a href="#">Not management service ready</a> on page 192
<a href="#">Management service ready</a> on page 192	<a href="#">Management service ready</a> on page 192	<a href="#">Configuration sync failed</a> on page 192
<a href="#">Node IPv6 address added</a> on page 193	<a href="#">Node IPv6 address deleted</a> on page 193	<a href="#">AP is connected to standby cluster over the expiration date</a> on page 193
<a href="#">Sync Configuration Success for Cluster Redundancy</a> on page 196	<a href="#">Standby Cluster Restores a Configuration for Cluster Redundancy</a> on page 196	<a href="#">Standby Cluster Back to Monitoring Mode for Cluster Redundancy</a> on page 194

Standby Cluster Restored a Configuration Success for Cluster Redundancy on page 194	AP Connected to Standby Cluster after Rehome Timeout on page 195	External DP Connected to Standby Cluster after Rehome Timeout on page 195
Sync Configuration started for Cluster Redundancy on page 195	Standby Cluster Restored a Configuration Success for Cluster Redundancy on page 194	Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy on page 196
Sync Configuration Success for Cluster Redundancy on page 196		

## Cluster created successfully

TABLE 382 Cluster created successfully event

Event	Cluster created successfully
Event Type	clusterCreatedSuccess
Event Code	801
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Cluster [{clusterName}] created with node [{nodeName}]
Description	This event occurs when a cluster and a node are created.

## New node joined successfully

TABLE 383 New node joined successfully event

Event	New node joined successfully
Event Type	newNodeJoinSuccess
Event Code	802
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	New node [{nodeName}] joined cluster [{clusterName}]
Description	This event occurs when a node joins a cluster session.

## New node failed to join

TABLE 384 New node failed to join event

Event	New node failed to join
Event Type	newNodeJoinFailed
Event Code	803
Severity	Critical
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	New node [{nodeName}] failed to join cluster [{clusterName}]
Description	This event occurs when a node fails to join a cluster session. The controller web Interface displays the error message.
Auto Clearance	This event triggers the alarm 801, which is auto cleared by the event code 802.

## Node removal completed

TABLE 385 Node removal completed event

Event	Node removal completed
Event Type	removeNodeSuccess
Event Code	804
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] removed from cluster [{clusterName}]
Description	This event occurs when a node is removed from the cluster session.

## Node removal failed

TABLE 386 Node removal failed event

Event	Node removal failed
Event Type	removeNodeFailed
Event Code	805
Severity	Major
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] failed to remove from cluster [{clusterName}].
Description	This event occurs when a node cannot be removed from the cluster.
Auto Clearance	This event triggers the alarm 802, which is auto cleared by the event code 804.

## Node out of service

TABLE 387 Node out of service event

Event	Node out of service
Event Type	nodeOutOfService
Event Code	806
Severity	Critical
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service. Reason [{reason}].
Description	This event occurs when a node is out of service.
Auto Clearance	This event triggers the alarm 803, which is auto cleared by the event code 835.

## Cluster in maintenance state

TABLE 388 Cluster in maintenance state event

Event	Cluster in maintenance state
Event Type	clusterInMaintenanceState

**TABLE 388 Cluster in maintenance state event (continued)**

Event	Cluster in maintenance state
Event Code	807
Severity	Critical
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}} is in maintenance state
Description	This event occurs when a node is in a maintenance state.
Auto Clearance	This event triggers the alarm 804, which is auto cleared by the event code 808.

## Cluster back in service

**TABLE 389 Cluster back in service event**

Event	Cluster back in service
Event Type	clusterBackToInService
Event Code	808
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	{{clusterName}} is now in service
Description	This event occurs when a cluster is back in service.

## Cluster backup completed

**TABLE 390 Cluster backup completed event**

Event	Cluster backup completed
Event Type	backupClusterSuccess
Event Code	809
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} backup completed
Description	This event occurs when a cluster backup is complete.

## Cluster backup failed

**TABLE 391 Cluster backup failed event**

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} backup failed. Reason {{reason}}.

**TABLE 391 Cluster backup failed event (continued)**

Event	Cluster backup failed
Description	This event occurs when a cluster backup fails.
Auto Clearance	This event triggers the alarm 805, which is auto cleared by the event code 809.

## Cluster restore completed

**TABLE 392 Cluster restore completed event**

Event	Cluster restore completed
Event Type	restoreClusterSuccess
Event Code	811
Severity	Informational
Attribute	"nodeName"="xxx", "clusterName"="xxx",
Displayed on the web interface	Node [nodeName] in cluster [clusterName] restore completed
Description	This event occurs when restoration of a node to a cluster is successful.

## Cluster restore failed

**TABLE 393 Cluster restore failed event**

Event	Cluster restore failed
Event Type	restoreClusterFailed
Event Code	812
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [clusterName] restore failed. Reason [reason].
Description	This event occurs when restoration of a node in a cluster fails.
Auto Clearance	This event triggers the alarm 806, which is auto cleared by the event code 811.

## Cluster node upgrade completed

**TABLE 394 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", "fromVersion"="x.x", "toVersion"="x.x"
Displayed on the web interface	Node [nodeName] in cluster [clusterName] upgraded from [fromVersion] to [toVersion]
Description	This event occurs when version upgrade of a node is successful.



## Entire cluster upgraded successfully

**TABLE 395** Entire cluster upgraded successfully event

Event	Entire cluster upgraded successfully
Event Type	upgradeEntireClusterSuccess
Event Code	814
Severity	Informational
Attribute	clusterName="xxx", "fromVersion"="x.x", "toVersion"="x.x"
Displayed on the web interface	Cluster {{clusterName}} upgraded from {{fromVersion}} to {{toVersion}}.
Description	This event occurs when version upgrade of a cluster is successful.

## Cluster upgrade failed

**TABLE 396** 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}} Reason {{reason}}.
Description	This event occurs when the version upgrade of a cluster fails.
Auto Clearance	This event triggers the alarm 807, which is auto cleared by the event code 814.

## Cluster application stopped

**TABLE 397** Cluster application stopped event

Event	Cluster application stopped
Event Type	clusterAppStop
Event Code	816
Severity	Critical
Attribute	"appName"="xxxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Application {{appName}} on node {{nodeName}} stopped
Description	This event occurs when an application on node is stopped.
Auto Clearance	This event triggers the alarm 808, which is auto cleared by the event code 817.

## Cluster application started

**TABLE 398** Cluster application started event

Event	Cluster application started
Event Type	clusterAppStart

**TABLE 398** Cluster application started event (continued)

Event	Cluster application started
Event Code	817
Severity	Informational
Attribute	"appName"="xxxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Application [[appName]] on node [[nodeName]] started
Description	This event occurs when an application on node starts.

## Cluster backup started

**TABLE 399** Cluster backup started event

Event	Cluster backup started
Event Type	clusterBackupStart
Event Code	818
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Starting backup in cluster[[clusterName]]...
Description	This event occurs when a backup for a node commences.

## Cluster upgrade started

**TABLE 400** Cluster upgrade started event

Event	Cluster upgrade started
Event Type	clusterUpgradeStart
Event Code	819
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Starting upgrade in cluster[[clusterName]]...
Description	This event occurs when an upgrade for a node commences.

## Cluster leader changed

**TABLE 401** Cluster leader changed event

Event	Cluster leader changed
Event Type	clusterLeaderChanged
Event Code	820
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Node [[nodeName]] in cluster [[clusterName]] promoted to leader
Description	This event occurs when a node is changed to a lead node.

## Node bond interface down

TABLE 402 Node bond interface down event

Event	Node bond interface down
Event Type	nodeBondInterfaceDown
Event Code	821
Severity	Major
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 down.
Description	This event occurs when the network interface of a node is down.
Auto Clearance	This event triggers the alarm 809, which is auto cleared by the event code 822.

## Node bond interface up

TABLE 403 Node bond interface up event

Event	Node bond interface up
Event Type	nodeBondInterfaceUp
Event Code	822
Severity	Informational
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Network interface [{networkInterface}   {ifName}] on node [{nodeName}] is up.
Description	This event occurs when the network interface of a node is up.

## Node IP address changed

TABLE 404 Node IP address changed event

Event	Node IP address changed
Event Type	nodeIPChanged
Event Code	823
Severity	Informational
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx", "ip"="xxx.xxx.xxx.xxx"
Displayed on the web interface	IP address of network interface [{networkInterface}   {ifName}] on node [{nodeName}] changed to [{ip}].
Description	This event occurs when the node's network interface IP address changes.

## Node physical interface down

TABLE 405 Node physical interface down event

Event	Node physical interface down
Event Type	nodePhyInterfaceDown
Event Code	824

**TABLE 405 Node physical interface down event (continued)**

Event	Node physical interface down
Severity	Critical
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Physical network interface [{networkInterface}   {ifName}] on node [{nodeName}] is down.
Description	This event occurs when the node's physical interface is down.
Auto Clearance	This event triggers the alarm 810, which is auto cleared by the event code 825.

## Node physical interface up

**TABLE 406 Node physical interface up event**

Event	Node physical interface up
Event Type	nodePhyInterfaceUp
Event Code	825
Severity	Informational
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 up.
Description	This event occurs when the node's physical interface is up.

## Cluster node rebooted

**TABLE 407 Cluster node rebooted event**

Event	Cluster node rebooted
Event Type	nodeRebooted
Event Code	826
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "clusterName"="xxx",
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] rebooted
Description	This event occurs when the node, belonging to a cluster reboots.

## NTP time synchronized

**TABLE 408 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

**TABLE 408 NTP time synchronized event (continued)**

Event	NTP time synchronized
Description	This event occurs when the date and time settings of a node synchronizes with the NTP server.

## Cluster node shutdown

**TABLE 409 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 "
Displayed on the web interface	Node [{nodeName}] has been shut down
Description	This event occurs when the node is shut down.
Auto Clearance	This event triggers the alarm 813, which is auto cleared by the event code 826.

## Cluster upload started

**TABLE 410 Cluster upload started event**

Event	Cluster upload started
Event Type	clusterUploadStart
Event Code	830
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting upload in cluster [{clusterName}].
Description	This event occurs when the cluster upload process starts.

## Cluster upload completed

**TABLE 411 Cluster upload completed event**

Event	Cluster upload completed
Event Type	uploadClusterSuccess
Event Code	831
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] upload completed
Description	This event occurs when the cluster upload process is successful.

## Cluster upload failed

TABLE 412 Cluster upload failed event

Event	Cluster upload failed
Event Type	uploadClusterFailed
Event Code	832
Severity	Major
Attribute	"clusterName"="xxx", "reason"="xxx"
Displayed on the web interface	Cluster [{clusterName}] upload failed. Reason [{reason}]
Description	This event occurs when the cluster upload process fails.

## SSH tunnel switched

TABLE 413 SSH tunnel switched event

Event	SSH tunnel switched
Event Type	sshTunnelSwitched
Event Code	833
Severity	Major
Attribute	"clusterName"="xx", "nodeName"="xx", "nodeMac"="xx.xx.xx.xx.xx", "wsgMgmtIp"="xx.xx.xx.xx", "status"="ON->OFF", "sourceBladeUUID"="054ee469"
Displayed on the web interface	Node [{nodeName}] SSH tunnel switched [{status}]
Description	This event occurs when the SSH tunnel is switched.

## Cluster remove node started

TABLE 414 Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834
Severity	Informational
Attribute	"clusterName"="xxx", "nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Start to remove node [{nodeName}] from cluster [{clusterName}]
Description	This event occurs when the node start is removed.

## Node back in service

TABLE 415 Node back in service event

Event	Node back in service
Event Type	nodeBackToInService
Event Code	835
Severity	Informational

**TABLE 415 Node back in service event (continued)**

Event	Node back in service
Attribute	"clusterName"="xx", "nodeName"="xxx", "nodeMac"="xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is in service
Description	This event occurs when a node status changes to 'in service'.

## Resync NTP time

**TABLE 416 Resync NTP time event**

Event	Resync NTP time
Event Type	resyncNTPTime
Event Code	837
Severity	Major
Attribute	"nodeName"="xx", "status"="xx"
Displayed on the web interface	Node [{nodeName}] resyncs time from [{reason}]. The time difference is [{status}] seconds.
Description	This event occurs when cluster time is not synchronized.

## Disk usage exceed threshold

**TABLE 417 Disk usage exceed threshold event**

Event	Disk usage exceed threshold
Event Type	diskUsageExceed
Event Code	838
Severity	Critical
Attribute	"nodeName"="xx", "status"="xx"
Displayed on the web interface	The disk usage of node [{nodeName}] is over {status}%.
Description	This event occurs when the disk usage exceeds the threshold limit of 96%. For event 838, the threshold is 95%.

## Cluster out of service

**TABLE 418 Cluster out of service event**

Event	Cluster out of service
Event Type	clusterOutOfService
Event Code	843
Severity	Critical
Attribute	"clusterName"="xx"
Displayed on the web interface	Cluster [{clusterName}] is out of service.
Description	This event occurs when the cluster is out of service.
Auto Clearance	This event triggers the alarm 843, which is auto cleared by the event code 808.

## Initiated moving APs in node to a new cluster

TABLE 419 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 SZ.

## Cluster upload vSZ-D firmware started

TABLE 420 Cluster upload vSZ-D firmware started event

Event	Cluster upload vSZ-D firmware started
Event Type	clusterUploadVDPFirmwareStart
Event Code	845
Severity	Informational
Attribute	"clusterName"="xx"
Displayed on the web interface	Starting upload vSZ-D firmware in cluster {{clusterName}}
Description	This event occurs when the cluster starts and uploads vSZ-data plane firmware.

## Cluster upload vSZ-D firmware completed

TABLE 421 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"
Displayed on the web interface	Cluster {{clusterName}} upload vSZ-D firmware completed. {{status}}
Description	This event occurs when the cluster upload process of vSZ-data plane firmware is successful.



## Cluster upload vSZ-D firmware failed

TABLE 422 Cluster upload vSZ-D firmware failed event

Event	Cluster upload vSZ-D firmware failed
Event Type	uploadClusterVDPFirmwareFailed
Event Code	847
Severity	Informational
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload vSZ-D firmware failed. Reason:{{reason}}.
Description	This event occurs when the cluster upload process of vSZ-data plane firmware fails.

## Cluster upload AP firmware started

TABLE 423 Cluster upload AP firmware started event

Event	Cluster upload AP firmware started
Event Type	clusterUploadAPFirmwareStart
Event Code	848
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting upload AP firmware in cluster {{clusterName}}
Description	This event occurs when the cluster upload process to the AP firmware starts.

## Cluster upload AP firmware completed

TABLE 424 Cluster upload AP firmware completed event

Event	Cluster upload AP firmware completed
Event Type	clusterUploadAPFirmwareSuccess
Event Code	849
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} upload AP firmware completed.
Description	This event occurs when the cluster upload process to the AP firmware is successful.

## Cluster upload AP firmware failed

TABLE 425 Cluster upload AP firmware failed event

Event	Cluster upload AP firmware failed
Event Type	clusterUploadAPFirmwareFailed
Event Code	850
Severity	Major

**TABLE 425 Cluster upload AP firmware failed event (continued)**

Event	Cluster upload AP firmware failed
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster [[clusterName]] upload AP firmware failed. Reason:{{reason}}.
Description	This event occurs when the cluster upload process to the AP firmware fails.

## Cluster add AP firmware started

**TABLE 426 Cluster add AP firmware started event**

Event	Cluster add AP firmware started
Event Type	clusterAddAPFirmwareStart
Event Code	851
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting add AP firmware in cluster [[clusterName]]
Description	This event occurs when the cluster add process to the AP firmware process starts.

## Cluster add AP firmware completed

**TABLE 427 Cluster add AP firmware completed event**

Event	Cluster add AP firmware completed
Event Type	clusterAddAPFirmwareSuccess
Event Code	852
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting add AP firmware in cluster [[clusterName]]
Description	This event occurs when the cluster add process to the AP firmware is successful.

## Cluster add AP firmware failed

**TABLE 428 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}}.
Description	This event occurs when the cluster add process to the AP firmware fails.

## Cluster name is changed

TABLE 429 Cluster name is changed event

Event	Cluster name is changed
Event Type	clusterNameChanged
Event Code	854
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster name is changed to {{clusterName}}
Description	<p>This event occurs when the cluster node name is modified. By enabling email and SNMP notification in the controller user interface (<b>Configuration &gt; System &gt; Event Management</b>) of the event, SNMP trap and email will be generated on successful cluster-name modification.</p> <p>Cluster name change will fail if any node in either a two, three or four node cluster is out of service. For example, if in a three node cluster, any one node is powered off or the Ethernet cable is unplugged, cluster name change will fail.</p>

## Unsync NTP Time

TABLE 430 Unsync NTP Time event

Event	Unsync NTP Time
Event Type	unsyncNTPTime
Event Code	855
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx", "status"="xxx"
Displayed on the web interface	Node {{nodeName}} time is not synchronized because of {{reason}}. The time difference is {{status}} seconds.
Description	This event occurs when the cluster time is not synchronized.

## Cluster upload KSP file started

TABLE 431 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.

## Cluster upload KSP file completed

TABLE 432 Cluster upload KSP file completed event

Event	Cluster upload KSP file completed
Event Type	clusterUploadKspFileSuccess
Event Code	857
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Starting upload KSP file in cluster {{clusterName}}
Description	This event occurs when the cluster uploads the <i>ksp</i> file successfully.

## Cluster upload KSP file failed

TABLE 433 Cluster upload KSP file failed event

Event	Cluster upload KSP file failed
Event Type	clusterUploadKspFileFailed
Event Code	858
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{ clusterName}} upload KSP file failed.
Description	This event occurs when the cluster fails to upload the <i>ksp</i> file.
Auto Clearance	This event triggers the alarm 858, which is auto cleared by the event code 857.

## NTP unreachable server

TABLE 434 NTP unreachable server

Event	NTP unreachable server
Event Type	NTP server reach failed
Event Code	859
Severity	Critical
Attribute	NTP server
Displayed on the web interface	System cannot reach NTP sever [NTP Server]
Description	This event occurs when system fails to reach the NTP server.

## Configuration backup started

TABLE 435 Configuration backup started event

Event	Configuration backup started
Event Type	clusterCfgBackupStart
Event Code	860

**TABLE 435 Configuration backup started event (continued)**

Event	Configuration backup started
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration backup is started.
Description	This event occurs when cluster configuration backup starts.

## Configuration backup succeeded

**TABLE 436 Configuration backup succeeded**

Event	Configuration backup succeeded
Event Type	clusterCfgBackupSuccess
Event Code	861
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration backup succeeded.
Description	This event occurs when cluster backup configuration is successful.

## Configuration backup failed

**TABLE 437 Configuration backup failed event**

Event	Configuration backup failed
Event Type	clusterCfgBackupFailed
Event Code	862
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration backup failed.
Description	This event occurs when backup configuration fails.
Auto Clearance	This event triggers the alarm 862, which is auto cleared by the event code 861.

## Configuration restore succeeded

**TABLE 438 Configuration restore succeeded event**

Event	Configuration restore succeeded
Event Type	clusterCfgRestoreSuccess
Event Code	863
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration restore succeeded.
Description	This event occurs when the cluster restore configuration is successful.

## Configuration restore failed

TABLE 439 Configuration restore failed event

Event	Configuration restore failed
Event Type	clusterCfgRestoreFailed
Event Code	864
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [[clusterName]] configuration restore failed.
Description	This event occurs when the restore configuration fails.
Auto Clearance	This event triggers the alarm 864, which is auto cleared by the event code 863.

## AP Certificate Expired

TABLE 440 AP Certificate Expired event

Event	AP Certificate Expired
Event Type	apCertificateExpire
Event Code	865
Severity	Critical
Attribute	"count"="XXX"
Displayed on the web interface	[[count]] APs need to update their certificates.
Description	This event occurs when the AP certificate expires.
Auto Clearance	This event triggers the alarm 865, which is auto cleared by the event code 866.

## AP Certificate Updated

TABLE 441 AP Certificate Updated event

Event	AP Certificate Updated
Event Type	apCertificateExpireClear
Event Code	866
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Clear AP certificate expiration alarm.
Description	This event occurs when the AP certificates are updated.

## Configuration restore started

TABLE 442 Configuration restore started event

Event	Configuration restore started
Event Type	clusterCfgRestoreStarted

**TABLE 442 Configuration restore started event (continued)**

Event	Configuration restore started
Event Code	867
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration restore started.
Description	This event occurs when the cluster configuration is restored.

## Upgrade SSTable failed

**TABLE 443 Upgrade SSTable failed event**

Event	Upgrade SSTable failed
Event Type	upgradeSSTableFailed
Event Code	868
Severity	Major
Attribute	"nodeName"="xxx"
Displayed on the web interface	Node [{nodeName}] upgrade SSTable failed.
Description	This event occurs when the upgrade to the SS table fails.

## Reindex elastic search finished

**TABLE 444 Reindex elastic search finished event**

Event	Reindex elastic search finished
Event Type	Reindex ElasticSearch finished
Event Code	869
Severity	Major
Attribute	
Displayed on the web interface	Reindex ElasticSearch finished.
Description	This event occurs when the re-index elastic search is completed.

## Initiated APs contact APR

**TABLE 445 Initiated APs contact APR event**

Event	Initiated APs contact APR
Event Type	clusterInitContactApr
Event Code	870
Severity	Major
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{ clusterName}] initiated APs contact APR
Description	This event occurs on receiving APs contact APR configuration command.

## All nodes back in service

TABLE 446 All nodes back in service event

Event	All nodes back in service
Event Type	allNodeBackToInService
Event Code	871
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	All nodes in cluster [{clusterName}] are back in service.
Description	This event occurs when all nodes are back in service.

## Not management service ready

TABLE 447 Not management service ready event

Event	Not management service ready
Event Type	allServiceOutOfService
Event Code	872
Severity	Informational
Attribute	"clusterName"="xx", "nodeName"="xx", "reason"="xxx"
Displayed on the web interface	Not all management services on Node [{nodeName}] in cluster [{clusterName}] are ready. Reason\:[{reason}].
Description	This event occurs when any applications of the node is down and the management service state is marked as out of service

## Management service ready

TABLE 448 Management service ready event

Event	Management service ready
Event Type	allServiceInService
Event Code	873
Severity	Informational
Attribute	"clusterName"="xx", "nodeName"="xx"
Displayed on the web interface	All management services on Node [{nodeName}] in cluster [{clusterName}] are ready
Description	This event occurs when all applications of the node is in service and the management service state is marked as in service.

## Configuration sync failed

TABLE 449 Configuration sync failed event

Event	Configuration sync failed
Event Type	clusterRedundancySyncCfgFailed
Event Code	874



**TABLE 449 Configuration sync failed event (continued)**

Event	Configuration sync failed
Severity	Major
Attribute	"clusterName"="xx", "reason"="xxx"
Displayed on the web interface	Cluster {{clusterName}} configuration sync failed. Reason: {{reason}}
Description	This event occurs when synchronization configuration fails in a cluster redundancy.

## Node IPv6 address added

**TABLE 450 Node IPv6 address added event**

Event	Node IPv6 address added
Event Type	nodeIPv6Added
Event Code	2501
Severity	Informational
Attribute	"nodeMac"="xxx", "ifName"=" xx:xx:xx:xx:xx:xx", "ip"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Network interface {{networkInterface   ifName}} on node {{nodeName}} added IPv6 address {{ip}}.
Description	This event occurs when the node adds the IPv6 address.

## Node IPv6 address deleted

**TABLE 451 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.

## AP is connected to standby cluster over the expiration date

**TABLE 452 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.

## Sync Configuration Failed for Cluster Redundancy

TABLE 453 Sync Configuration Failed for Cluster Redundancy

Event	Sync Configuration Failed for Cluster Redundancy
Event Type	SyncConfigurationFailedforClusterRedundancy
Event Code	874
Severity	Medium
Attribute	"count"="XXX"
Displayed on the web interface	{{count}} sync configuration failed for cluster redundancy.
Description	This event occurs when sync configuration is failed for cluster redundancy.

## Standby Cluster Failed to Restore a Configuration for Cluster Redundancy

TABLE 454 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.

## Standby Cluster Back to Monitoring Mode for Cluster Redundancy

TABLE 455 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.

## Standby Cluster Restored a Configuration Success for Cluster Redundancy

TABLE 456 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

**TABLE 456 Standby Cluster Restored a Configuration Success for Cluster Redundancy event (continued)**

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.

## AP Connected to Standby Cluster after Rehome Timeout

**TABLE 457 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.

## External DP Connected to Standby Cluster after Rehome Timeout

**TABLE 458 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.

## Sync Configuration started for Cluster Redundancy

**TABLE 459 Sync Configuration started for Cluster Redundancy Event**

Event	Sync Configuration started for Cluster Redundancy
Event Type	SyncCfgStartClusterRedundancy
Event Code	875
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [[clusterName]] sync configuration start for cluster redundancy.
Description	This event occurs when sync configuration start for cluster redundancy.

## Sync Configuration Success for Cluster Redundancy

**TABLE 460** Sync Configuration Success for Cluster Redundancy Event

Event	Sync Configuration Success for Cluster Redundancy
Event Type	SyncCfgSuccessClusterRedundancy
Event Code	876
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [[clusterName]] sync configuration success for cluster redundancy.
Description	This event occurs when sync configuration success for cluster redundancy.

## Standby Cluster Restores a Configuration for Cluster Redundancy

**TABLE 461** 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.

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

**TABLE 462** Active Cluster unable to Connect to other Active Clusters for Cluster Redundancy event

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

## Certificate is about to Expire

**TABLE 463** Certificate is about to Expire event

Event	Certificate is about to Expire
Event Type	certificateAboutToExpire
Event Code	890
Severity	Major

**TABLE 463 Certificate is about to Expire event (continued)**

Event	Certificate is about to Expire
Attribute	"certName"="xxx", days="x", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate [{certName}] is about to expire in [{days}] days ({expireDateTime})
Description	This event occurs when certificate is about to expire.

## Certificate is already Expired

**TABLE 464 Certificate is already Expired event**

Event	Certificate is already Expired
Event Type	certificateExpire
Event Code	891
Severity	Major
Attribute	"certName"="xxx", "expireDateTime"="xxxx/xx/xx xx:xx:xx"
Displayed on the web interface	Certificate is already expired
Description	This event occurs when certificate is already expired

## Result of Renew Certificate

**TABLE 465 Result of Renew Certificate event**

Event	Result of Renew Certificate
Event Type	certificateGenerateResult
Event Code	892
Severity	Major
Attribute	"certName"="xxx", "result"="xxx"
Displayed on the web interface	Result of renew certificate [{certName}] : {result}
Description	This event occurs to show the result of renew certificate

## Configuration Events

Following are events related to configuration.

- [Configuration updated](#) on page 198
- [Configuration update failed](#) on page 198
- [Configuration receive failed](#) on page 198
- [Incorrect flat file configuration](#) on page 199
- [Zone configuration preparation failed](#) on page 199
- [AP configuration generation failed](#) on page 199
- [End-of-life AP model detected](#) on page 200
- [VLAN configuration mismatch on non-DHCP/NAT WLAN](#) on page 200

- [VLAN configuration mismatch on a DHCP/NAT WLAN on page 200](#)

## Configuration updated

TABLE 466 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" "SZMgmtIp"="2.2.2.2" "cause"="detail of the configuration applied"
Displayed on the web interface	Configuration [{{cause}}] applied successfully in [{{processName}}] process at {produce.short.name} [{{SZMgmtIp}}]
Description	This event occurs when the configuration notification receiver (CNR) process successfully applies the configuration to the modules.

## Configuration update failed

TABLE 467 Configuration update failed event

Event	Configuration update failed
Event Type	cfgUpdFailed
Event Code	1008
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" , "srcProcess"="cnr" "realm"="NA" "processName"="aut" "SZMgmtIp"="x.x.x.x" "cause"="xx"
Displayed on the web interface	Failed to apply configuration [{{cause}}] in [{{processName}}] process at {produce.short.name} [{{SZMgmtIp}}].
Description	This event occurs when the CNR receives a negative acknowledgment when applying the configuration settings to the module. Possible cause is that a particular process/module is down.

## Configuration receive failed

TABLE 468 Configuration receive failed event

Event	Configuration receive failed
Event Type	cfgRcvFailed
Event Code	1009
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cnr" "realm"="NA" "SZMgmtIp"="2.2.2.2" "cause"= "mention the configuration that is not received properly"
Displayed on the web interface	Failed to fetch configuration [{{cause}}] by CNR in {produce.short.name} [{{SZMgmtIp}}].
Description	This event occurs when the CNR receives an error or negative acknowledgment/improper/incomplete information from the configuration change notifier (CCN).

## Incorrect flat file configuration

TABLE 469 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" "SZMgmtIp"="2.2.2.2" "cause"="mention the configuration that is not received properly" "file"="mention the config file name"
Displayed on the web interface	{{srcProcess}} detected an configuration parameter is incorrectly configured in file {{file}} at {produce.short.name} {{SZMgmtIp}}.
Description	This event occurs when any flat file configuration parameter is not semantically or syntactically correct.

## Zone configuration preparation failed

TABLE 470 Zone configuration preparation failed event

Event	Zone configuration preparation failed
Event Type	zoneCfgPrepareFailed
Event Code	1021
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone"
Displayed on the web interface	Failed to prepare zone {{zoneName}} configuration required by ap configuration generation
Description	This event occurs when the controller is unable to prepare a zone configuration required by the AP.

## AP configuration generation failed

TABLE 471 AP configuration generation failed event

Event	AP configuration generation failed
Event Type	apCfgGenFailed
Event Code	1022
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "apCfgGenFailedCount"="25"
Displayed on the web interface	Failed to generate configuration for {{apCfgGenFailedCount}} AP(s) under zone{{zoneName}}.
Description	This event occurs when the controller fails to generate the AP configuration under a particular zone.

## End-of-life AP model detected

TABLE 472 End-of-life AP model detected event

Event	End-of-life AP model detected
Event Type	cfgGenSkippedDueToEolAp
Event Code	1023
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90", "zoneName"="openZone", "model"="R300,T300"
Displayed on the web interface	Detected usage of end-of-life ap model(s)[{model}] while generating configuration for AP(s) under zone[{zoneName}]
Description	This event occurs when the controller detects the AP model's end-of-life under a certain zone.

## VLAN configuration mismatch on non-DHCP/NAT WLAN

TABLE 473 VLAN configuration mismatch on non-DHCP/NAT WLAN event

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN.
Event Type	apCfgNonDhcpNatWlanVlanConfigMismatch
Event Code	1024
Severity	Critical
Attribute	"ssid"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [{apMac}] detected VLAN configuration mismatch on non-DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This event occurs when the AP detects a non DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

## VLAN configuration mismatch on a DHCP/NAT WLAN

TABLE 474 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"
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.



## Datablade Events

The following are the events related to Datablade Based Service.

- [DP integrity test failed](#) on page 201
- [DP CLI enable failed](#) on page 201
- [DP re-authentication](#) on page 202
- [DP password min length updated](#) on page 202
- [DP password changed](#) on page 202
- [DP enable password changed](#) on page 203
- [DP https authentication failed](#) on page 203
- [DP certificate uploaded](#) on page 203
- [DP Scg FQDN updated](#) on page 203
- [DP initial upgrade](#) on page 204
- [DP discontinuous time change NTP server DP Ntp time sync](#) on page 204
- [DP user login](#) on page 204
- [DP user login failed](#) on page 205
- [DP user logout](#) on page 205
- [DP account locked](#) on page 205
- [DP session idle updated](#) on page 205
- [DP session idle terminated](#) on page 206
- [DP SSH tunnel failed](#) on page 206
- [DP https connection failed](#) on page 206
- [DP IPsec tunnel create failed](#) on page 207

### DP integrity test failed

TABLE 475 DP integrity test failed event

Event	DP integrity test failed
Event Type	dpIntegrityTestFailed
Event Code	99200
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	Data plane [[dpKey]] self integrity test failed
Description	This event occurs when the data plane self integrity test failed.

### DP CLI enable failed

TABLE 476 DP CLI enable failed event

Event	DP CLI enable failed
Event Type	dpCliEnableFailed

**TABLE 476 DP CLI enable failed event (continued)**

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.

## DP re-authentication

**TABLE 477 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.

## DP password min length updated

**TABLE 478 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.

## DP password changed

**TABLE 479 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.

## DP enable password changed

**TABLE 480 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.

## DP https authentication failed

**TABLE 481 DP https authentication failed event**

Event	DP https authentication failed
Event Type	dpHttpsAuthFailed
Event Code	99206
Severity	Informational
Attribute	"dpKey"="XXXX", "reason"="xxx"
Displayed on the web interface	Data plane [{dpKey}] certificate verification failed, [{source}].
Description	This event occurs when the data plane certificate verification failed.

## DP certificate uploaded

**TABLE 482 DP certificate uploaded event**

Event	DP certificate uploaded
Event Type	dpCertUploaded
Event Code	99207
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	Data plane [{dpKey}] certificate trusted CA chain uploaded.
Description	This event occurs when the data plane certificate trusted CA chain uploaded.

## DP Scg FQDN updated

**TABLE 483 DP Scg FQDN updated event**

Event	DP Scg FQDN updated
Event Type	dpScgFqdnUpdated
Event Code	99208
Severity	Informational

**TABLE 483 DP Scg FQDN updated event (continued)**

Event	DP Scg FQDN updated
Attribute	"dpKey"="XXXX", "fqdn"="xxx.xxx.xxx"
Displayed on the web interface	SZ {{scgIP}} FQDN {{fqdn}} setting on DP {{dpKey}}.
Description	This event occurs when the SZ FQDN setting on data plane.

## DP initial upgrade

**TABLE 484 DP initial upgrade event**

Event	DP initial upgrade
Event Type	dpInitUpgrade
Event Code	99210
Severity	Informational
Attribute	"dpKey"="XXXX", "source"="xxx"
Displayed on the web interface	Data plane {{dpKey}} initiate to upgrade, {{source}}.
Description	This event occurs when the data plane initiate to upgrade.

## DP discontinuous time change NTP server DP Ntp time sync

**TABLE 485 DP discontinuous time change NTP server DP Ntp time sync event**

Event	DP discontinuous time change NTP server DP Ntp time sync
Event Type	dpDiscontinuousTimeChangeNTPServerdpNtpTimeSync
Event Code	99211
Severity	Informational
Attribute	"dpKey"="XXXX", "before"="XXXX", "after"="XXXX", "source"="x.x.x.x"
Displayed on the web interface	Data plane {{dpKey}} time change due to ntp sync, from {{before}} to {{after}}, Source: {{source}}.
Description	This event occurs when the data plane time change due to ntp sync.

## DP user login

**TABLE 486 DP user login event**

Event	DP user login
Event Type	dpUserLogin
Event Code	99212
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User login into data plane {{dpKey}}, Source: {{source}}.
Description	This event occurs when the user login into data plane.

## DP user login failed

TABLE 487 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.

## DP user logout

TABLE 488 DP user logout event

Event	DP user logout
Event Type	dpUserLogout
Event Code	99214
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	User logout to data plane {{dpKey}}, Source: {{source}}.
Description	This event occurs when the user logout to data plane.

## DP account locked

TABLE 489 DP account locked event

Event	DP account locked
Event Type	dpAccountLocked
Event Code	99215
Severity	Informational
Attribute	"dpKey"="XXXX"
Displayed on the web interface	User account was locked, data plane: {{dpKey}}.
Description	This event occurs when the user account was locked.

## DP session idle updated

TABLE 490 DP session idle updated event

Event	DP session idle updated
Event Type	dpSessionIdleUpdated
Event Code	99220
Severity	Informational

**TABLE 490 DP session idle updated event (continued)**

Event	DP session idle updated
Attribute	"dpKey"="XXXX", "sessionIdle"="xx", "Source"="console/webGui"
Displayed on the web interface	Data plane [{dpKey}] session timeout [{sessionIdle}] change, [{source}].
Description	This event occurs when the data plane session timeout change.

## DP session idle terminated

**TABLE 491 DP session idle terminated event**

Event	DP session idle terminated
Event Type	dpSessionIdleTerminated
Event Code	99221
Severity	Informational
Attribute	"dpKey"="XXXX", "Source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] session terminated due to timeout, [{source}].
Description	This event occurs when the data plane session terminated due to timeout.

## DP SSH tunnel failed

**TABLE 492 DP SSH tunnel failed event**

Event	DP SSH tunnel failed
Event Type	dpSshTunnFailed
Event Code	99230
Severity	Informational
Attribute	"dpKey"="XXXX", "scgIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] establish ssh tunnel failed, SZ [{scgIP}].
Description	This event occurs when the data plane establish ssh tunnel failed.

## DP https connection failed

**TABLE 493 DP https connection failed event**

Event	DP https connection failed
Event Type	dpHttpsConnFailed
Event Code	99231
Severity	Informational
Attribute	"dpKey"="XXXX", "scgIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey}] https connection failed, SZ [{scgIP}].
Description	This event occurs when the data plane https connection failed.

## DP IPsec tunnel create failed

TABLE 494 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.

## Data Plane Events

Following are the events related to data plane.

<a href="#">Data plane discovered on page 208</a>	<a href="#">Data plane discovery failed on page 208</a>	<a href="#">Data plane configuration updated on page 208</a>
<a href="#">Data plane configuration update failed on page 208</a>	<a href="#">Data plane heartbeat lost on page 209</a>	<a href="#">Data plane IP address updated on page 209</a>
<a href="#">Data plane updated to a new control plane on page 210</a>	<a href="#">Data plane status update failed on page 210</a>	<a href="#">Data plane statistics update failed on page 210</a>
<a href="#">Data plane connected on page 211</a>	<a href="#">Data plane disconnected on page 211</a>	<a href="#">Data plane physical interface down on page 211</a>
<a href="#">Data plane physical interface up on page 211</a>	<a href="#">Data plane packet pool is under low water mark on page 212</a>	<a href="#">Data plane packet pool is under critical low water mark on page 212</a>
<a href="#">Data plane packet pool is above high water mark on page 212</a>	<a href="#">Data plane core dead on page 213</a>	<a href="#">Data plane process restarted on page 213</a>
<a href="#">Data plane discovery succeeded on page 213</a>	<a href="#">Data plane managed on page 214</a>	<a href="#">Data plane deleted on page 214</a>
<a href="#">Data plane license is not enough on page 214</a>	<a href="#">Data plane upgrade started on page 215</a>	<a href="#">Data plane upgrading on page 215</a>
<a href="#">Data plane upgrade succeeded on page 215</a>	<a href="#">Data plane upgrade failed on page 215</a>	<a href="#">Data plane of data center side successfully connects to the CALEA server on page 216</a>
<a href="#">Data plane of data center side fails to connect to the CALEA server on page 216</a>	<a href="#">Data plane successfully connects to the other data plane on page 217</a>	<a href="#">Data plane fails to connect to the other data plane on page 217</a>
<a href="#">Data plane disconnects to the other data plane on page 218</a>	<a href="#">Start CALEA mirroring client in data plane on page 218</a>	<a href="#">Data plane DHCP IP pool usage rate is 100 percent on page 219</a>
<a href="#">Data plane DHCP IP pool usage rate is 80 percent on page 219</a>	<a href="#">Data plane NAT session capacity usage rate is 80 percent on page 219</a>	<a href="#">Data plane NAT session capacity usage rate is 100 percent on page 220</a>
<a href="#">Data plane DHCP IP capacity usage rate is 80 percent on page 220</a>	<a href="#">Data plane DHCP IP capacity usage rate is 100 percent on page 220</a>	<a href="#">dplpmiThempBB on page 221</a>
<a href="#">dplpmiThempP on page 221</a>	<a href="#">dplpmiFan on page 222</a>	<a href="#">dplpmiREThempBB on page 222</a>
<a href="#">dplpmiREThempP on page 222</a>	<a href="#">dplpmiREFan on page 223</a>	<a href="#">Data plane backup success on page 223</a>
<a href="#">Data plane backup failed on page 223</a>	<a href="#">Data plane restore success on page 223</a>	<a href="#">Data plane restore failed on page 224</a>
<a href="#">Remote Administration Start on page 224</a>	<a href="#">Remote Administration Stop on page 224</a>	

## Data plane discovered

TABLE 495 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.

## Data plane discovery failed

TABLE 496 Data plane discovery failed event

Event	Data plane discovery failed
Event Type	dpDiscoveryFail (detected on the server side)
Event Code	502
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to send a discovery request to {produce.short.name} [{cpName}   wsgIP].
Description	This event occurs when the data plane fails to connect to the controller.

## Data plane configuration updated

TABLE 497 Data plane configuration updated event

Event	Data plane configuration updated
Event Type	dpConfUpdated
Event Code	504
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"="123456781234567"
Displayed on the web interface	Data plane [{dpName&&dpKey}] updated to configuration [{configID}].
Description	This event occurs when the data plane configuration is updated.

## Data plane configuration update failed

TABLE 498 Data plane configuration update failed event

Event	Data plane configuration update failed
Event Type	dpConfUpdateFailed
Event Code	505
Severity	Major



**TABLE 498 Data plane configuration update failed event (continued)**

Event	Data plane configuration update failed
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "configID"=" 123456781234567"
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to update to configuration [{configID}]
Description	This event occurs when the data plane configuration update fails.
Auto Clearance	This event triggers the alarm 501, which is auto cleared by the event code 504.

## Data plane rebooted

**NOTE**

This event is not applicable for SZ.

**TABLE 499 Data plane rebooted event**

Event	Data plane rebooted
Event Type	dpReboot (server side detect)
Event Code	506
Severity	Minor
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Data plane [{dpName   dpKey}] rebooted
Description	This event occurs when the data plane is rebooted.

## Data plane heartbeat lost

**TABLE 500 Data plane heartbeat lost event**

Event	Data plane heartbeat lost
Event Type	dpLostConnection (detected on the server side)
Event Code	507
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx",
Displayed on the web interface	Data plane [{dpName&&dpKey}] heartbeat lost.
Description	This event occurs when the data plane heartbeat lost.

## Data plane IP address updated

**TABLE 501 Data plane IP address updated event**

Event	Data plane IP address updated
Event Type	dpIPChanged
Event Code	508
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx",

## Events Types

### Data Plane Events

**TABLE 501** Data plane IP address updated event (continued)

Event	Data plane IP address updated
Displayed on the web interface	Data plane {{dpName&&dpKey}} IP address changed
Description	This event occurs when the IP address of the data plane is modified.

## Data plane updated to a new control plane

**TABLE 502** 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.

## Data plane status update failed

**TABLE 503** Data plane status update failed event

Event	Data plane status update failed
Event Type	dpUpdateStatusFailed
Event Code	510
Severity	Minor
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane {{dpName&&dpKey}} failed to update its status to {produce.short.name} {{cpName     wsgIP}}.
Description	This event occurs when the data plane fails to update its status on the controller.

## Data plane statistics update failed

**TABLE 504** Data plane statistics update failed event

Event	Data plane statistics update failed
Event Type	dpUpdateStatisticFailed
Event Code	511
Severity	Minor
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane {{dpName&&dpKey}} failed to update its statistics to {produce.short.name} {{cpName     wsgIP}}.
Description	This event occurs when the data plane fails to update statistics to the controller.

## Data plane connected

TABLE 505 Data plane connected event

Event	Data plane connected
Event Type	dpConnected
Event Code	512
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] connected to {produce.short.name} [{cpName     wsgIP}].
Description	This event occurs when the data plane connects to the controller.

## Data plane disconnected

TABLE 506 Data plane disconnected event

Event	Data plane disconnected
Event Type	dpDisconnected
Event Code	513
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}], Reason: [{reason}].
Description	This event occurs when the data plane disconnects from the controller.
Auto Clearance	This event triggers the alarm 503, which is auto cleared by the event code 512.

## Data plane physical interface down

TABLE 507 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.

## Data plane physical interface up

TABLE 508 Data plane physical interface up event

Event	Data plane physical interface up
Event Type	dpPhyInterfaceUp

**TABLE 508** Data plane physical interface up event (continued)

Event	Data plane physical interface up
Event Code	515
Severity	Informational
Attribute	"portID"="xx", "dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName&&dpKey}] is up.
Description	This event occurs when the network link of the data plane is UP.

## Data plane packet pool is under low water mark

**TABLE 509** 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", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName&&dpKey}] is under low-water mark.
Description	This event occurs when the data core packet pool is below the water mark level.
Auto Clearance	This event triggers the alarm 516, which is auto cleared by the event code 518.

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

**TABLE 510** Data plane's packet pool is under critical low water mark event

Event	Data plane packet pool is under critical low water mark
Event Type	dpPktPoolCriticalLow
Event Code	517
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName&&dpKey}] is under critical low-water mark.
Description	This event occurs when the data core packet pool reaches the critical water mark level.

## Data plane packet pool is above high water mark

**TABLE 511** Data plane packet pool is above high water mark event

Event	Data plane packet pool is above high water mark
Event Type	dpPktPoolRecover
Event Code	518
Severity	Informational
Attribute	dpKey="xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName&&dpKey}] is above high-water mark

**TABLE 511 Data plane packet pool is above high water mark event (continued)**

Event	Data plane packet pool is above high water mark
Description	This event occurs when the data plane's packet pool is recovered when it is above the high-water mark.

## Data plane core dead

**TABLE 512 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"
Displayed on the web interface	Data plane [{dpName&&dpKey}] has dead data core.
Description	This event occurs when one or multiple data core packet pool is lost /dead.

## Data plane process restarted

**TABLE 513 Data plane process restarted event**

Event	Data plane process restarted
Event Type	dpProcessRestart
Event Code	520
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	[{processName}] process got re-started on data plane [{dpName&&dpKey}].
Description	This event occurs when a process in the data plane restarts since it fails to pass the health check.

**NOTE**

Event 530 is not applicable for SZ.

## Data plane discovery succeeded

**TABLE 514 Data plane discovery succeeded event**

Event	Data plane discovery succeeded
Event Type	dpDiscoverySuccess
Event Code	530
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] sent a discovery request to {produce.short.name} [{wsgIP}]
Description	This event occurs when data plane sends a discovery request to the {produce.short.name} successfully.

**NOTE**

Event 532 is not applicable for SZ.

## Data plane managed

**TABLE 515** 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}].
Description	This event occurs when data plane is approved by the {produce.short.name}.

**NOTE**

Events 537 to 553 are not applicable for SZ.

## Data plane deleted

**TABLE 516** Data plane deleted event

Event	Data plane deleted
Event Type	dpDeleted
Event Code	537
Severity	Informational
Attribute	"dpKey"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] deleted.
Description	This event occurs when data plane is deleted.

## Data plane license is not enough

**TABLE 517** Data plane license is not enough event

Event	Data plane license is not enough
Event Type	dpLicenseInsufficient
Event Code	538
Severity	Major
Attribute	"count"=<delete-vdp-count>
Displayed on the web interface	Data plane license is not enough, [{count}] instance of data plane will be deleted.
Description	This event occurs when data plane licenses are insufficient.

## Data plane upgrade started

TABLE 518 Data plane upgrade started event

Event	Data plane upgrade started
Event Type	dpUpgradeStart
Event Code	550
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}]started the upgrade process.
Description	This event occurs when data plane starts the upgrade process.

## Data plane upgrading

TABLE 519 Data plane upgrading event

Event	Data plane upgrading
Event Type	dpUpgrading
Event Code	551
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] is upgrading.
Description	This event occurs when data plane starts to upgrade programs and configuration.

## Data plane upgrade succeeded

TABLE 520 Data plane upgrade succeeded event

Event	Data plane upgrade succeeded
Event Type	dpUpgradeSuccess
Event Code	552
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] has been upgraded successfully..
Description	This event occurs when data plane upgrade is successful.

## Data plane upgrade failed

TABLE 521 Data plane upgrade failed event

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

**TABLE 521 Data plane upgrade failed event (continued)**

Event	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 event occurs when data plane upgrade fails.
Auto Clearance	This event triggers the alarm 553, which is auto cleared by the event code 552.

## Data Plane Upgrade Failed Due to Corrupted RPM

**TABLE 522 dpUpgradeFailedDueToCorruptedRpm event**

Event	dpUpgradeFailedDueToCorruptedRpm
Event Type	dpUpgradeFailedDueToCorruptedRpm
Event Code	554
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
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.

## Data plane of data center side successfully connects to the CALEA server

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 523 Data plane of data center side successfully connects to the CALEA server event**

Event	Data plane of data center side successfully connects to the CALEA server
Event Type	dpDcToCaleaConnected
Event Code	1257
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [[dpName&&dpKey]] successfully connects to the CALEA server[[caleaServerIP]].
Description	This event occurs when the data plane successfully connects to the CALEA server.

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

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 524 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



**TABLE 524 Data plane of data center side fails to connect to the CALEA server event (continued)**

Event	Data plane of data center side fails to connect to the CALEA server.
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [[dpName&&dpKey]] fails to connects to the CALEA server[[caleaServerIP]]
Description	This event occurs when the data plane fails to connect to the CALEA server.
Auto Clearance	This event triggers the alarm 1258, which is auto cleared by the event code 1257.

## Data plane successfully connects to the other data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 525 Data plane successfully connects to the other data plane event**

Event	Data plane successfully connects to the other data plane
Event Type	dpP2PTunnelConnected
Event Code	1260
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane [[dpName&&dpKey]] successfully connects to the other Data Plane[[targetDpKey&&targetDpIP]]
Description	This event occurs when the data plane connects to another data plane.

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

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 526 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.

## Data plane disconnects to the other data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 527 Data plane disconnects to the other data plane event**

Event	Data plane disconnects to the other data plane
Event Type	dpP2PTunnelDisconnected
Event Code	1262
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] disconnects to the other Data Plane[{targetDpKey&&targetDpIp}]
Description	This event occurs when the data plane disconnects from another data plane.

## Start CALEA mirroring client in data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 528 Start CALEA mirroring client in data plane event**

Event	Start CALEA mirroring client in data plane
Event Type	dpStartMirroringClient
Event Code	1263
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx"
Displayed on the web interface	Start CALEA mirroring client [{userName}   IP   clientMac] on WLAN [{ssid}] from AP [{apName&&apMac}]
Description	This event occurs when the CALEA server starts mirroring the client image.

## Stop CALEA mirroring client in data plane

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 529 Stop CALEA mirroring client in data plane event**

Event	Stop CALEA mirroring client in data plane
Event Type	dpStopMirroringClient
Event Code	1264
Severity	Warning
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx"
Displayed on the web interface	Stop CALEA mirroring client [{userName}   IP   clientMac] on WLAN [{ssid}   authType] from AP [{apName&&apMac}]. TxBytes[{txBytes}]
Description	This event occurs when the CALEA server stops mirroring the client image.

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

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 530** Data plane DHCP IP pool usage rate is 100 percent event

Event	Data plane DHCP IP pool usage rate is 100 percent
Event Type	dpDhcpIpPoolUsageRate100
Event Code	1265
Severity	Critical
Attribute	"dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane[{{dpName&&dpKey}}] DHCP IP Pool usage rate is 100 percent
Description	This event occurs when the data plane DHCP pool usage rate is 100%.

## Data plane DHCP IP pool usage rate is 80 percent

**NOTE**

This section is not applicable for SZ300/SZ100.

**TABLE 531** Data plane DHCP IP pool usage rate is 80 percent event

Event	Data plane DHCP IP pool usage rate is 80 percent
Event Type	dpDhcpIpPoolUsageRate80
Event Code	1266
Severity	Warning
Attribute	"dpName"="xxxxxxx", "dpKey"="xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane[{{dpName&&dpKey}}] DHCP IP Pool usage rate is 80 percent
Description	This event occurs when the data plane DHCP pool usage rate is 80%.

## Data plane NAT session capacity usage rate is 80 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 532** Data plane NAT session capacity usage rate is 80 percent event

Event	Data plane NAT session capacity usage rate is 80 percent
Event Type	dpNatSessionCapacityUsageRate80
Event Code	1283
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{{dpKey}}] NAT Session Capacity usage rate is 80 percent. ( total [{{totalLicenseCnt}}, consumed [{{consumedLicenseCnt}}, available [{{availableLicenseCnt}}] )
Description	This event occurs when the data plane NAT session capacity usage rate is 80%.

## Data plane NAT session capacity usage rate is 100 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 533 Data plane NAT session capacity usage rate is 100 percent event**

Event	Data plane NAT session capacity usage rate is 100 percent
Event Type	dpNatSessionCapacityUsageRate100
Event Code	1284
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{{dpKey}}] NAT Session Capacity usage rate is 100 percent. (total [{{totalLicenseCnt}}, consumed [{{consumedLicenseCnt}}, available [{{availableLicenseCnt}}])
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

## Data plane DHCP IP capacity usage rate is 80 percent

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 534 Data plane DHCP IP capacity usage rate is 80 percent event**

Event	Data plane DHCP IP capacity usage rate is 80 percent
Event Type	dpDhcpIpCapacityUsageRate80
Event Code	1285
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{{dpKey}}] DHCP IP Capacity usage rate is 80 percent. (total [{{totalLicenseCnt}}, consumed [{{consumedLicenseCnt}}, available [{{availableLicenseCnt}}])
Description	This event occurs when the data plane DHCP IP capacity usage rate is 80%.

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

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 535 Data plane DHCP IP capacity usage rate is 100 percent event**

Event	Data plane DHCP IP capacity usage rate is 100 percent
Event Type	dpDhcpIpCapacityUsageRate100
Event Code	1286
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"

**TABLE 535 Data plane DHCP IP capacity usage rate is 100 percent event (continued)**

Event	Data plane DHCP IP capacity usage rate is 100 percent
Displayed on the web interface	Data Plane[{{dpKey}}] DHCP IP Capacity usage rate is 100 percent. (total [{{totalLicenseCnt}}, consumed [{{consumedLicenseCnt}}, available [{{availableLicenseCnt}}])
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

## dplpmiThempBB

**NOTE**

Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

**TABLE 536 dplpmiThempBB event**

Event	dplpmiThempBB
Event Type	dplpmiThempBB
Event Code	2902
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{{status}}] on data plane [{{dpName&&dpKey}}]
Description	This event occurs when the baseboard temperature status on the data plane is sent. Baseboard threshold temperatures are in the range of 100 Celsius to 610 Celsius. The default threshold is 610C.

## dplpmiThempP

**NOTE**

Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

**TABLE 537 dplpmiThempP event**

Event	dplpmiThempP
Event Type	dplpmiThempP
Event Code	2907
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{{id}}] temperature [{{status}}] on data plane [{{dpName&&dpKey}}].
Description	This event occurs when the processor temperature status on the data plane is sent. The threshold value is in the range of 10 to 110 Celsius. The default threshold is 110C.

## dplpmiFan

**NOTE**

Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

**TABLE 538 dplpmiFan event**

Event	dplpmiFan
Event Type	dplpmiFan
Event Code	2909
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the system fan module status on the data plane is sent.

## dplpmiREThempBB

**NOTE**

Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

**TABLE 539 dplpmiREThempBB event**

Event	dplpmiREThempBB
Event Type	dplpmiREThempBB
Event Code	2927
Severity	Informational
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the baseboard temperature comes back to the normal status.

## dplpmiREThempP

**NOTE**

Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

**TABLE 540 dplpmiREThempP event**

Event	dplpmiREThempP
Event Type	dplpmiREThempP
Event Code	2932
Severity	Informational
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the processor temperature comes back to the normal status.

## dplpmiREFan

### NOTE

Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

**TABLE 541 dplpmiREFan event**

Event	dplpmiREFan
Event Type	dplpmiREFan
Event Code	2934
Severity	Informational
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan {{id}} module {{status}} on data plane {{dpName&&dpKey}}].
Description	This event occurs when system fan module comes back to the normal status.

## Data plane backup success

**TABLE 542 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"
Displayed on the web interface	Data Plane {{dpName&&dpKey}} backup successful.
Description	This event occurs when Data plane backup is successful.

## Data plane backup failed

**TABLE 543 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"
Displayed on the web interface	Data Plane {{dpName&&dpKey}} backup failed.
Description	This event occurs when Data plane backup fails.

## Data plane restore success

**TABLE 544 Data plane restore success event**

Event	Data plane restore success
Event Type	dpRestoreSuccess

**TABLE 544 Data plane restore success event (continued)**

Event	Data plane restore success
Event Code	1292
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] restore successful.
Description	This event occurs when Data plane restore is successful.

## Data plane restore failed

**TABLE 545 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.

## Remote Administration Start

**TABLE 546 Remote administration event**

Event	Remote administration
Event Type	dpreoteadministration
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.

## Remote Administration Stop

**TABLE 547 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.



## dplpmiThempIOH

TABLE 548 dplpmiThempIOH event

Event	dplpmiThempIOH
Event Type	dplpmiThempIOH
Event Code	2904
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	IOH temperature [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the IOH temperature status on the data plane is sent..

## dplpmiPsStatus

TABLE 549 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.

## dplpmiREThempMemP

TABLE 550 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}].
Description	This event occurs when the processor memory temperature status recover from abnormal condition.

## dplpmiPsStatus

TABLE 551 dplpmiPsStatus event

Event	dplpmiPsStatus
Event Type	dplpmiPsStatus
Event Code	2913
Severity	Major

TABLE 551 dplpmiPsStatus event (continued)

Event	dplpmiPsStatus
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.

## dplpmiREThempMemP

TABLE 552 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}].
Description	This event occurs when the processor memory temperature status recover from abnormal condition.

## dplpmiRePsStatus

TABLE 553 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.

## dpSSDHealthDegrade

TABLE 554 dpSSDHealthDegrade event

Event	dpSSDHealthDegrade
Event Type	dpSSDHealthDegrade
Event Code	2961
Severity	Major
Attribute	"dpKey"="xxxxxxx","id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx: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.

## Data Plane Upgrade Failed Due to Corrupted RPM

TABLE 555 dpUpgradeFailedDueToCorruptedRpm event

Event	dpUpgradeFailedDueToCorruptedRpm
Event Type	dpUpgradeFailedDueToCorruptedRpm
Event Code	554
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx"
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.

## Data Streaming Event

Following are the events related to Data Streaming events.

<a href="#">Connected to Data a Streaming Endpoint</a> on page 227	<a href="#">Disconnected to Data a Streaming Endpoint</a> on page 227	<a href="#">Connected to Data a Streaming Endpoint Failure</a> on page 228
--	---	--

## Connected to Data a Streaming Endpoint

TABLE 556 Connected to Data a Streaming Endpoint event

Event	Connected to Data a Streaming Endpoint
Event Type	connectedtoDataStreamingEndpoint
Event Code	4701
Severity	Informational
Displayed on the web interface	Connect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ connected to data a streaming endpoint.

## Disconnected to Data a Streaming Endpoint

TABLE 557 Disconnected to Data a Streaming Endpoint event

Event	Disconnected to Data a Streaming Endpoint
Event Type	disconnectedtoDataStreamingEndpoint
Event Code	4702
Severity	Warning
Displayed on the web interface	Disconnect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ disconnected to data a streaming endpoint.

## Connected to Data a Streaming Endpoint Failure

TABLE 558 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.

## IPMI Events

### NOTE

This section is not applicable for vSZ-E.

Following are the events related to IPMIs.

- [ipmiThempBB](#) on page 228
- [ipmiThempP](#) on page 229
- [ipmiFan](#) on page 229
- [ipmiFanStatus](#) on page 229
- [ipmiREThempBB](#) on page 230
- [ipmiREThempP](#) on page 230
- [ipmiREFan](#) on page 230
- [ipmiREFanStatus](#) on page 230

## ipmiThempBB

TABLE 559 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}]
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.

## ipmiThempP

TABLE 560 ipmiThempP event

Event	ipmiThempP
Event Type	ipmiThempP
Event Code	907
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This event is triggered when the threshold value 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.

## ipmiFan

TABLE 561 ipmiFan event

Event	ipmiFan
Event Type	ipmiFan
Event Code	909
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}]
Description	This event occurs when the system fan module status is sent.
Auto Clearance	This event triggers the alarm 909, which is auto cleared by the event code 934.

## ipmiFanStatus

TABLE 562 ipmiFanStatus event

Event	ipmiFanStatus
Event Type	ipmiFanStatus
Event Code	912
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the fan module status is sent.
Auto Clearance	This event triggers the alarm 912, which is auto cleared by the event code 937.

## ipmiREThempBB

TABLE 563 ipmiREThempBB event

Event	ipmiREThempBB
Event Type	ipmiREThempBB
Event Code	927
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the baseboard temperature comes back to the normal status.

## ipmiREThempP

TABLE 564 ipmiREThempP event

Event	ipmiREThempP
Event Type	ipmiREThempP
Event Code	932
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the processor temperature comes back to the normal status.

## ipmiREFan

TABLE 565 ipmiREFan event

Event	ipmiREFan
Event Type	ipmiREFan
Event Code	934
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}].
Description	This event occurs when the system fan module comes back to the normal status.

## ipmiREFanStatus

TABLE 566 ipmiREFanStatus event

Event	ipmiREFanStatus
Event Type	ipmiREFanStatus
Event Code	937
Severity	Informational

**TABLE 566 ipmiREFanStatus event (continued)**

Event	ipmiREFanStatus
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module <code>[[id]]</code> <code>[[status]]</code> on control plane <code>[[nodeMac]]</code> .
Description	This event occurs when the fan module comes back to the normal status.

## Licensing Interface Events

Following are the events related to licensing.

- [License sync succeeded](#) on page 231
- [License sync failed](#) on page 232
- [License import succeeded](#) on page 232
- [License import failed](#) on page 232
- [License data changed](#) on page 232
- [License going to expire](#) on page 233
- [Insufficient license capacity](#) on page 233
- [Data plane DHCP IP license insufficient](#) on page 233
- [Data plane NAT session license insufficient](#) on page 234
- [AP number limit exceeded](#) on page 234
- [Insufficient license capacity](#) on page 235
- [Data plane DHCP IP capacity license has been removed](#) on page 235
- [Data plane NAT session capacity license has been removed](#) on page 235
- [Insufficient license capacity](#) on page 236

## License sync succeeded

**TABLE 567 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 <code>[[nodeName]]</code> sync-up license with license server <code>[[licenseServerName]]</code> succeeded.
Description	This event occurs when the controller successfully synchronizes the license data with the license server.

## Events Types

### Licensing Interface Events

## License sync failed

TABLE 568 License sync failed event

Event	License sync failed
Event Type	licenseSyncFail
Event Code	1251
Severity	Warning
Attribute	"nodeName"="xxxxxxx", "licenseServerName"="ruckuswireless.flexeraoperation.com"
Displayed on the web interface	Node [{nodeName}] sync-up license with license server [{licenseServerName}] failed.
Description	This event occurs when the controller fails to synchronize the license data with the license server.

## License import succeeded

TABLE 569 License import succeeded event

Event	License import succeeded
Event Type	licenseImportSuccess
Event Code	1252
Severity	Informational
Attribute	"nodeName"="xxxxxxx",
Displayed on the web interface	Node [{nodeName}] import license data succeeded.
Description	This event occurs when the controller successfully imports the license data

## License import failed

TABLE 570 License import failed event

Event	License import failed
Event Type	licenseImportFail
Event Code	1253
Severity	Warning
Attribute	"nodeName"="xxxxxxx",
Displayed on the web interface	Node [{nodeName}] import license data failed.
Description	This event occurs when the controller fails to imports the license data

## License data changed

TABLE 571 License data changed event

Event	License data changed
Event Type	licenseChanged
Event Code	1254



**TABLE 571 License data changed event (continued)**

Event	License data changed
Severity	Informational
Attribute	"nodeName"="xxxxxxx"
Displayed on the web interface	Node [{nodeName}] license data has been changed.
Description	This event occurs when the controller license data is modified.

## License going to expire

**TABLE 572 License going to expire event**

Event	License going to expire
Event Type	licenseGoingToExpire
Event Code	1255
Severity	Major
Attribute	"nodeName"="xxx", "licenseType"=" xxx"
Displayed on the web interface	The [{licenseType}] on node [{nodeName}] will expire on [{associationTime}].
Description	This event occurs when the validity of the license is going to expire.

## Insufficient license capacity

**TABLE 573 Insufficient license capacity event**

Event	Insufficient license capacity
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1256
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing AP connections to terminate.
Description	This event occurs when connected APs are rejected due to insufficient licenses.

## Data plane DHCP IP license insufficient

**NOTE**

This event is not applicable for SZ300/SZ100.

**TABLE 574 Data plane DHCP IP license insufficient event**

Event	Data plane DHCP IP license insufficient
Event Type	dpDhcpIpLicenseNotEnough
Event Code	1277
Severity	Major

## Events Types

### Licensing Interface Events

**TABLE 574 Data plane DHCP IP license insufficient event (continued)**

Event	Data plane DHCP IP license insufficient
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This event occurs when Data Plane DHCP IP license insufficient. ( total [[totalLicenseCnt]], consumed [[consumedLicenseCnt]], available [[availableLicenseCnt]] )
Description	This event occurs when the data plane DHCP IP address license is insufficient.

## Data plane NAT session license insufficient

### NOTE

This event is not applicable for SZ300/SZ100.

**TABLE 575 Data plane NAT session license insufficient event**

Event	Data plane NAT session license insufficient
Event Type	dpNatSessionLicenseNotEnough
Event Code	1278
Severity	Major
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This event occurs when Data Plane NAT session license insufficient. ( total [[totalLicenseCnt]], consumed [[consumedLicenseCnt]], available [[availableLicenseCnt]] )
Description	This event occurs when the data plane NAT session license is insufficient.

## AP number limit exceeded

**TABLE 576 AP number limit exceeded event**

Event	AP number limit exceeded
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1280
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [[licenseType]] license is detected and it will cause existing AP connections to terminate.
Description	This event occurs when an approved AP is rejected due to number of APs having exceeded the limit.

## Insufficient license capacity

TABLE 577 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.

## Data plane DHCP IP capacity license has been removed

**NOTE**

This section is not applicable for SZ300/SZ100.

TABLE 578 Data plane DHCP IP capacity license has been removed event

Event	Data plane DHCP IP capacity license has been removed
Event Type	dpDhcpIpLicenseRemoved
Event Code	1287
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 has been removed one unit. Current assignment (total [{{totalLicenseCnt}}], consumed [{{consumedLicenseCnt}}], available [{{availableLicenseCnt}}])
Description	This event occurs when the data plane DHCP IP capacity license is removed.

## Data plane NAT session capacity license has been removed

**NOTE**

This section is not applicable for SZ300/SZ100.

TABLE 579 Data plane NAT session capacity license has been removed event

Event	Data plane NAT session capacity license has been removed
Event Type	dpNatSessionLicenseRemoved
Event Code	1288
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 has been removed one unit. Current assignment (total [{{totalLicenseCnt}}], consumed [{{consumedLicenseCnt}}], available [{{availableLicenseCnt}}])
Description	This event occurs when data plane NAT session capacity license is removed.

## Insufficient license capacity

TABLE 580 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.

## Session Events

Following event is related to user equipment TTG session.

- [Delete all sessions](#) on page 236

## Delete all sessions

TABLE 581 Delete all sessions event

Event	Delete all sessions
Event Type	delAllSess
Event Code	1237
Severity	Minor
Attribute	"mynold"="NA" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "cause"="Admin Delete" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	All sessions got terminated on {produce.short.name} [{{SZMgmtIp}}] due to [{{cause}}]
Description	This event occurs when all sessions are deleted based on the indicators received from the controller web Interface or CLI.

## System Events

Following are the events related to system log severity.

**NOTE**

{produce.short.name} refers to SZ or vSZ-E

<a href="#">No LS responses</a> on page 237	<a href="#">LS authentication failure</a> on page 237	<a href="#">{produce.short.name} connected to LS</a> on page 238
<a href="#">{produce.short.name} failed to connect to LS</a> on page 238	<a href="#">{produce.short.name} received passive request</a> on page 238	<a href="#">{produce.short.name} sent controller information report</a> on page 238
<a href="#">{produce.short.name} received management request</a> on page 239	<a href="#">{produce.short.name} sent AP info by venue report</a> on page 239	<a href="#">{produce.short.name} sent query venues report</a> on page 239

{produce.short.name} sent associated client report on page 240	{produce.short.name} forwarded calibration request to AP on page 240	{produce.short.name} forwarded footfall request to AP on page 240
{produce.short.name} received unrecognized request on page 241	Syslog server reachable on page 241	Syslog server unreachable on page 241
Syslog server switched on page 241	System service failure on page 242	Generate AP config for plane load rebalance succeeded on page 242
FTP transfer on page 243	FTP transfer error on page 243	File upload on page 243
Email sent successfully on page 244	Email sent failed on page 244	SMS sent successfully on page 244
SMS sent failed on page 244	Process restart on page 245	Service unavailable on page 245
Keepalive failure on page 245	Resource unavailable on page 246	Unconfirmed program detection on page 246
All data planes in the zone affinity profile are disconnected on page 246	CALEA UE Matched on page 247	ZD AP migrating on page 247
ZD AP migrated on page 247	ZD AP rejected on page 248	ZD AP migration failed on page 248
Database error on page 248	Database error on page 248	SZ Login Fail on page 249
SZ Login on page 249	SZ Logout on page 249	Password expiration on page 250
Admin account lockout on page 250	Admin session expired on page 250	Disable inactive admins on page 251
Two factor auth failed on page 251	Admin account lockout after failed attempts on page 251	Discontinuous time change on page 251

## No LS responses

TABLE 582 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"="", "SZMgmtIp"=""
Displayed on the web interface	Smart Zone [{SZMgmtIp}] no response from LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller does not get a response while connecting to the location based service.

## LS authentication failure

TABLE 583 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"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] authentication failed: url=[{url}], port=[{port}]
Description	This event occurs due to the authentication failure on connecting to the location based service.

## {produce.short.name} connected to LS

TABLE 584 {produce.short.name} connected to LS event

Event	{produce.short.name} connected to LS
Event Type	scgLBSCConnectSuccess
Event Code	723
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "url"="", "port"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] connected to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller successfully connects to the location based service.

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

TABLE 585 {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"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] connection failed to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller failed to connect to the location based service.
Auto Clearance	This event triggers the alarm 724, which is auto cleared by the event code 723.

## {produce.short.name} received passive request

TABLE 586 {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"="", "SZMgmtIp"="", "band"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] received Passive Request, band=[{band}], type=[{type}]
Description	This event occurs when the controller receives a passive request.

## {produce.short.name} sent controller information report

TABLE 587 {produce.short.name} sent controller information report event

Event	{produce.short.name} sent controller information report
Event Type	scgLBSSentControllerInfo
Event Code	727

**TABLE 587 {produce.short.name} sent controller information report event (continued)**

Event	{produce.short.name} sent controller information report
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "api"="", "sw"="", "clusterName"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] sent Controller Info Report: mac ={{mac}}, api={{api}}, sw={{sw}}, clusterName ={{clusterName}}
Description	This event occurs when the controller sends the controller information report.

## {produce.short.name} received management request

**TABLE 588 {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"="", "SZMgmtIp"=""
Displayed on the web interface	Smart Zone [{SZMgmtIp}] received Management Request: venue={{venue}}, type={{type}}
Description	This event occurs when the controller receives the management request.

## {produce.short.name} sent AP info by venue report

**TABLE 589 {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"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] sent AP Info by Venue Report: venue={{venue}}, count ={{count}}
Description	This event occurs when the controller sends the venue report regarding AP information.

## {produce.short.name} sent query venues report

**TABLE 590 {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"="", "SZMgmtIp"=""
Displayed on the web interface	Smart Zone [{SZMgmtIp}] sent Query Venues Report: count={{count}}
Description	This event occurs when the controller sends the query venue report.

## {produce.short.name} sent associated client report

TABLE 591 {produce.short.name} sent associated client report event

Event	{produce.short.name} sent associated client report
Event Type	scgLBSendClientInfo
Event Code	731
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "count"="", "SZMgmtIp"="", "type"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] sent Associated Client Report: count=[{count}], type=[{type}]
Description	This event occurs when the controller sends the associated client report.

## {produce.short.name} forwarded calibration request to AP

TABLE 592 {produce.short.name} forwarded calibration request to AP event

Event	{produce.short.name} forwarded calibration request to AP
Event Type	scgLBSFwdPassiveCalReq
Event Code	732
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "SZMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"="", "count"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] forwarded Passive Calibration Request to [{apName&&apMac}]: venue=[{venue}], interval=[{interval}s], duration=[{duration}m], band=[{band}], count=[{count}]
Description	This event occurs when the controller sends a forward calibration request to the AP on its reconnection to the controller.

## {produce.short.name} forwarded footfall request to AP

TABLE 593 {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	"nodeMac"="xx:xx:xx:xx:xx:xx", "SZMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue"="", "interval"="", "duration"="", "band"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] forwarded Passive Footfall Request to [{apName&&apMac}]: venue=[{venue}], interval=[{interval}s] duration=[{duration}m], band=[{band}]
Description	This event occurs when the controller sends a forward footfall request to the AP on its reconnection to the controller.



## {produce.short.name} received unrecognized request

TABLE 594 {produce.short.name} received unrecognized request event

Event	{produce.short.name} received unrecognized request
Event Type	scgLBSRcvdUnrecognizedRequest
Event Code	734
Severity	Warning
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "type"="", "length"="", "SZMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SZMgmtIp}] received Unrecognized: length =[{length}]
Description	This event occurs when the controller receives an unrecognized request.

## Syslog server reachable

TABLE 595 Syslog server reachable event

Event	Syslog server reachable
Event Type	syslogServerReachable
Event Code	750
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is reachable on {produce.short.name}.
Description	This event occurs when the syslog server can be reached.

## Syslog server unreachable

TABLE 596 Syslog server unreachable event

Event	Syslog server unreachable
Event Type	syslogServerUnreachable
Event Code	751
Severity	Major
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is unreachable on {produce.short.name}.
Description	This event occurs when the syslog server is unreachable.
Auto Clearance	This event triggers the alarm 751, which is auto cleared by the event code 750.

## Syslog server switched

TABLE 597 Syslog server switched event

Event	Syslog server switched
Event Type	syslogServerSwitched

**TABLE 597 Syslog server switched event (continued)**

Event	Syslog server switched
Event Code	752
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx", "srcAddress"="xxx.xxx.xxx.xxx", "destAddress"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Syslog server is switched from [[srcAddress]] to [[destAddress]] on {produce.short.name}.
Description	This event occurs when the syslog server is switched.

## System service failure

**TABLE 598 System service failure event**

Event	System service failure
Event Type	systemservicefailure
Event Code	753
Severity	Critical
Attribute	"sysService"="", "hostName"="".
Displayed on the web interface	Service [sysService] on node [hostName] failed and respawning
Description	This event occurs when the service is not available.

## Generate AP config for plane load rebalance succeeded

**TABLE 599 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	
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing succeeded.
Description	This event occurs when the user executes the load of data plane for re-balancing and generates a new AP configuration successfully.

## Generate AP config for plane load rebalance failed

**TABLE 600 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	

**TABLE 600** Generate AP config for plane load rebalance failed event (continued)

Event	Generate AP config for plane load rebalance failed
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing failed.
Description	This event occurs when the user executes the load of data plane for re-balancing and generation of a new AP configuration fails.

## FTP transfer

**TABLE 601** FTP transfer event

Event	FTP transfer
Event Type	ftpTransfer
Event Code	970
Severity	Informational
Attribute	"ip"="xxx.xxx.xxx.xxx", "portID"="xxxx", "reason"="xxxxx"
Displayed on the web interface	File [[reason]] transferred to FTP server [[ip]:{portID}] successfully
Description	This event occurs when a file transfer to the FTP server is successful.

## FTP transfer error

**TABLE 602** 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.

## File upload

**TABLE 603** File upload event

Event	File upload
Event Type	fileUpload
Event Code	980
Severity	Informational
Attribute	"ip"="xxx.xxx.xxx.xxx", "cause"="xxxxx"
Displayed on the web interface	Backup file [[cause]] uploading from [[ip]] failed
Description	This event occurs when the backup file upload fails.

## Email sent successfully

TABLE 604 Email sent successfully event

Event	Email sent successfully
Event Type	mailSendSuccess
Event Code	981
Severity	Informational
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	[[srcProcess]] sent email to [[receiver]] successfully.
Description	This event occurs when system sends mail successfully.

## Email sent failed

TABLE 605 Email sent failed event

Event	Email sent failed
Event Type	mailSendFailed
Event Code	982
Severity	Warning
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	[[srcProcess]] sent email to [[receiver]] failed.
Description	This event occurs when the system fails to send the mail.

## SMS sent successfully

TABLE 606 SMS sent successfully event

Event	SMS sent successfully
Event Type	smsSendSuccess
Event Code	983
Severity	Informational
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx", "nodeName"="xxxxx", "tenantUUID"="xxxxx"
Displayed on the web interface	[[srcProcess]] sent short message to [[receiver]] successfully.
Description	This event occurs when system sends the short message successfully.

## SMS sent failed

TABLE 607 SMS sent failed event

Event	SMS sent failed
Event Type	smsSendFailed

**TABLE 607 SMS sent failed event (continued)**

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 successfully.

## Process restart

**TABLE 608 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" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	[[processName]] process got re-started on {produce.short.name} [[SZMgmtIp]]
Description	This event occurs when any process crashes and restarts.

## Service unavailable

**TABLE 609 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" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	[[processName]] process is not stable on {produce.short.name} [[SZMgmtIp]]
Description	This event occurs when the process repeatedly restarts and is unstable.

## Keepalive failure

**TABLE 610 Keepalive failure event**

Event	Keepalive failure
Event Type	keepAliveFailure
Event Code	1003
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="nc" "realm"="NA" "processName"="aut" "SZMgmtIp"="2.2.2.2"

**TABLE 610** Keepalive failure event (continued)

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

## Resource unavailable

**TABLE 611** 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" "SZMgmtIp" = "3.3.3.3" "cause" = "resource that is not available"
Displayed on the web interface	System resource {{cause}} not available in {{srcProcess}} process at {{produce.short.name}} {{SZMgmtIp}}
Description	This event is generated due to unavailability of any other system resource, such as memcached.

## Unconfirmed program detection

**TABLE 612** 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.

## All data planes in the zone affinity profile are disconnected

**NOTE**

Events 1257 to 1267 are not applicable to SZ300/SZ100.

**TABLE 613** 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}}.

**TABLE 613 All data planes in the zone affinity profile are disconnected event (continued)**

Event	All data planes in the zone affinity profile are disconnected
Description	This event occurs when all the data planes disconnect from the zone affinity profile.

## CALEA UE Matched

**TABLE 614 CALEA UE Matched event**

Event	CALEA UE Matched
Event Type	dpCaleaUeInterimMatched
Event Code	1268
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	CALEA matches client {{clientMac}} on WLAN {{ssid   authType}}from AP {{apName&&apMac}}. TxBytes{{txBytes}}, RxBytes{{rxBytes}}.
Description	This event occurs when the data plane CALEA user equipment and client matches.

## ZD AP migrating

**TABLE 615 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"="R700", "firmware"="3.2.0.0.x"
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 {produce.short.name} AP firmware image.

## ZD AP migrated

**TABLE 616 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 {produce.short.name} AP firmware image.

## ZD AP rejected

TABLE 617 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"="R700"
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 {produce.short.name} AP firmware because of the ACL setting.

## ZD AP migration failed

TABLE 618 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"="R700", "firmware"="3.2.0.0.x"
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 a ZoneDirector AP fails to upgrade with [produce.short.name] AP firmware image.

## Database error

TABLE 619 Database error event

Event	Database error
Event Type	cassandraError
Event Code	3001
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SZMgmtIp"="2.2.2.2" reason="reason"
Displayed on the web interface	Database internal error on node [{nodeName}], reason: [{reason}].
Description	This event occurs when internal errors occurs on the database.

## Database error

TABLE 620 Database error event

Event	Database error
Event Type	recoverCassandraError



**TABLE 620 Database error event (continued)**

Event	Database error
Event Code	3011
Severity	Informational
Attribute	"nodeName"="xxx","reason"="recovery reason"
Displayed on the web interface	Recover database error on node [{nodeName}], reason : [].
Description	This event occurs when the internal errors on the database are fixed.

## SZ Login Fail

**TABLE 621 SZ login fail event**

Event	SZ login fail
Event Type	szLoginFail
Event Code	8007
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on failed from [{ip}].
Description	Administrator logged on failed SZ.

## SZ Login

**TABLE 622 SZ login event**

Event	SZ login
Event Type	szLogin
Event Code	8008
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on from [{ip}].
Description	Administrator logged on SZ.

## SZ Logout

**TABLE 623 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.

## Password expiration

TABLE 624 Password expiration event

Event	Password expiration
Event Type	passwordExpiration
Event Code	8010
Severity	Informational
Attribute	userId = "x", time = "mm:dd:yyyy hh:mm:ss"
Displayed on the web interface	Administrative account [{userId}] password has expired as of [{time}].
Description	This event occurs when the password expires.

## Admin account lockout

TABLE 625 Admin account lockout event

Event	Admin account lockout
Event Type	Admin account lockout
Event Code	8011
Severity	Warning
Attribute	User Account Name User IP Address Lock Duration Time
Displayed on the web interface	Administrative account [User Account Name] has been locked out because of repeated login failures from [User IP Address], wait for [Lock Duration Time] minutes to re-login.
Description	This event occurs when the account is locked.

## Admin session expired

TABLE 626 Admin session expired event

Event	Admin session expired
Event Type	AdminSessionExpired
Event Code	8012
Severity	Informational
Attribute	userName = "x"
Displayed on the web interface	Administrative account [{userName}] login session has timed out.
Description	This event occurs when the session is timed out due to inactivity or because of absolute session timeout.

## Disable inactive admins

TABLE 627 Disable inactive admins event

Event	Disable inactive admins
Event Type	DisableInactiveAdmins
Event Code	8013
Severity	Informational
Attribute	userName = "x", inactiveDays="x"
Displayed on the web interface	Administrative account [{userName}] has been disabled due to not logging for [{inactiveDays}] days.
Description	This event occurs when the account is disabled for a period of time.

## Two factor auth failed

TABLE 628 Two factor auth failed event

Event	Two factor auth failed
Event Type	TwoFactorAuthFailed
Event Code	8014
Severity	Warning
Attribute	userName = "x"
Displayed on the web interface	Administrative account [{userName}] failed to response the SMS one time password code.
Description	This event occurs when the account fails to send a one time password code as a SMS text.

## Admin account lockout after failed attempts

TABLE 629 Admin account lockout after failed attempts

Event	Admin account lockout after failed attempts
Event Type	Admin account lockout after failed attempts
Event Code	8016
Severity	Warning
Attribute	User account name, User IP address
Displayed on the web interface	Administrative account [User account name] is locked out because of repeated login failure from [User IP Address]
Description	This event occurs when the user account is locked on failed attempts

## Discontinuous time change

TABLE 630 Discontinuous time change

Event	Discontinuous time change
Event Type	Discontinuous time change
Event Code	99301
Severity	Warning

**TABLE 630 Discontinuous time change (continued)**

Event	Discontinuous time change
Attribute	FromTime, ToTime, NTP Server, SZ IP
Displayed on the web interface	The discontinuous time of the controller is changed from [ Fromtime] to [Totime], server: [NTP Server], IP: [SZ IP]
Description	This event occurs when the discontinuous time of the controller changes to more than a minute

## Connected to Data a Streaming Endpoint

**TABLE 631 Connected to Data a Streaming Endpoint event**

Event	Connected to Data a Streaming Endpoint
Event Type	connectedtoDataStreamingEndpoint
Event Code	4701
Severity	Informational
Displayed on the web interface	Connect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ connected to data a streaming endpoint.

## Disconnected to Data a Streaming Endpoint

**TABLE 632 Disconnected to Data a Streaming Endpoint event**

Event	Disconnected to Data a Streaming Endpoint
Event Type	disconnectedtoDataStreamingEndpoint
Event Code	4702
Severity	Warning
Displayed on the web interface	Disconnect to [{connectorType}] with name [{name}], address [{hostname}:{port}].
Description	This event occurs when SZ disconnected to data a streaming endpoint.

## Connected to Data a Streaming Endpoint Failure

**TABLE 633 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.

## Failure of Key Generation

TABLE 634 Failure of Key Generation

Event	Failure of Key Generation
Event Type	keyGenFail
Event Code	99100
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Failure of Key generation. Reason : {{reason}} failed
Description	This event occurs when Smart Zone key generation is failed.

## Failure Certificate

TABLE 635 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.

## Failure of IPsec

TABLE 636 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.

## IPsec KE is Up

TABLE 637 IPsec IKE is Up Event

Event	IPsec IKE is Up
Event Type	IPSecIKEup
Event Code	99103
Severity	Informational

TABLE 637 IPsec IKE is Up Event (continued)

Event	IPsec IKE is Up
Attribute	"ctrlBladeMac"="00:0c:29:de:ae:63", "srcProcess"="strongswan", "SCGMgmtIp"="10.206.66.223", "reason"="System IPsec IKE is up"
Displayed on the web interface	IPsec IKE is Up. Reason : [[reason]] failed
Description	This event occurs when Smart Zone IPsec IKE is up.

## IPsec IKE is Down

TABLE 638 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.

## Switch Events

Following are the events related to switch severity:

- [Switch critical message](#) on page 255
- [Switch alert message](#) on page 255
- [Switch warning message](#) on page 255
- [Switch CPU warning threshold exceed](#) on page 256
- [Switch CPU major threshold exceed](#) on page 256
- [Switch CPU critical threshold exceed](#) on page 256
- [Switch memory warning threshold exceed](#) on page 256
- [Switch memory major threshold exceed](#) on page 257
- [Switch memory critical threshold exceed](#) on page 257
- [Switch custom warning threshold exceed](#) on page 257
- [Switch custom major threshold exceed](#) on page 258
- [Switch custom critical threshold exceed](#) on page 258
- [GetCACert Request](#) on page 258
- [Certificate signing request](#) on page 259
- [Accept certificate signing request](#) on page 259
- [Reject certificate signing request](#) on page 259

- [Pending certificate signing request](#) on page 259
- [Over Switch Max Capacity](#) on page 260
- [Switch Duplicated](#) on page 260
- [Switch Firmware Upgrade](#) on page 261
- [Switch is Offline for 15 Minutes](#) on page 260
- [Switch Firmware Upgrade Failed](#) on page 261
- [Switch Configuration Update](#) on page 261
- [Switch Configuration Update Failed](#) on page 261
- [Switch Reboot](#) on page 262

## Switch critical message

**TABLE 639** Switch critical message event

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

## Switch alert message

**TABLE 640** Switch alert message event

Event	Switch alert message
Event Type	SwitchAlertMessage
Event Code	20001
Severity	Major
Description	This event occurs when there is a switch alert message.

## Switch warning message

**TABLE 641** Switch warning message event

Event	Switch warning message
Event Type	SwitchWarningMessage
Event Code	20003
Severity	Warning
Description	This event occurs when there is a switch warning message.

## Switch CPU warning threshold exceed

TABLE 642 Switch CPU warning threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	warningCpuThresholdExceed
Event Code	22010
Severity	Warning
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (1% - Major Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU warning threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the warning threshold.

## Switch CPU major threshold exceed

TABLE 643 Switch CPU major threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	majorCpuThresholdExceed
Event Code	22011
Severity	Major
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU major threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the major threshold.

## Switch CPU critical threshold exceed

TABLE 644 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"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU critical threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the critical threshold.

## Switch memory warning threshold exceed

TABLE 645 Switch memory warning threshold exceed event

Event	Switch memory warning threshold exceed
Event Type	warningMemoryThresholdExceed



**TABLE 645** Switch memory warning threshold exceed event (continued)

Event	Switch memory warning threshold exceed
Event Code	22020
Severity	Warning
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (1% - Major Threshold), switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory warning threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the warning threshold.

## Switch memory major threshold exceed

**TABLE 646** Switch memory major threshold exceed event

Event	Switch memory major threshold exceed
Event Type	majorMemoryThresholdExceed
Event Code	22021
Severity	Major
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Warning Threshold - Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the major threshold.

## Switch memory critical threshold exceed

**TABLE 647** Switch memory critical threshold exceed event

Event	Switch memory critical threshold exceed
Event Type	criticalMemoryThresholdExceed
Event Code	22022
Severity	Critical
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Major Threshold - 100%),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory critical threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the critical threshold of 100%.

## Switch custom warning threshold exceed

**TABLE 648** Switch custom warning threshold exceed event

Event	Switch custom warning threshold exceed
Event Type	hitWarningSwitchCombinedEvent
Event Code	22030
Severity	Warning
Attribute	UserDefinedDescription = "x"

**TABLE 648** Switch custom warning threshold exceed event (continued)

Event	Switch custom warning threshold exceed
Displayed on the web interface	[Custom Warning Event] {userDefinedDescription}
Description	This event occurs when the Switch custom warning event crosses the threshold.

## Switch custom major threshold exceed

**TABLE 649** Switch custom major threshold exceed event

Event	Switch custom major threshold exceed
Event Type	hitMajorSwitchCombinedEvent
Event Code	22031
Severity	Major
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Major Event] {userDefinedDescription}
Description	This event occurs when the Switch custom major event crosses the threshold.

## Switch custom critical threshold exceed

**TABLE 650** Switch custom critical threshold exceed event

Event	Switch custom critical threshold exceed
Event Type	hitCriticalSwitchCombinedEvent
Event Code	22032
Severity	Critical
Attribute	UserDefinedDescription = "x"
Displayed on the web interface	[Custom Critical Event] {userDefinedDescription}
Description	This event occurs when the Switch custom critical event crosses the threshold.

## GetCACert Request

**TABLE 651** 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.

## Certificate signing request

**TABLE 652** Certificate signing request event

Event	Certificate signing request
Event Type	certificateSigningRequest
Event Code	22001
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Certificate Signing Request.
Description	This event occurs when there is a SCEP Certificate Signing Request.

## Accept certificate signing request

**TABLE 653** Accept certificate signing request event

Event	Accept certificate signing request
Event Type	acceptCertificateSigningRequest
Event Code	22002
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Accept Certificate Signing Request.
Description	This event occurs when there is a SCEP Accept Certificate Signing Request.

## Reject certificate signing request

**TABLE 654** Reject certificate signing request event

Event	Reject certificate signing request
Event Type	rejectCertificateSigningRequest
Event Code	22003
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Reject Certificate Signing Request.
Description	This event occurs when there is a SCEP Reject Certificate Signing Request.

## Pending certificate signing request

**TABLE 655** Pending certificate signing request event

Event	Pending certificate signing request
Event Type	pendingCertificateSigningRequest
Event Code	22004
Severity	Major

**TABLE 655 Pending certificate signing request event (continued)**

Event	Pending certificate signing request
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.

## Over Switch Max Capacity

**TABLE 656 Over Switch Max Capacity event**

Event	Over Switch Max Capacity
Event Type	OverSwitchMaxCapacity
Event Code	21001
Severity	Critical
Displayed on the web interface	The volume of switches is over system capacity.
Description	This event occurs when the volumn of switches is over system capacity

## Switch Duplicated

**TABLE 657 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	[[{switchSerialNumber} / {switchName}] A duplicated switch mac address from {duplicatedSwitchSerialNumber}/{duplicatedSwitchName} is coming while existing one ({switchMac}) is online.
Description	This event occurs when duplicated switches are detected.

## Switch is Offline for 15 Minutes

**TABLE 658 Switch is Offline for 15 Minutes event**

Event	Switch is Offline for 15 Minutes
Event Type	SwitchOffline+B688
Event Code	21000
Severity	Warning
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[[{switchSerialNumber} / {switchName}] offline for more than 15 minutes
Description	This event occurs when the switch is offline over 15 minutes

## Switch Firmware Upgrade

**TABLE 659** Switch Firmware Upgrade event

Event	Switch Firmware Upgrade
Event Type	SwitchFirmwareUpgrade
Event Code	22041
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} Switch firmware upgraded
Description	This event occurs when the switch firmware is upgraded.

## Switch Firmware Upgrade Failed

**TABLE 660** Switch Firmware Upgrade Failed event

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

## Switch Configuration Update

**TABLE 661** Switch Configuration Update event

Event	Switch Configuration Update
Event Type	SwitchConfigurationUpdate
Event Code	22051
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	{{switchSerialNumber} / {switchName}} switch configuration update
Description	This event occurs when the switch configuration is updated.

## Switch Configuration Update Failed

**TABLE 662** Switch Configuration Update Failed event

Event	Switch Configuration Update Failed
Event Type	SwitchConfigurationUpdateFailed
Event Code	22052
Severity	Critical

**TABLE 662 Switch Configuration Update Failed event (continued)**

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

## Switch Reboot

**TABLE 663 Switch Reboot event**

Event	Switch Reboot
Event Type	SwitchReboot
Event Code	22061
Severity	Informational
Attributes	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[[switchSerialNumber] / {switchName}] offline for more than 15 minutes
Description	This event occurs when the Switch re-booted by the controller.

## Switch Delete

**TABLE 664 Switch Delete Event**

Event	Switch Delete
Event Type	switchDeleteByController
Event Code	22071
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch was deleted by the controller.
Description	This event occurs when the switch was deleted by the controller.

## Switch Disconnected from the Controller

**TABLE 665 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.

## Switch is Connected to the Controller

TABLE 666 Switch is Connected to the Controller Event

Event	Switch is Connected to the Controller
Event Type	switchConnectToController
Event Code	22082
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch is connected to the controller.
Description	This event occurs when the switch is connected to the controller.

## Switch Discovered by the Controller

TABLE 667 Switch Discovered by the Controller Event

Event	Switch Discovered by the Controller
Event Type	switchDiscoverByController
Event Code	22091
Severity	Informational
Attribute	"switchSerialNumber"="x",switchName = "x"
Displayed on the web interface	[serialNumber / switchName] Switch discovered by the controller.
Description	This event occurs when the switch is discovered by the controller.

## Threshold Events

Following are the events related to threshold limits.

- [CPU threshold exceeded](#) on page 264
- [Memory threshold exceeded](#) on page 264
- [Disk usage threshold exceeded](#) on page 264
- [CPU threshold back to normal](#) on page 265
- [Memory threshold back to normal](#) on page 265
- [Disk threshold back to normal](#) on page 265
- [The drop of client count threshold exceeded](#) on page 265
- [License threshold exceeded](#) on page 266
- [HDD health degradation](#) on page 266
- [Rate limit threshold surpassed](#) on page 266
- [Rate limit threshold restored](#) on page 267
- [Rate limit for TOR surpassed](#) on page 267
- [The number of users exceed its limit](#) on page 268
- [The number of devices exceeded its limit](#) on page 268

**Events Types**  
Threshold Events

- [Over AP maximum capacity](#) on page 268
- [Over Device Maximum Capacity](#) on page 268
- [Device Capacity Threshold Back to Normal](#) on page 269

## CPU threshold exceeded

**TABLE 668 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 953.

## Memory threshold exceeded

**TABLE 669 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%.
Auto Clearance	This event triggers the alarm 951, which is auto cleared by the event code 954.

## Disk usage threshold exceeded

**TABLE 670 Disk usage threshold exceeded event**

Event	Disk usage threshold exceeded
Event Type	diskUsageThresholdExceeded
Event Code	952
Severity	Critical
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk usage threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This event occurs when the disk usage exceeds the threshold limit of 80%.
Auto Clearance	This event triggers the alarm 952, which is auto cleared by the event code 955.



## CPU threshold back to normal

TABLE 671 CPU threshold back to normal event

Event	CPU threshold back to normal
Event Type	cpuThresholdBackToNormal
Event Code	953
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	CPU threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the CPU usage comes back to normal.

## Memory threshold back to normal

TABLE 672 Memory threshold back to normal event

Event	Memory threshold back to normal
Event Type	memoryThresholdBackToNormal
Event Code	954
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Memory threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the memory usage comes back to normal.

## Disk threshold back to normal

TABLE 673 Disk threshold back to normal event

Event	Disk threshold back to normal
Event Type	diskUsageThresholdBackToNormal
Event Code	955
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the disk usage comes back to normal.

## The drop of client count threshold exceeded

TABLE 674 The drop of client count threshold exceeded event

Event	The drop of client count threshold exceeded
Event Type	clientCountDropThresholdExceeded
Event Code	956
Severity	Warning

**TABLE 674** The drop of client count threshold exceeded event (continued)

Event	The drop of client count threshold exceeded
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%.

## License threshold exceeded

**TABLE 675** License threshold exceeded event

Event	License threshold exceeded
Event Type	licenseThresholdExceeded
Event Code	960
Severity	Critical 90%; Major 80%; Informational 70%;
Attribute	"perc"="xxx", "nodeName"="", "nodeMac"="xx:xx:xx:xx:xx", licenseType="SG00"
Displayed on the web interface	[{{licenseType}}] limit reached at [{{perc}}%]
Description	This event occurs when the number of user equipment attached to the system have exceeded the license limit.

## HDD health degradation

**NOTE**

This event is not applicable for vSZ-H and vSZ-E.

**TABLE 676** HDD health degradation event

Event	HDD health degradation
Event Type	HDDHealthDegradation
Event Code	961
Severity	Critical
Attribute	"nodeName"="xxx", "status"="xxxxx"
Displayed on the web interface	Hard drive detects health degradation [{{status}}] on control plane [{{nodeName}}], please backup the system to prevent losing the data on disk
Description	This event occurs when the hard drive detects health degradation.

## Rate limit threshold surpassed

**TABLE 677** Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major

**TABLE 677 Rate limit threshold surpassed event (continued)**

Event	Rate limit threshold surpassed
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SZMgmtIp"="2.2.2.2" "aaaSrvIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "MOR"=1000 "THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold surpassed for AAA Server [{aaaSrvIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is surpassed. The threshold limit for this event is dependent of the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds the limit of 701.

## Rate limit threshold restored

**TABLE 678 Rate limit threshold restored event**

Event	Rate limit threshold restored
Event Type	rateLimitThresholdRestored
Event Code	1301
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SZMgmtIp"="2.2.2.2" "aaaSrvIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "MOR"=1000 "THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold restored for AAA Server [{aaaSrvIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is restored. The threshold limit for this event is dependent of the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server is lesser or equal to 700.

## Rate limit for TOR surpassed

**TABLE 679 Rate limit for TOR surpassed event**

Event	Rate limit for TOR surpassed
Event Type	rateLimitTORSurpassed
Event Code	1302
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SZMgmtIp"="2.2.2.2" "aaaSrvIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "MOR"=1000 "THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSrvIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This event occurs when the rate limit for total outstanding requests (TOR) is surpassed. Threshold limits for this event is dependent of the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds 1000.
Auto Clearance	This event triggers the alarm1302, which is auto cleared by the event code 1301.

## The number of users exceed its limit

**TABLE 680** The number of users exceed its limit

Event	The number of users exceed its limit
Event Type	tooManyUsers
Event Code	7001
Severity	Major
Attribute	This event has no attributes.
Displayed on the web interface	The number of users exceed its limits. The threshold limit for SZ100 is 114000 and 38000 for vSZ-E.
Description	This event occurs when the number of users exceeds the specified limit.

## The number of devices exceeded its limit

**TABLE 681** The number of devices exceeded its limit event

Event	The number of devices exceeded its limit
Event Type	tooManyDevices
Event Code	7002
Severity	Major
Attribute	This event has not attributes.
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 SZ100 is 342000 and 152000 for vSZ-E.

## Over AP maximum capacity

**TABLE 682** Over AP maximum capacity event

Event	Over AP maximum capacity
Event Type	apCapacityReached
Event Code	962
Severity	Warning
Attribute	
Displayed on the web interface	The volume of AP is over system capacity.
Description	This event occurs when the volume of AP is over system capacity.

## Over Device Maximum Capacity

**TABLE 683** Over Device Maximum Capacity event

Event	Over Device Maximum Capacity
Event Type	connectedDeviceMaxCapacityReached
Event Code	963
Severity	Warning

**TABLE 683 Over Device Maximum Capacity event (continued)**

Event	Over Device Maximum Capacity
Attributes	"deviceType"="xx"
Displayed on the web interface	The volume of {{deviceType}} is over maximum device capacity.
Description	This event is triggered when the volume is over maximum device capacity.

## Device Capacity Threshold Back to Normal

**TABLE 684 Device Capacity Threshold Back to Normal event**

Event	Device Capacity Threshold Back to Normal
Event Type	connectedDeviceThresholdBackToNormal
Event Code	964
Severity	Informational
Displayed on the web interface	The device capacity threshold back to normal
Description	This event occurs when the device capacity threshold back to normal.

## Tunnel Events - Access Point (AP)

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

- [Data plane accepted a tunnel request](#) on page 270
- [Data plane rejected a tunnel request](#) on page 270
- [Data plane terminated a tunnel](#) on page 270
- [AP created a tunnel](#) on page 271
- [AP tunnel disconnected](#) on page 271
- [AP SoftGRE tunnel fails over primary to secondary](#) on page 271
- [AP SoftGRE tunnel fails over secondary to primary](#) on page 272
- [AP SoftGRE gateway reachable](#) on page 272
- [AP SoftGRE gateway not reachable](#) on page 272
- [Data plane set up a tunnel](#) on page 273
- [AP secure gateway association success](#) on page 273
- [AP is disconnected from secure gateway](#) on page 273
- [AP secure gateway association failure](#) on page 273

## Events Types

### Tunnel Events - Access Point (AP)

## Data plane accepted a tunnel request

### NOTE

This event is not applicable for vSZ-E.

**TABLE 685** Data plane accepted a tunnel request event

Event	Data plane accepted a tunnel request
Event Type	dpAcceptTunnelRequest
Event Code	601
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] accepted a tunnel request from AP [{apName&&apMac}].
Description	This event occurs when the data plane accepts a tunnel request from the AP.

## Data plane rejected a tunnel request

### NOTE

This event is not applicable for vSZ-E.

**TABLE 686** 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"="xxxxxxxxxxxx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] rejected a tunnel request from AP [{apName&&apMac}] because of reason [{reason}].
Description	This event occurs when the data plane rejects a tunnel request from the AP.

## Data plane terminated a tunnel

### NOTE

This event is not applicable for vSZ-E.

**TABLE 687** Data plane terminated a tunnel event

Event	Data plane terminated a tunnel
Event Type	dpTearDownTunnel
Event Code	603
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx", "reason"="xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] terminated a tunnel from AP [{apName&&apMac}]. Reason: [{reason}]
Description	This event occurs when the data plane terminates a tunnel from the AP.

## AP created a tunnel

**NOTE**

This event is not applicable for vSZ-E.

**TABLE 688 AP created a tunnel event**

Event	AP created a tunnel
Event Type	apBuildTunnelSuccess
Event Code	608
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dpIP"="xxx.xxx.xxx.xxx",
Displayed on the web interface	AP [{apName&&apMac}] created a tunnel to data plane [{dpIP}].
Description	This event occurs when AP creates a tunnel to the data plane.

## AP tunnel disconnected

**NOTE**

This event is not applicable for vSZ-E.

**TABLE 689 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.

## AP SoftGRE tunnel fails over primary to secondary

**TABLE 690 AP SoftGRE tunnel fails over primary to secondary event**

Event	AP SoftGRE tunnel fails over primary to secondary
Event Type	apSoftGRETunnelFailoverPtoS
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.

## Events Types

### Tunnel Events - Access Point (AP)

## AP SoftGRE tunnel fails over secondary to primary

TABLE 691 AP SoftGRE tunnel fails over secondary to primary event

Event	AP SoftGRE tunnel fails over secondary to primary
Event Type	apSoftGRE TunnelFailoverStoP
Event Code	612
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "primaryGRE"="xxx.xxx.xxx.xxx", "secondaryGRE"="xxxx"
Displayed on the web interface	AP [{apName&&apMac}] fails over from secondaryGRE[{secondaryGRE}] to primaryGRE[{primaryGRE}].
Description	This event occurs when AP moves from a secondary to a primary GRE.

## AP SoftGRE gateway reachable

TABLE 692 AP SoftGRE gateway reachable event

Event	AP SoftGRE gateway reachable
Event Type	apSoftGREGatewayReachable
Event Code	613
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softgreGW"="xxx.xxx.xxx.xxx", "softgreGWAddress"="xxxx"
Displayed on the web interface	AP [{apname&&apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully
Description	This event occurs when AP builds a soft GRE tunnel successfully.

## AP SoftGRE gateway not reachable

TABLE 693 AP SoftGRE gateway not reachable event

Event	AP SoftGRE gateway not reachable
Event Type	apSoftGREGatewayNotReachable
Event Code	614
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softGREGatewayList"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}].
Description	This event occurs when AP fails to build a soft GRE tunnel either on the primary or the secondary GRE.
Auto Clearance	This event triggers the alarm 614, which is auto cleared by the event code 613.



## Data plane set up a tunnel

### NOTE

This event is not applicable for vSZ-E.

**TABLE 694** Data plane set up a tunnel event

Event	Data plane set up a tunnel
Event Type	dpSetUpTunnel
Event Code	627
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] set up a tunnel from AP [{apName&&apMac}]
Description	This event occurs when the data plane sets up a tunnel from the AP.

## AP secure gateway association success

**TABLE 695** AP secure gateway association success event

Event	AP secure gateway association success
Event Type	ipsecTunnelAssociated
Event Code	660
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is able to reach secure gateway [{ipsecGWAddress}] successfully.
Description	This event occurs when the AP is able to reach the secure gateway successfully.

## AP is disconnected from secure gateway

**TABLE 696** AP is disconnected from secure gateway event

Event	AP is disconnected from secure gateway
Event Type	ipsecTunnelDisassociated
Event Code	661
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is disconnected from secure gateway [{ipsecGWAddress}]
Description	This event occurs when the AP is disconnected from secure gateway.

## AP secure gateway association failure

**TABLE 697** AP secure gateway association failure event

Event	AP secure gateway association failure
Event Type	ipsecTunnelAssociateFailed

## Events Types

### Tunnel Events - Data Plane

**TABLE 697 AP secure gateway association failure event (continued)**

Event	AP secure gateway association failure
Event Code	662
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is unable to establish secure gateway with [{ipsecGWAddress}].
Description	This event occurs when the AP is unable to reach the secure gateway.
Auto Clearance	This event triggers the alarm 662, which is auto cleared by the event code 660.

## Tunnel Events - Data Plane

### NOTE

Events 615, 616, 617, 620, 622, 624 and 625 are not applicable for SZ.

Following are the events related to tunnel events on the data plane.

- [DP sGRE GW unreachable](#) on page 274
- [DP sGRE keep alive timeout](#) on page 275
- [DP sGRE GW inactive](#) on page 275
- [DP DHCPRelay no response](#) on page 275
- [DP DHCPRelay failover](#) on page 275
- [DP sGRE new tunnel](#) on page 276
- [DP sGRE keepalive recovery](#) on page 276
- [DP DHCPRelay response recovery](#) on page 276
- [DP sGRE GW reachable](#) on page 277
- [DP sGRE GW active](#) on page 277

## DP sGRE GW unreachable

**TABLE 698 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 dataplane detects that a core network gateway is unreachable.

## DP sGRE keep alive timeout

TABLE 699 DP sGRE keep alive timeout event

Event	DP sGRE keep alive timeout
Event Type	dpSgreKeepAliveTimeout
Event Code	616
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] detected KeepAlive packet to Core Gateway [{{GatewayIP}}] is lost due to timeout
Description	This event occurs when the data plane detects that a keep alive packet to the core network gateway is lost due to a timeout.

## DP sGRE GW inactive

TABLE 700 DP sGRE GW inactive event

Event	DP softGRE GW inactive
Event Type	dpSgreGWInact
Event Code	617
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] detected [{{GatewayIP}}] is inactive because there is no RX traffic
Description	This event occurs when the data plane detects that a core network gateway is inactive.

## DP DHCPRelay no response

TABLE 701 DP DHCPRelay no response event

Event	DP DHCPRelay no response
Event Type	dpDhcpRelayNoResp
Event Code	618
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{{dpName&&dpKey}}] detected no response from DHCP server [{{dhcpIP}}] for a while
Description	This event occurs when the data plane does not get a response from the DHCP server.

## DP DHCPRelay failover

TABLE 702 DP DHCPRelay failover event

Event	DP DHCPRelay failover
Event Type	dpDhcpRelayFailOver
Event Code	619

## Events Types

### Tunnel Events - Data Plane

**TABLE 702 DP DHCPRelay failover event (continued)**

Event	DP DHCPRelay failover
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 fall over.

## DP sGRE new tunnel

**TABLE 703 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", "apIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] established a [greType] tunnel with AP[apIP].
Description	This event occurs when the data plane establishes a tunnel with AP.

## DP sGRE keepalive recovery

**TABLE 704 DP sGRE keepalive recovery event**

Event	DP sGRE keepalive recovery
Event Type	dpSgreKeepAliveRecovery
Event Code	622
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected KeepAlive packet to Core Gateway [gatewayIP] is now responsive.
Description	The event occurs when the core gateway resumes answering to keepalive.

## DP DHCPRelay response recovery

**TABLE 705 DP DHCPRelay response recovery event**

Event	DP DHCPRelay response recovery
Event Type	dpDhcpRelayRespRecovery
Event Code	623
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected DHCP server [dhcpIP] is now responsive.
Description	This event occurs when the DHCP server resumes to answer the relay request from data plane.

## DP sGRE GW reachable

TABLE 706 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.

## DP sGRE GW active

TABLE 707 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.

## AP Ethernet PHY Down Shift

TABLE 708 AP Ethernet PHY Down Shift event

Event	AP Ethernet PHY Down Shift
Event Type	ethPhyDownShift
Event Code	354
Severity	Major
Attribute	"apName"="xxxx", "apMac"="xx:xx:xx:xx:xx:xx", "linkDs"="xxxx"
Displayed on the web interface	AP [[apName&&apMac]] ethPhyDownShift [[linkDs]].
Description	This event triggers when the ethernet PHY downshift the link speed.

## Events Types

### AP Ethernet Phy Error Count

# AP Ethernet Phy Error Count

TABLE 709 AP Ethernet Phy Error Count event

Event	AP Ethernet Phy Error Count
Event Type	ethPhyError
Event Code	353
Severity	Informational
Attribute	"apName"="xxxx", "apMac"="xx:xx:xx:xx:xx:xx", "linkDs"="xxxx"
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.



© 2022 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>