Ruckus

Simply Better Wireless.

Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone™ Essentials

Alarm and Event Reference Guide for SmartZone 3.5.1

Part Number 800-71513-001 Rev A
Published June 2017

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Contents

About This Guide

Document Conventions . . . 20
Terminology . . . 21
Related Documentation . . . 22
Online Training Resources . . . 22
Documentation Feedback . . . 23

1 Revision History

SmartZone Version 3.5.1 . . . 25
New Event . . . 25
SmartZone Version 3.5 . . . 25
Deprecated Alarm and Event . . . 25
New Alarm . . . 25
New Event . . . 26
SmartZone Version 3.4.1 . . . 28
SmartZone Version 3.4 . . . 28
New Alarm . . . 28
Displayed on the Web Interface . . . 29
New Event . . . 30
SmartZone Version 3.2.1 . . . 31
New Alarm . . . 31
New Event . . . 31
Event on Web Interface . . . 31
SmartZone Version 3.2 . . . 32
New Alarm . . . 32
Attribute Change . . . 32
Renamed Alarm . . . 33
New Event . . . 33
Severity Change . . . 35
Attribute Change . . . 35
Renamed Event . . . 35
Auto Clearance of Event . . . 36
SmartZone Version 3.1.1 . . . 36

New Alarm 36
New Event 36
Re-added Event 37
Renamed Event 37
Deprecated Event 37
RuckOS Version 3.1 38
New Alarm 38
Deprecated Alarm 38
Renamed Alarm Type 38
Renamed Alarm 39
New Event 39
Renamed Event 40

2 Alarm and Event Management

Overview. 44
Alarm and Event Management 44
Event Categories 44
Event Attributes 45
Generation of Alarm and Event. 45

3 Alarm Types

Accounting Alarms 50
Accounting server not reachable 50
AP Authentication Alarms 51
RADIUS server unreachable. 51
LDAP server unreachable. 52
AD server unreachable. 52
WeChat ESP authentication server unreachable. 53
WeChat ESP authentication server unresolvable 54
WeChat ESP DNAT server unreachable 54
WeChat ESP DNAT server unresolvable. 55
AP Communication Alarms 56
AP rejected 56
AP configuration update failed 57
AP swap model mismatched 57
AP pre-provision model mismatched 58
AP firmware update failed 59
AP WLAN oversubscribed 60
AP LBS Alarms 61

No LS responses 61
LS authentication failure 62
AP failed to connect to LS 63
AP State Change Alarms 64
AP rebooted by system 64
AP disconnected 65
AP deleted 65
AP cable modem interface down 66
AP DHCP service failure 66
AP NAT failure 67
Authentication Alarms 68
Authentication server not reachable 68
Authentication failed over to secondary 69
Authentication fallback to primary 69
AD/LDAP connectivity failure 70
Bind fails with AD/LDAP 71
Bind success with LDAP, but unable to find clear text password for the user 72
RADIUS fails to connect to AD NPS server 73
RADIUS fails to authenticate with AD NPS server 74
Fails to establish TLS tunnel with AD/LDAP 75
Control and Data Plane Interface Alarms 76
GtpManager (DP) disconnected 76
Cluster Alarms 77
New node failed to join 78
Node removal failed 79
Node out of service 79
Cluster in maintenance state 80
Cluster backup failed 81
Cluster restore failed 82
Cluster upgrade failed 83
Cluster application stopped 84
Node bond interface down 84
Node physical interface down 85
Cluster node rebooted 86
Cluster node shut down 86
Disk usage exceed threshold 87
Cluster out of service 88
Cluster upload AP firmware failed 88
Cluster add AP firmware failed 89

Unsync NTP time . . . 89
Cluster upload KSP file failed . . . 89
Configuration backup failed . . . 90
Configuration restore failed . . . 90
AP Certificate Expired . . . 92
Configuration Alarms. . . . 93
Zone configuration preparation failed . . . 93
AP configuration generation failed . . . 94
End-of-life AP model detected . . . 95
VLAN configuration mismatch on non DHCP/NAT WLAN . . . 96
VLAN configuration mismatch on DHCP/NAT WLAN . . . 97
Data Plane Alarms . . . 98
Data plane configuration update failed . . . 98
Data plane disconnected . . . 99
Data plane physical interface down . . . 99
Data plane process restarted . . . 100
Data plane license is not enough . . . 100
Data plane upgrade failed . . . 101
Data plane of data center side fails to connect to the CALEA server. . . . 102
Data Plane fails to connects to the other data plane. . . . 103
Data Plane DHCP IP Pool usage rate is 100 percent . . . 104
IPMI Alarms . . . 105
ipmiThempBB . . . 105
ipmiThempP . . . 106
ipmiFan . . . 106
ipmiFanStatus . . . 107
Licensing Interface Alarms . . . 108
License going to expire . . . 108
Insufficient license capacity . . . 109
SCI Alarms . . . 110
Connect to SCI failure . . . 110
SCI has been disabled . . . 110
SCI and FTP have been disabled . . . 111
System Alarms . . . 112
No LS responses . . . 112
LS authentication failure . . . 113
{produce.short.name} failed to connect to LS . . . 113
Syslog server unreachable . . . 114
Process restart. . . . 114

Service unavailable . . . 115
Keepalive failure . . . 115
Resource unavailable . . . 116
HIP failed over . . . 117
The last one data plane is disconnected zone affinity profile . . . 118
Threshold Alarms . . . 119
CPU threshold exceeded . . . 119
Memory threshold exceeded . . . 120
Disk usage threshold exceeded . . . 120
License threshold exceeded . . . 121
Rate limit for TOR surpassed . . . 122
The number of users exceeded its limit . . . 122
The number of devices exceeded its limit . . . 123
Tunnel Alarms - Access Point . . . 124
AP softGRE gateway not reachable . . . 124
AP is disconnected from secure gateway . . . 125
AP secure gateway association failure . . . 126
4 Events Types
Accounting Events . . . 128
Accounting server not reachable . . . 128
AP accounting response while invalid config . . . 129
AP account message drop while no accounting start message . . . 130
Unauthorized COA/DM message dropped . . . 131
AP Communication Events . . . 132
AP discovery succeeded . . . 132
AP managed . . . 133
AP rejected . . . 133
AP firmware updated . . . 134
AP firmware update failed . . . 134
Updating AP firmware . . . 135
Updating AP configuration . . . 135
AP configuration updated . . . 136
AP configuration update failed . . . 136
AP pre-provision model mismatched . . . 137
AP swap model mismatched . . . 137
AP WLAN oversubscribed . . . 138
AP illegal to change country code . . . 138
AP configuration get failed . . . 139

Rogue AP 139
SSID-spoofing rogue AP 139
Mac-spoofing rogue AP 141
Same-network rogue AP 141
Ad-hoc network device 142
Rogue AP disappeared 142
AP LBS Events 143
No LS responses 143
LS authentication failure 144
AP connected to LS. 144
AP failed to connect to LS 145
AP started location service 145
AP stopped location service 146
AP received passive calibration request 146
AP received passive footfall request 147
AP received unrecognized request 147
AP Mesh Events 148
EMAP downlink connected to MAP 148
EMAP downlink disconnected from MAP 149
EMAP uplink connected to MAP 149
EMAP uplink disconnected from MAP 150
MAP disconnected. 150
MAP downlink connected 150
MAP downlink connected to EMAP 151
MAP downlink disconnected from EMAP 151
RAP downlink connected to MAP 152
MAP uplink connected to EMAP 152
MAP uplink disconnected from EMAP 153
MAP uplink connected to RAP 153
MAP uplink connected to MAP 154
Mesh state updated to MAP 154
Mesh state updated to MAP no channel 155
Mesh state updated to RAP 155
Mesh state update to RAP no channel 156
MAP downlink connected to MAP 156
MAP downlink disconnected from MAP 157
RAP downlink disconnected from MAP 157
AP State Change Events 158
AP rebooted by user 159

AP rebooted by system 159
AP disconnected 160
AP IP address updated 160
AP reset to factory default 161
AP channel updated 161
AP country code updated 162
AP channel updated because dynamic frequency selection (DFS) detected a radar . . 162
AP change control plane 163
AP connected 163
AP deleted 164
AP heartbeat lost 164
AP tagged as critical 164
AP cable modem interface down 165
AP brownout 165
AP cable modem power-cycled by user 166
AP smart monitor turn off WLAN 166
AP client load balancing limit reached 167
AP client load balancing limit recovered 167
AP WLAN state changed 168
AP capacity reached 168
AP capacity recovered 169
AP cable modem interface up 169
AP cable modem soft-rebooted by user 170
AP cable modem set to factory default by user 170
AP health high latency flag 171
AP health low capacity flag 171
AP health high connection failure flag 172
AP health high client count flag 172
AP health high latency clear 173
AP health low capacity clear 173
AP health high connection failure clear 174
AP health high client count clear 174
Primary DHCP AP is down 175
Primary DHCP AP is up 175
Secondary DHCP AP is down 176
Secondary DHCP AP is up 176
Primary or secondary DHCP AP detects 90% of the configured total IPs 177
Both primary and secondary DHCP server APs are down 177
AP NAT gateway IP failover detected for particular VLAN pool 178

AP NAT gateway IP fall back detected for particular VLAN pool 178
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 179
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 180
AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down 181
AP health high airtime utilization flag. 181
AP health high airtime utilization clear. 182
AP Authentication Events 183
Radius server reachable. 183
Radius server unreachable 184
LDAP server reachable. 184
LDAP server unreachable. 185
AD server reachable. 185
AD server unreachable. 186
Wechat ESP authentication server reachable 186
WeChat ESP authentication server unreachable. 187
WeChat ESP authentication server resolvable 187
WeChat ESP authentication server unresolvable 188
WeChat ESP DNAT server reachable 188
WeChat ESP DNAT server unreachable 189
WeChat ESP DNAT server resolvable. 189
WeChat ESP DNAT server unresolvable. 190
AP USB Events. 191
AP USB software package downloaded. 191
AP USB software package download failed 191
Authentication Events 192
Authentication server not reachable 192
Authentication failed over to secondary 193
Authentication fallback to primary. 193
AD/LDAP connected successfully 194
AD/LDAP connectivity failure 194
Bind fails with AD/LDAP. 195
Bind success with LDAP, but unable to find clear text password for the user. 195
RADIUS fails to connect to AD NPS server. 196
RADIUS fails to authenticate with AD NPS server. 196
Successfully established the TLS tunnel with AD/LDAP 197
Fails to establish TLS tunnel with AD/LDAP 198

Authorization Events 199
DM received from AAA. 199
DM NACK sent to AAA 200
DM sent to NAS. 200
DM NACK received from NAS 201
CoA received from AAA 201
CoA NACK sent to AAA 202
CoA sent NAS 202
CoA NAK received NAS. 203
CoA authorize only access reject 203
CoA RWSG MWSG notification failure 204
Control and Data Plane Interface Events 205
DP connected 205
GtpManager (DP) disconnected 206
Session updated at DP 206
Session update at DP failed 207
Session deleted at DP 207
Session delete at DP failed. 208
C2d configuration failed 209
Client Events. 210
Client authentication failed 211
Client joined. 211
Client failed to join 212
Client disconnected 212
Client connection timed out 213
Client authorization successfully. 213
Client authorization failed 214
Client session expired 214
Client roaming 215
Client logged out 215
Client roaming disconnected 216
Client blocked 216
Client grace period. 217
Onboarding registration succeeded 217
Onboarding registration failed 218
Remediation succeeded 218
Remediation failed 219
Force DHCP disconnected 219
WDS device joined. 220

WDS device left 220
Client is blocked because of barring UE rule 221
Client is unblocked because of barring UE rule. 221
Start CALEA mirroring client. 222
Stop CALEA mirroring client. 222
Wired client joined 223
Wired client failed to join. 223
Wired client disconnected 224
Wired client authorization successfully 224
Wired client session expired. 225
Cluster Events. 226
Cluster created successfully. 227
New node joined successfully 227
New node failed to join. 228
Node removal completed. 228
Node removal failed 229
Node out of service 229
Cluster in maintenance state 230
Cluster back in service 230
Cluster backup completed. 230
Cluster backup failed 231
Cluster restore completed 231
Cluster restore failed 232
Cluster node upgrade completed. 232
Entire cluster upgraded successfully 233
Cluster upgrade failed 233
Cluster application stopped 234
Cluster application started 234
Cluster backup started. 235
Cluster upgrade started 235
Cluster leader changed 236
Node bond interface down. 236
Node bond interface up 237
Node IP address changed 237
Node physical interface down 238
Node physical interface up. 238
Cluster node rebooted 239
NTP time synchronized 240
Cluster node shutdown 240

Cluster upload started 241
Cluster upload completed 241
Cluster upload failed 242
SSH tunnel switched 242
Cluster remove node started 243
Node back in service 243
Disk usage exceed threshold 244
Cluster out of service 244
Initiated moving APs in node to a new cluster 245
Cluster upload vSZ-D firmware started. 245
Cluster upload vSZ-D firmware completed 246
Cluster upload vSZ-D firmware failed 246
Cluster upload AP firmware started 247
Cluster upload AP firmware completed 247
Cluster upload AP firmware failed. 248
Cluster add AP firmware started 248
Cluster add AP firmware completed. 249
Cluster add AP firmware failed 249
Cluster name is changed 250
Unsync NTP time 250
Cluster upload KSP file started. 251
Cluster upload KSP file completed 251
Cluster upload KSP file failed 251
Configuration backup started 252
Configuration backup succeeded. 252
Configuration backup failed 253
Configuration restore succeeded 253
Configuration restore failed 253
AP Certificate Expired 254
AP Certificate Updated 254
Configuration restore started 255
Upgrade SSTable failed 255
Reindex Elastic Search finished 256
Initiated APs contact APR 256
Node IPv6 address added 257
Node IPv6 address deleted 257
Configuration Events. 258
Configuration updated 258
Configuration update failed 258

Configuration receive failed 259
Incorrect flat file configuration. 259
Zone configuration preparation failed 260
AP configuration generation failed 260
End-of-life AP model detected 262
VLAN configuration mismatch on non-DHCP/NAT WLAN 262
VLAN configuration mismatch on a DHCP/NAT WLAN 263
Data Plane Events. 264
Data plane discovered 265
Data plane discovery failed. 265
Data plane configuration updated 265
Data plane configuration update failed 267
Data plane rebooted 267
Data plane heartbeat lost 268
Data plane IP address updated 268
Data plane updated to a new control plane 268
Data plane status update failed 269
Data plane statistics update failed 269
Data plane connected 270
Data plane disconnected 270
Data plane physical interface down 271
Data plane physical interface up. 271
Data plane packet pool is under low water mark 272
Data plane packet pool is under critical low water mark 272
Data plane packet pool is above high water mark 273
Data plane core dead. 273
Data plane process restarted 274
Data plane discovery succeeded 274
Data plane managed 275
Data plane deleted. 275
Data plane license is not enough 276
Data plane upgrade started 276
Data plane upgrading. 277
Data plane upgrade succeeded 277
Data plane upgrade failed 278
Data plane of data center side successfully connects to the CALEA server 278
Data plane of data center side fails to connect to the CALEA server. 279
Data plane successfully connects to the other data plane 279
Data plane fails to connects to the other data plane 280

Data plane disconnects to the other data plane 280
Start CALEA mirroring client. 281
Stop CALEA mirroring client. 281
Data plane DHCP IP pool usage rate is 100 percent 282
Data plane DHCP IP pool usage rate is 80 percent 282
IPMI Events. 283
ipmiThempBB 283
ipmiThempP 284
ipmiFan 284
ipmiFanStatus 285
ipmiREThempBB 285
ipmiREThempP 286
ipmiREFan 286
ipmiREFanStatus 287
Licensing Interface Events. 288
License sync succeeded 288
License sync failed. 289
License import succeeded. 289
License import failed 290
License data changed 290
License going to expire 291
Insufficient license capacity 291
SCI Events 292
Connect to SCI 292
Disconnect to SCI 292
Connect to SCI failure 293
SCI has been disabled 293
SCI and FTP have been disabled 294
Session Events 295
Delete all sessions 295
System Events 296
No LS responses 297
LS authentication failure. 297
{produce.short.name} connected to LS 298
{produce.short.name} failed to connect to LS 298
{produce.short.name} received passive request. 299
{produce.short.name} sent controller information report. 299
{produce.short.name} received management request 300
{produce.short.name} sent AP info by venue report 300

{produce.short.name} sent query venues report. 301
{produce.short.name} sent associated client report 301
{produce.short.name} forwarded calibration request to AP 302
{produce.short.name} forwarded footfall request to AP 302
{produce.short.name} received unrecognized request 303
Syslog server reachable 303
Syslog server unreachable 304
Syslog server switched 304
Generate AP config for plane load rebalance succeeded 305
Generate AP config for plane load rebalance failed. 305
FTP transfer 306
FTP transfer error. 306
File upload 306
Email sent successfully 307
Email sent failed 307
SMS sent successfully 308
SMS sent failed 308
Process restart. 309
Service unavailable. 309
Keepalive failure 310
Resource unavailable 310
Data plane of data center side successfully connects to the CALEA server 311
Data plane of data center side fails to connect to the CALEA server. 311
Data Plane of data center side disconnects to CALEA server. 312
Data plane successfully connects to the other data plane 312
Data plane fails to connects to the other data plane. 313
Data plane disconnects to the other data plane 313
Start CALEA mirroring client in data plane 314
Stop CALEA mirroring client in data plane 314
Data plane DHCP IP pool usage rate is 100 percent 315
Data plane DHCP IP pool usage rate is 80 percent 315
All data planes in the zone affinity profile are disconnected. 316
CALEA UE Matched. 316
ZD AP migrating. 317
ZD AP migrated 317
ZD AP rejected. 318
ZD AP migration failed 318
Database error. 319
Database error. 319

Threshold Events 321
CPU threshold exceeded 321
Memory threshold exceeded 322
Disk usage threshold exceeded 322
CPU threshold back to normal 323
Memory threshold back to normal 323
Disk threshold back to normal 323
License threshold exceeded. 324
Rate limit threshold surpassed 324
Rate limit threshold restored 325
Rate limit for TOR surpassed 326
The number of users exceed its limit 326
The number of devices exceeded its limit. 327
Tunnel Events - Access Point (AP) 328
Data plane accepted a tunnel request 328
Data plane rejected a tunnel request 329
Data plane terminated a tunnel. 329
AP created a tunnel 330
AP tunnel disconnected 330
AP SoftGRE tunnel fails over primary to secondary 331
AP SoftGRE tunnel fails over secondary to primary 331
AP SoftGRE gateway reachable. 332
AP SoftGRE gateway not reachable. 332
Data plane set up a tunnel 333
AP secure gateway association success 333
AP is disconnected from secure gateway. 334
AP secure gateway association failure 334
Tunnel Events - Data Plane. 335
DP Core GW unreachable 335
DPs GRE keep alive timeout 336
DP Core GW inactive 336
DP DHCPRelay no response 337
DP DHCPRelay failover 337
DP sGRE new tunnel 338
DP sGRE keepalive recovery 338
DP DHCPRelay response recovery 339
DP Core GW reachable 339
DP Core GW active 340

Index

About This Guide

This *SmartZone™ Alarm and Event Reference Guide* describes the various types of alarms and events that the controller (SZ-100 or vSZ-E) 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 Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

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

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

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name] >`
`monospace bold`	Represents information that you enter	`[Device name] >` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

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
CoA	Change of Authorization
Controller	Refers to either SZ-100 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

Table 3. Terms used

Term	Description
MTU	Maximum Transmission Unit
MWSG	Metro Wireless Security Gateway
NAS	Network Access Server
NTP	Network Time Protocol)
PDP	Packet Data Protocol
produce.short.name	Refers to either SZ-100 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

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Online Training Resources

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

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

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

For example:

- SZ-100 and vSZ-E Alarm and Event Reference Guide for SmartZone 3.5.1
- Part number: 800-71513-001
- Page 60

Revision History

1

This chapter contains revision history for:

- SmartZone Version 3.5.1
- SmartZone Version 3.5
- SmartZone Version 3.4.1
- SmartZone Version 3.4
- SmartZone Version 3.2.1
- SmartZone Version 3.2
- SmartZone Version 3.1.1
- RuckOS Version 3.1

SmartZone Version 3.5.1

The following are the changes for version 3.5.1.

New Event

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

SmartZone Version 3.5

The following are the changes for version 3.5.

Deprecated Alarm and Event

Code	Type	Replace With
Alarm 835 and Event 837	resyncNTPTime	Alarm and Event 855 - unsyncNTPTime

New Alarm

- Description for Alarm 346 is changed.

Alarm Code	Alarm
341	apDHCPServiceFailure
346	apNATFailureDetectedbySZ
855	unsyncNTPTime
858	clusterUploadKspFileFailed
974	csvFtpTransferMaxRetryReached
975	csvDiskThreshholdExceeded

Alarm Code	Alarm
976	csvDiskMaxCapacityReached
1024	apCfgNonDhcpNatWlanVlanConfigMismatch
1025	apCfgDhcpNatWlanVlanConfigMismatch
1258	dpDcToCaleaConnectFail
1261	dpP2PTunnelConnectFail
1265	dpDhcpIpPoolUsageRate100
1267	zoneAffinityLastDpDisconnected
1762	racADLDAPTLSFailed
4003	disabledSciDueToUpgrade
4004	disabledSciDueToUpgrade
4005	disabledSciAndFtpDueToMutuallyExclusive

New Event

Event Code	Event
117	apGetConfigFailed
228	clientBlockByBarringUERule
229	clientUnblockByBarringUERule
328	apHealthLatencyFlag
329	apHealthCapacityFlag
330	apHealthConnectionFailureFlag
331	apHealthClientCountFlag
332	apHealthLatencyClear
333	apHealthCapacityClear
334	apHealthConnectionFailureClear
335	apHealthClientCountClear
336	apDHCPFailoverDetected
337	apDHCPFallbackDetected
338	apSecondaryDHCPAPDown

Event Code	Event
339	apSecondaryDHCPAPUp
340	apDHCPIPPoolMaxThresholdReached
341	apDHCPServiceFailure
342	apNATFailoverDetected
343	apNATFallbackDetected
344	apNATVlanCapacityAffected
345	apNATVlanCapacityRestored
346	apNATFailureDetectedbySZ
347	apHealthAirUtilizationFlag
348	apHealthAirUtilizationClear
855	unsyncNTPTime
869	Reindex ElasticSearch finished
870	clusterInitContactApr
972	csvFtpTransfer
973	csvFtpTransferError
974	csvFtpTransferMaxRetryReached
975	csvDiskThreshholdExceeded
976	csvDiskMaxCapacityReached
977	csvDiskThreshholdBackToNormal
1024	apCfgNonDhcpNatWlanVlanConfigMismatch
1025	apCfgDhcpNatWlanVlanConfigMismatch
1257	dpDcToCaleaConnected
1258	dpDcToCaleaConnectFail
1259	dpDcToCaleaDisconnected
1268	dpCaleaUeInterimMatched’
1260	dpP2PTunnelConnected
1261	dpP2PTunnelConnectFail
1262	dpP2PTunnelDisconnected

Event Code	Event
1263	dpStartMirroringClient
1264	dpStopMirroringClient
1265	dpDhcpIpPoolUsageRate100
1266	dpDhcpIpPoolUsageRate80
1267	zoneAffinityLastDpDisconnected
1761	racADLDAPTLSSuccess
1762	racADLDAPTLSFailed
4001	connectedToSci
4002	disconnectedFromSci
4003	disabledSciDueToUpgrade
4004	disabledSciDueToUpgrade
4005	disabledSciAndFtpDueToMutuallyExclusive

SmartZone Version 3.4.1

No changes to this version.

SmartZone Version 3.4

The following are the changes for version 3.4.

New Alarm

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

Displayed on the Web Interface

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

New Event

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

SmartZone Version 3.2.1

The following are the changes for version 3.2.1.

New Alarm

Alarm Code	Alarm
865	apCertificateExpire

New Event

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

Event on Web Interface

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

SmartZone Version 3.2

The following are the changes for version 3.2.

New Alarm

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

Attribute Change

Table 4.

Module	Attribute	Attribute Change
DataPlane	dpMac	dpKey

Renamed Alarm

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

New Event

Event Code	Event
370	apUsbSoftwarePackageDownloaded
371	apUsbSoftwarePackageDownloadFailed
516	dpPktPoolLow
517	dpPktPoolCriticalLow
518	dpPktPoolRecover
519	dpCoreDead
530	dpDiscoverySuccess
532	dpStatusManaged
537	dpDeleted
538	dpLicenseInsufficient
550	dpUpgradeStart
551	dpUpgrading
552	dpUpgradeSuccess
553	dpUpgradeFailed
615	dpSgreGWUnreachable
616	dpSgreKeepAliveTimeout
617	dpSgreGWInact
620	dpSgreNewTunnel

Event Code	Event
622	dpSgreKeepAliveRecovery
624	dpSgreGWReachable
625	dpSgreGWAct
750	syslogServerReachable
751	syslogServerUnreachable
752	syslogServerSwitched
770	planeLoadingRebalancingSucceeded
771	planeLoadingRebalancingFailed
845	clusterUploadVDPFirmwareStart
846	uploadClusterVDPFirmwareSuccess
847	uploadClusterVDPFirmwareFailed
1255	licenseGoingToExpire
1256	apConnectionTerminatedDueToInsufficientLicense
1751	racADLDAPSuccess
1752	racADLDAPFail
1753	racADLDAPBindFail
1754	racLDAPFailToFindPassword
1755	racADNPSFail
1756	racADNPSFailToAuthenticate
2151	espAuthServerReachable
2152	espAuthServerUnreachable
2153	espAuthServerResolvable
2154	espAuthServerUnResolvable
2161	espDNATServerReachable
2162	espDNATServerUnreachable
2163	espDNATServerResolvable
2164	espDNATServerUnresolvable

Severity Change

Event Code and Event	Severity Changed From	Severity Changed To
837 - resyncNTPTime	Informational	Major
2102 - radiusServerUnreachable	Informational	Major
2122 - ldapServerUnreachable	Informational	Major
2142 - adServerUnreachable	Informational	Major

Attribute Change

Module	Attribute	Attribute Change
Data Plane	dpMac	dpKey
AP Communication Events System Events	“model"="ZF7343"	"model"="R700”
System Events	"model"="ZF7962", “firmware”=“3.0.0.0.0”	"model"="R700", “firmware”=“3.2.0.0.x”

Renamed Event

Event Code	Event Name	Renamed To
320	AP CLB limit reached	AP client load balancing limit reached
321	AP CLB limit recovered	AP client load balancing limit recovered
619	DP DHCPRelay failOver	DP DHCPRelay failover
1202	DP Disconnected	GtpManager (DP) disconnected

Auto Clearance of Event

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

SmartZone Version 3.1.1

The following are the changes for version 3.1.1.

New Alarm

Alarm Code	Alarm
661	ipsecTunnelDisassociated
662	ipsecTunnelAssociateFailed

New Event

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

Event Code	Event
2122	ldapServerUnreachable
2141	adServerReachable
2142	adServerUnreachable
2201	zoneInitiatedMovingAp
2501	nodeIPv6Added
2502	nodeIPv6Deleted

Re-added Event

Event Code	Event
101	apDiscoverySuccess

Renamed Event

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

Deprecated Event

Event Code	Event Name
1604	authSuccess
1605	authFailed

RuckOS Version 3.1

The following are the changes for version 3.1.

New Alarm

Alarm Code	**Alarm**
520	dpProcessRestart
862	clusterCfgBackupFailed
864	clusterCfgRestoreFailed
902	ipmiThempBB
1651	authFailedOverToSecondary
1652	authFallbackToPrimary
7003	tooManyUsers
7004	tooManyDevices

Deprecated Alarm

Alarm Code	**Alarm**
1008	cfgUpdFailed
1909	apAcctRespWhileInvalidConfig

Renamed Alarm Type

Alarm Code	**Alarm Type**	**Renamed To**
843	clusterOutofService	clusterOutOfService

Renamed Alarm

Alarm Code	Alarm Type	Renamed To
701	No LS Responses	No LS responses
721	No LS Responses	No LS responses
1302	Rate Limit for TOR surpassed	Rate limit for TOR surpassed

New Event

Event Code	Event
223	remediationSuccess
224	remediationFailure
325	cableModemUp
520	dpProcessRestart
627	dpSetUpTunnel
860	clusterCfgBackupStart
861	clusterCfgBackupSuccess
862	clusterCfgBackupFailed
863	clusterCfgRestoreSuccess
864	clusterCfgRestoreSuccess
902	ipmiThempBB
927	ipmiREThempBB
932	ipmiREThempP
934	ipmiREFan
937	ipmiREFanStatus
953	cpuThresholdBackToNormal
954	memoryThresholdBackToNormal
955	diskUsageThresholdBackToNormal
1651	authFailedOverToSecondary
1652	authFallbackToPrimary

Event Code	Event
7001	tooManyUsers
7002	tooManyDevices

Renamed Event

Event Code	Event Name	Renamed To
181	Ssid-spoofing rogue AP	SSID-spoofing rogue AP
209	Client Roaming	Client roaming
220	Client Grace Period	Client grace period
308	AP channel updated because Dynamic Frequency Selection (DFS) detected a radar event	AP channel updated because dynamic frequency selection (DFS) detected a radar event
317	AP Brownout	AP brownout
323	AP capacity Reached	AP capacity reached
405	eMAP downlink connected to MAP	EMAP downlink connected to MAP
406	eMAP downlink disconnected from MAP	EMAP downlink disconnected from MAP
407	eMAP uplink connected to MAP	EMAP uplink connected to MAP
408	eMAP uplink disconnected from MAP	EMAP uplink disconnected from MAP
422	Mesh state updated to MAP No Channel	Mesh state updated to MAP no channel
424	Mesh state update to RAP No Channel	Mesh state update to RAP no channel
515	Data plane physical Interface Up	Data plane physical interface up
615	DP SoftgreGW Unreachable	DP softGRE GW unreachable
618	DP DhcpRelay No Resp	DP DHCPRelay no response
619	DP DhcpRelay FailOver	DP DHCPRelay failOver

Event Code	Event Name	Renamed To
623	DP DhcpRelay Resp Recovery	DP DHCPRelay response recovery
701	No LS Responses	No LS responses
707	AP received Passive Calibration Request	AP received passive calibration request
708	AP received Passive Footfall Request	AP received passive footfall request
709	AP received Unrecognized Request	AP received unrecognized request
721	No LS Responses	No LS responses
725	SCG received Passive Request	SCG received passive request
727	SCG sent Controller Information report	SCG sent controller information report
728	SCG received Management Request	SCG received management request
729	SCG sent AP Info by Venue Report	SCG sent AP info by venue report
730	SCG sent Query Venues Report	SCG sent query venues report
731	SCG sent Associated Client Report	SCG sent associated client report
732	SCG forwarded Calibration Request to AP	SCG forwarded calibration request to AP
733	SCG forwarded Footfall Request to AP	SCG forwarded footfall request to AP
734	SCG received Unrecognized Request	SCG received unrecognized request
833	SSH Tunnel Switched	SSH tunnel switched
837	Resync NTP Time	Resync NTP time
970	FTP Transfer	FTP transfer
971	FTP Transfer Error	FTP transfer error

Event Code	Event Name	Renamed To
980	File Upload	File upload
981	Email Sent Successfully	Email sent successfully
982	Email Sent Failed	Email sent failed
983	SMS Sent Successfully	SMS sent successfully
984	SMS Sent Failed	SMS sent failed
1012	Incorrect Flat File Configuration	Incorrect flat file configuration
1647	CoA Sent NAS	CoA sent NAS
1648	CoA NAK Received NAS	CoA NAK received NAS
1649	CoA Authorize Only Access Reject	CoA authorize only access reject
1650	CoA RWSG MWSG Notification Failure	CoA RWSG MWSG notification failure
2001	ZD AP Migrating	ZD AP migrating
2002	ZD AP Migrated	ZD AP migrated
2003	ZD AP Rejected	ZD AP rejected
2004	ZD AP Migration Failed	ZD AP migration failed
1302	Rate Limit for TOR surpassed	Rate limit for TOR surpassed
1911	Unauthorized CoA/DM message dropped	Unauthorized COA/DM message dropped
1641	DM Received from AAA	DM received from AAA
1643	DM Sent to NAS	DM sent to NAS
1644	DM NACK Received from NAS	DM NACK received from NAS
1645	CoA Received from AAA	CoA received from AAA

Alarm and Event Management

2

In this chapter:

- Overview
- Alarm and Event Management

Overview

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

NOTE: Refer to About This Guide for the conventions used in this guide.

Alarm and Event Management

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

- Event Categories
- Event Attributes
- Generation of Alarm and Event

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 due to the volume. 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 involved in generating an alarm or event.

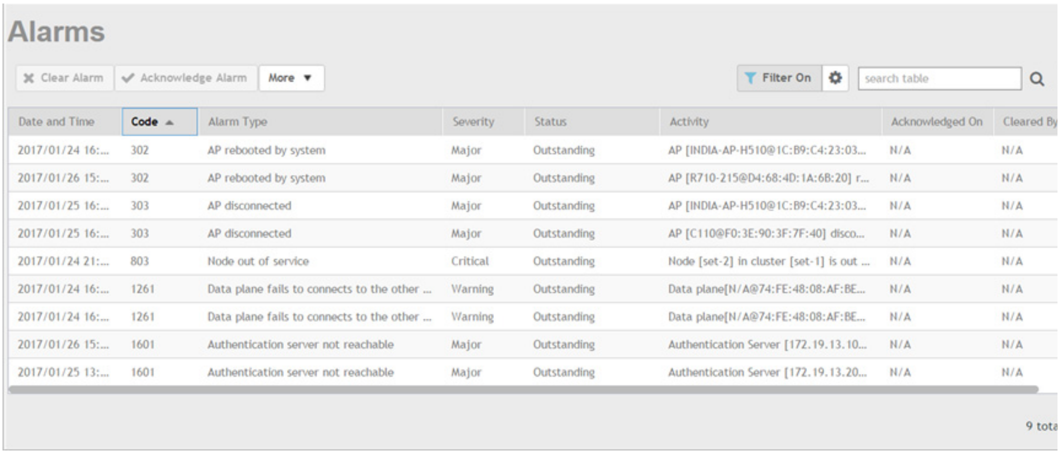
1. Alarm
   a. An alarm is a persistent indication of a fault that clears only when the triggering condition has been resolved.
   b. An alarm can be filtered in the controller web interface based on:
      - Acknowledge Time: The time when the alarm is acknowledged
      - Date and Time - Date and time 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 **Events & Alarms > 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 provides the following information as seen in Figure 1.

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

2 Event - On an event generation the:

a 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 is automatically purged.

b 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.

c The controller provides an **Events** log window as seen in Figure 2 for users to visualize and analyze the events. To view the below event information in the controller web interface navigate to **Events & Alarms > Events.**

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

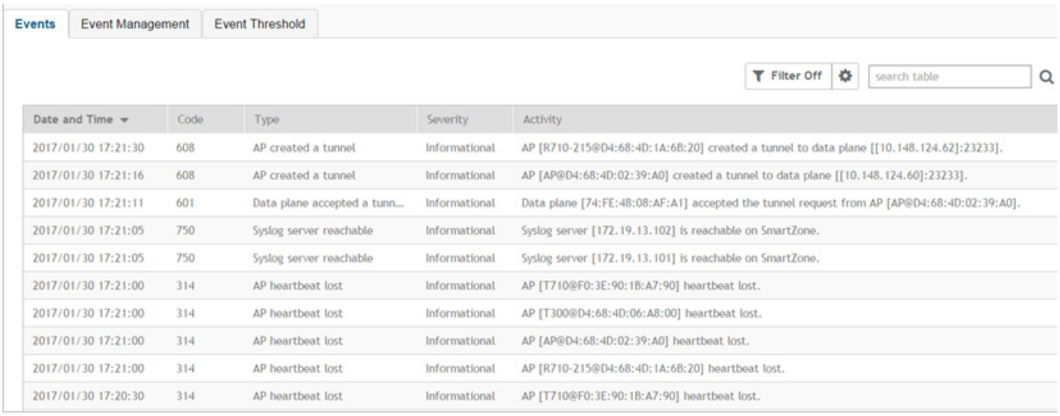
Event Management lists the disabled events that are filtered at the source whenever possible to minimize resources for processing events. The SMTP server is disabled by default. You must enable and configure the SMTP server so notification emails can be delivered successfully.

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 and Events Types for the list of alarm and event that the controller generates.

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

NOTE: Refer to the Administrator Guide for viewing Alarms and Events.

Alarm Types 3

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.

In this chapter:

- Accounting Alarms
- AP Authentication Alarms
- AP Communication Alarms
- AP LBS Alarms
- AP State Change Alarms
- Authentication Alarms
- Control and Data Plane Interface Alarms
- Cluster Alarms
- Configuration Alarms
- Data Plane Alarms
- IPMI Alarms
- Licensing Interface Alarms
- SCI Alarms
- System Alarms
- Threshold Alarms
- Tunnel Alarms - Access Point

Accounting Alarms

Following are the alarms related to accounting.

- Accounting server not reachable

Accounting server not reachable

Table 5. Accounting server not reachable alarm

Alarm	Accounting server not reachable
Alarm Type	accSrvrNotReachable
Alarm Code	1602
Severity	Major
Aggregation Policy	An alarm is raised for every event from the event code 1602. A single event triggers a single alarm.
Attribute	“mvnoId”=12, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd”, “realm”=”wlan.3gppnetwork.org" “radProxyIp”=”7.7.7.7”, “accSrvrIp"=”30.30.30.30” " {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.

NOTE: Refer to Accounting Events.

AP Authentication Alarms

Following are the alarms related to AP authentication.

- RADIUS server unreachable
- LDAP server unreachable
- AD server unreachable
- WeChat ESP authentication server unreachable
- WeChat ESP authentication server unresolvable
- WeChat ESP DNAT server unreachable
- WeChat ESP DNAT server unresolvable

RADIUS server unreachable

Table 6. RADIUS server unreachable alarm

Alarm	RADIUS server unreachable
Alarm Type	radiusServerUnreachable
Alarm Code	2102
Severity	Major
Aggregation Policy	From the event code 2102 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x"," model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2101.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach radius server [{ip}].
Description	This alarm is triggered when an AP is unable to reach the RADIUS server.
Recommended Actions	Check the network connectivity between AP and RADIUS server.

LDAP server unreachable

Table 7. LDAP server unreachable alarm

Alarm	LDAP server unreachable
Alarm Type	ldapServerUnreachable
Alarm Code	2122
Severity	Major
Aggregation Policy	From the event code 2122 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x"," model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2121.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach LDAP server [{ip}].
Description	This alarm is triggered when the AP is unable to reach LDAP server.
Recommended Actions	Check the network connectivity between AP and LDAP server.

AD server unreachable

Table 8. AD server unreachable alarm

Alarm	AD server unreachable
Alarm Type	adServerUnreachable
Alarm Code	2142
Severity	Major
Aggregation Policy	From the event code 2142 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x"," model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2141.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].

Table 8. AD server unreachable alarm

Description	This alarm is triggered when the AP is unable to reach AD server.
Recommended Actions	Check the network connectivity between AP and AD server.

WeChat ESP authentication server unreachable

Table 9. WeChat ESP authentication server unreachable alarm

Alarm	WeChat ESP authentication server unreachable
Alarm Type	espAuthServerUnreachable
Alarm Code	2152
Severity	Major
Aggregation Policy	From the event code 2152 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2151
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach WeChat ESP authentication server [{ip}]
Description	This alarm is triggered when the 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 10. 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 the AP is unable to resolve the 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 11. 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"=""

Table 11. WeChat ESP DNAT server unreachable alarm

Auto Clearance	The alarm is auto cleared with the event code 2161.
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach WeChat ESP DNAT server [{ip}].
Description	This alarm is triggered when the AP is unable to reach the 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 12. 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 the WeChat ESP DNAT server domain name.
Recommended Actions	Check the DNS server configuration settings in the controller web interface.

NOTE: Refer to AP Authentication Events.

AP Communication Alarms

Following are the alarms related to access point communications.

- AP rejected
- AP configuration update failed
- AP swap model mismatched
- AP pre-provision model mismatched
- AP firmware update failed
- AP WLAN oversubscribed

AP rejected

Table 13. AP rejected alarm

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

AP configuration update failed

Table 14. 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 to trigger another configuration change. If it fails revert to the previous zone firmware.

AP swap model mismatched

Table 15. 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 16. AP pre-provision model mismatched alarm

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

AP firmware update failed

Table 17. 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 firmware update fails.
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 18. 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.
Attribute	"apMac"=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	AP [{apName&&apMac}] does not have enough capacity to deploy all wlans. Only maximum wlan number of the AP can be deployed
Description	This alarm is triggered when the AP exceeds the maximum capacity for deploying all WLANs. Only a maximum number of WLAN APs can be deployed.
Recommended Actions	Any of the following are the recommended actions. • Create a new WLAN group with WLANs. Ensure that it is not more than the AP's WLAN capacity. Apply the new WLAN group to either the AP or the AP's AP Group. • Find the WLAN group used by the AP and reduce the number of WLAN

NOTE: Refer to AP Communication Events.

AP LBS Alarms

Following are the alarms related to AP Location Based Service.

- No LS responses
- LS authentication failure
- AP failed to connect to LS

No LS responses

Table 19. 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 when the server is in maintenance mode. Report this to the location server owner.

LS authentication failure

Table 20. LS authentication failure alarm

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

AP failed to connect to LS

Table 21. AP failed to connect to LS alarm

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

NOTE: Refer to AP LBS Events.

AP State Change Alarms

Following are the alarms related to access point state changes.

- AP rebooted by system
- AP disconnected
- AP deleted
- AP cable modem interface down
- AP DHCP service failure
- AP NAT failure

AP rebooted by system

Table 22. 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 23. 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 connectivity between the AP and controller. Try rebooting the AP locally.

AP deleted

Table 24. AP deleted alarm

Alarm	AP deleted
Alarm Type	apDeleted
Alarm Code	306
Severity	Major
Aggregation Policy	From the event code 313 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“apMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	AP [{apName&&apMac}] deleted
Description	This alarm is triggered when the AP is deleted.
Recommended Actions	No action required.

AP cable modem interface down

Table 25. 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 26. AP DHCP service failure alarm

Alarm	Both primary and secondary DHCP server APs are down
Alarm Type	apDHCPServiceFailure
Alarm Code	341
Severity	Major
Aggregation Policy	From the event code xxx an alarm is raised for every event. A single event triggers a single alarm.
Attribute	”primaryServerMac”=“xx:xx:xx:xx:xx:xx”, “secondaryServerMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	AP DHCP service failure. Both primary DHCP AP [{primaryServerMac}] and secondary DHCP server AP [{secondaryServerMac}] are down.
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 27. AP NAT failure alarm

Alarm	AP NAT failure detected by controller due to three (3) consecutive NAT gateway APs are down
Alarm Type	apNATFailureDetectedbySZ
Alarm Code	346
Severity	Critical
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.

NOTE: Refer to AP State Change Events.

Authentication Alarms

The following are the alarms related to authentication.

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

Authentication server not reachable

Table 28. Authentication server not reachable alarm

Alarm	Authentication server not reachable
Alarm Type	authSrvrNotReachable
Alarm Code	1601
Severity	Major
Aggregation Policy	From the event code 1601 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=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 alarm is triggered when primary or secondary authentication 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 controller. Ensure that the AAA server is UP.

Authentication failed over to secondary

Table 29. 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	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "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 becomes available after the primary server becomes unreachable.
Recommended Actions	No operator action is required.

Authentication fallback to primary

Table 30. Authentication fallback to primary alarm

Alarm	Authentication fallback to primary
Alarm Type	authFallbackToPrimary
Alarm Code	1652
Severity	Major
Aggregation Policy	From the event code 1652 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "SZMgmtIp"="2.2.2.2"

Table 30. Authentication fallback to primary alarm

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 authentication server failover recovery has occurred.
Recommended Actions	No action is required.

AD/LDAP connectivity failure

Table 31. 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”, “mvnoId”=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 the RADIUS server fails to connect with an AD/LDAP server.
Recommended Actions	• Check whether AD/LDAP server instance is running on the target machine • Check whether the AD/LDAP server can be reached from the controller • Verify if AD/LDAP server instances are listening on ports 3268 and 389 • Verify if the requests are reaching AD/LDAP servers by any packet capture tool (tcpdump, wireshark)

Bind fails with AD/LDAP

Table 32. Bind fails with AD/LDAP alarm

Alarm	Bind fails with AD/LDAP
Alarm Type	racADLDAPBindFail
Alarm Code	1753
Severity	Major
Aggregation Policy	From the event code 1753 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”= “1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”=”Bind to AD/LDAP fails”
Displayed on the web interface	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”= “1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”=”Bind to AD/LDAP fails”
Description	This alarm is triggered when the RADIUS server binding to the AD/LDAP server fails.
Recommended Actions	• Verify the base and administrator domain names as configured in the controller web interface • Verify the administrator user name and password as configured in the controller web interface • Verify whether the configured administrator user name and password is authenticated by the AD/LDAP servers

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

Table 33. 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”, “mvnoId”=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	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12 “srcProcess”=”RAC”, “authSrvrIp”=“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 34. RADIUS fails to connect to AD NPS server alarm

Alarm	RADIUS fails to connect to AD NPS server
Alarm Type	racADNPSFail
Alarm Code	1755
Severity	Major
Aggregation Policy	From the event code 1755 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12 “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”=“testuser’ "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 {produce.short.name} [{SZMgmtIp}
Description	This alarm is triggered RADIUS server fails to connect to AD NPS server.
Recommended Actions	• Verify if the configured NPS server instance is up and running (Network Policy Server) • Verify if the NPS server instance is communicating on the standard RADIUS port 1812 • Ensure that Windows server where AD/NPS server is provisioned can be reached from the controller web interface

RADIUS fails to authenticate with AD NPS server

Table 35. RADIUS fails to authenticate with AD NPS server alarm

Alarm	RADIUS fails to authenticate with AD NPS server
Alarm Type	racADNPSFailToAuthenticate
Alarm Code	1756
Severity	Major
Aggregation Policy	From the event code 1756 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”=“testuser’ "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	• The shared secret for NPS server should be same as that of administrator password provisioned in the controller web interface for AD server • NPS should be configured to accept request (CHAP and MSCHAPv2) from the controller • For CHAP authentication to work the AD server should store the password in reversible encryption format • Ensure that NPS is registered with AD server

Fails to establish TLS tunnel with AD/LDAP

Table 36. Fails to establish TLS tunnel with AD/LDAP alarm

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

NOTE: Refer to Authentication Events.

Control and Data Plane Interface Alarms

NOTE: This section is not applicable to vSZ-E.

Following alarm relates to control and data plane.

- GtpManager (DP) disconnected

GtpManager (DP) disconnected

Table 37. 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 Control and Data Plane Interface Events event 1201.

NOTE: Refer to Control and Data Plane Interface Events.

Cluster Alarms

Following are alarms related to cluster.

- New node failed to join
- Node removal failed
- Node out of service
- Cluster in maintenance state
- Cluster backup failed
- Cluster restore failed
- Cluster upgrade failed
- Cluster application stopped
- Node bond interface down
- Node physical interface down
- Cluster node rebooted
- Cluster node shut down
- Disk usage exceed threshold
- Cluster out of service
- Cluster upload AP firmware failed
- Cluster add AP firmware failed
- Unsync NTP time
- Cluster upload KSP file failed
- Configuration backup failed
- Configuration restore failed
- AP Certificate Expired

New node failed to join

Table 38. 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.
Recommended Actions	When the operation fails, the user can run the *join process*. 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 **Diagnostics** > **Application Logs**. Possible causes are: • The joining node is unable to complete the syncing of data in time. This could be due to the existing node performing compaction/repair etc. • The communication between the nodes may be broken. This could cause the operation to timeout such as IP address change or due to other events, which affects the network. Usually, it does not last for a long period of time.

Node removal failed

Table 39. Node removal failed alarm

Alarm	Node removal failed
Alarm Type	removeNodeFailed
Alarm Code	802
Severity	Major
Aggregation Policy	From the event code 805 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 804.
Attribute	“clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Node [{nodeName}] failed to remove from cluster [{clusterName}].
Description	This alarm is triggered when it is unable to remove a node from the cluster.
Recommended Actions	In general, this alarm should rarely occur. If it occurs, restore to the previous backup file. 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 40. Node out of service alarm

Alarm	Node out of service
Alarm Type	nodeOutOfService
Alarm Code	803
Severity	Critical
Aggregation Policy	From the event code 806 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 835.
Attribute	“clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”

Table 40. Node out of service alarm

Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service. Reason:[{reason}].
Description	This alarm is triggered when a node is out of service.
Recommended Actions	The operator/user needs to check the application/interface state.

Cluster in maintenance state

Table 41. 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	Possible causes: • The entire system backup is in process. • In a two-node cluster, the remove-node process is working. 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 > Diagnostics > Application Logs & Status.

Cluster backup failed

Table 42. Cluster backup failed alarm

Alarm	Cluster backup failed
Alarm Type	backupClusterFailed
Alarm Code	805
Severity	Major
Aggregation Policy	From the event code 810 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 809.
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason:[{reason}].
Description	This alarm is triggered when a cluster backup fails.
Recommended Actions	Check the disk usage. Try restoring the communication between nodes for a few more times. If the backup continues to fail or if you encounter Python script errors, please 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. Possible causes: • Insufficient disk space. • Communication between nodes may be broken. • Errors due to the underlying Python script.

Cluster restore failed

Table 43. Cluster restore failed alarm

Alarm	Cluster restore failed
Alarm Type	restoreClusterFailed
Alarm Code	806
Severity	Major
Aggregation Policy	From the event code 812 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 811.
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] restore failed. Reason:[{reason}].
Description	This alarm is triggered when a cluster restore fails.
Recommended Actions	Try a few more times. If the backup restore continues failing, please send the complete log files to Ruckus support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status. 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.

Cluster upgrade failed

Table 44. Cluster upgrade failed alarm

Alarm	Cluster upgrade failed
Alarm Type	upgradeClusterFailed
Alarm Code	807
Severity	Major
Aggregation Policy	From the event code 815 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 814.
Attribute	"clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”, “fromVersion”="x.x", “toVersion”="x.x"
Displayed on the web interface	Cluster [{clusterName}] could not be upgraded from [{fromVersion}] to [{toVersion}]. Reason:[{reason}].
Description	This alarm is triggered when a version upgrade of a cluster fails.
Recommended Actions	Check the disk usage. Try restoring the communication between nodes for a few 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 > Diagnostics > Application Logs & Status. Possible causes: • Insufficient disk space • Communication between nodes might be broken. • Errors due to the underlying Python script.

Cluster application stopped

Table 45. 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 46. 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 46. Node bond interface down alarm

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 47. Node physical interface down alarm

Alarm	Node physical interface down
Alarm Type	nodePhyInterfaceDown
Alarm Code	810
Severity	Critical
Aggregation Policy	From the event code 824 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 825.
Attribute	"nodeName"="xxx", "nodeMac"=" xx:xx:xx:xx:xx:xx", "ifName"="xxxx"
Displayed on the web interface	Physical network interface [{networkInterface||ifName}] on node [{nodeName}] is down.
Description	This alarm is triggered when the physical interface of a node is down.
Recommended Actions	Check if the network cables of both the physical interfaces are broken. Alternatively, check if the 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 48. 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 49. Cluster node shut down alarm

Alarm	Cluster node shut down
Alarm Type	nodeShutdown
Alarm Code	813
Severity	Major
Aggregation Policy	From the event code 828 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 826.
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] has been shut down
Description	This alarm is triggered when the node shutdowns.

Table 49. Cluster node shut down alarm

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.

Disk usage exceed threshold

Table 50. Disk usage exceed threshold alarm

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

Cluster out of service

Table 51. 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 52. 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 53. 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 54. 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 55. Cluster upload KSP file failed alarm

Alarm	Cluster upload KSP file failed

Table 55. Cluster upload KSP file failed alarm

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"="xxx"
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 56. 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 57. Configuration restore failed alarm

Alarm	Configuration restore failed

Table 57. Configuration restore failed alarm

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 Expired

Table 58. AP Certificate Expired alarm

Alarm	AP Certificate Expired
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.
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.

NOTE: Refer to Cluster Events.

Configuration Alarms

Following are the alarms related to configuration.

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

Zone configuration preparation failed

Table 59. Zone configuration preparation failed alarm

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

AP configuration generation failed

Table 60. 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 61. End-of-life AP model detected alarm

Alarm	End-of-life AP model detected
Alarm Type	cfgGenSkippedDueToEolAp
Alarm Code	1023
Severity	Major
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“nodeMac”="50:A7:33:24:E7:90","zoneName"="openZone","model"= "R300,T300"
Displayed on the web interface	Detected usage of end-of-life ap model(s)[{model}] while generating configuration for AP(s) under zone[{zoneName}]
Description	This alarm is triggered when the controller detects the AP model’s end-of-life under a certain zone.
Recommended Actions	These obsoleted APs occupy licensed AP space. Disconnect these unsupported AP models from the given zone. • Reset the APs to a factory setting using the AP command line Delete these APs through the **controller user interface > AP List**

VLAN configuration mismatch on non DHCP/NAT WLAN

Table 62. 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 63. VLAN configuration mismatch on DHCP/NAT WLAN alarm

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

NOTE: Refer to Configuration Events.

Data Plane Alarms

Following are the alarms related to data plane.

- Data plane configuration update failed
- Data plane disconnected
- Data plane physical interface down
- Data plane process restarted
- Data plane license is not enough
- Data plane upgrade failed
- Data plane of data center side fails to connect to the CALEA server
- Data Plane fails to connects to the other data plane
- Data Plane DHCP IP Pool usage rate is 100 percent

Data plane configuration update failed

Table 64. 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 due to the server being busy at that particular moment. Check to see if the event is persistent.

Data plane disconnected

Table 65. 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 66. Data plane physical interface down alarm

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

Table 66. Data plane physical interface down alarm

Recommended Actions	Check if the fiber cable between the data plane and the switch is firmly connected.

Data plane process restarted

Table 67. Data plane process restarted alarm

Alarm	Data plane process restarted
Alarm Type	dpProcessRestart
Alarm Code	520
Severity	Major
Aggregation Policy	From the event code 520 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpKey="xx:xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	[{processName}] process got re-started on data plane [{dpName&&dpKey}]
Description	This alarm is triggered when 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 to vSZ-E.

Table 68. 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>

Table 68. Data plane license is not enough alarm

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. Purchase additional licenses.

Data plane upgrade failed

NOTE: Alarm 553 is applicable only to vSZ-E.

Table 69. 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.

Table 69. Data plane upgrade failed alarm

Recommended Actions	There are several possible reasons to trigger alarm 553. The operator has to ensure the accuracy of network connectivity and version availability. For advanced process, check the debug log for reason of upgrade failure. *Note*: Debug file includes the upgrade log file. The operator can get the debug log from vSZ web interface or through vSZ-D CLI. The operator can use the following vSZ-D CLI commands to: • View the previous upgrade status and reason in case of a failure - `ruckus# show upgrade-state` / `ruckus# show upgrade-history` • Save the debug file for viewing - `ruckus(debug)# save-log` • Check the connection status between vSZ and vSZ-D - `ruckus# show status` • Check the current vSZ-D software version - `ruckus# show version` *Note*: Refer to the vSZ-D CLI Reference Guide for details on the CLI commands mentioned above.

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

Table 70. Data plane of data center side fails to connect to the CALEA server alarm

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

Table 70. Data plane of data center side fails to connect to the CALEA server alarm

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 71. 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	Warning
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	Increase the size of the DHCP IP address pool, or reduce the number of stations requiring addresses.

Data Plane DHCP IP Pool usage rate is 100 percent

Table 72. 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 data plane DHCP pool usage rate reaches 100%
Recommended Actions	

NOTE: Refer to Data Plane Events.

IPMI Alarms

NOTE: This section is not applicable to vSZ-E.

Following are the alarms related to IPMIs.

- ipmiThempBB
- ipmiThempP
- ipmiFan
- ipmiFanStatus

ipmiThempBB

Table 73. ipmiThempBB alarm

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

ipmiThempP

Table 74. ipmiThempP alarm

Alarm	ipmiThempP
Alarm Type	ipmiThempP
Alarm Code	907
Severity	Major
Aggregation Policy	From the event code 907 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 932.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when processor temperature on the control plane reaches the threshold value. The default threshold is 11^{0}C.
Recommended Actions	Check and replace the CPU fan module if required. Decrease the ambient temperature if the fan module is working.

ipmiFan

Table 75. ipmiFan alarm

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

ipmiFanStatus

Table 76. ipmiFanStatus alarm

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

NOTE: Refer to IPMI Events.

Licensing Interface Alarms

The following are the alarms related to licensing.

- License going to expire
- Insufficient license capacity

License going to expire

Table 77. 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. Purchase additional licenses.

Insufficient license capacity

Table 78. Insufficient license capacity alarm

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

NOTE: Refer to Licensing Interface Events.

SCI Alarms

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

- Connect to SCI failure
- SCI has been disabled
- SCI and FTP have been disabled

Connect to SCI failure

Table 79. 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.
Recommended Actions	Check the connectivity between SCI and the controller server. Ensure that SCI MQTT server's IP address, port number, username and password are correct.

SCI has been disabled

Table 80. 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.
Displayed on the web interface	SCI has been disabled due to SZ upgrade, please reconfigure SCI if need

Table 80. SCI has been disabled alarm

Description	This alarm occurs when SCI is disabled due to the controller upgrade.
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 81. 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.
Displayed on the web interface	SCI and FTP have been disabled. It is recommended to enable SCI instead of FTP
Description	This event occurs when the SCI and FTP are disabled.
Recommended Actions	SCI and FTP cannot be enabled simultaneously. Both features have disabled during an upgrade of the controller. Enable either SCI or FTP feature on the controller dashboard.

NOTE: Refer to SCI Events.

System Alarms

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

Following are the alarms with the system log severity.

- No LS responses
- LS authentication failure
- {produce.short.name} failed to connect to LS
- Syslog server unreachable
- Process restart
- Service unavailable
- Keepalive failure
- Resource unavailable
- HIP failed over
- The last one data plane is disconnected zone affinity profile

No LS responses

Table 82. 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 83. 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 authentication failure when SmartZone tries connecting to the location based service.
Recommended Actions	Check the location server password.

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

Table 84. {produce.short.name} failed to connect to LSalarm

Alarm	{produce.short.name} failed to connect to LS
Alarm Type	scgLBSConnectFailed
Alarm Code	724
Severity	Major
Aggregation Policy	From the event code 724 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 723.
Attribute	“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 85. Syslog server unreachable alarm

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

Process restart

Table 86. Process restart alarm

Alarm	Process restart
Alarm Type	processRestart
Alarm Code	1001
Severity	Major
Aggregation Policy	From the event code 1001 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, " {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 87. 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 88. 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 88. Keepalive failure alarm

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

Resource unavailable

Table 89. 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 *br1* interface is running.

HIP failed over

NOTE: This alarm is not applicable to vSZ-E.

Table 90. HIP failed over alarm

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

The last one data plane is disconnected zone affinity profile

Table 91. 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	Alarm is raised for every event from event code 1267. A single event triggers a single alarm.
Attribute	“dpName="xxxxxxxx",“dpKey”=“xx:xx:xx:xx:xx:xx”, "zoneAffinityProfileId"="xxxxxxxx"
Displayed on the web interface	The Last one Data Plane[{dpName&&dpKey}] is disconnected Zone Affinity profile[{zoneAffinityProfileId}] .
Description	This alarm is logged when the last data plane is disconnected from the zone affinity.
Recommended Actions	

NOTE: Refer to System Events.

Threshold Alarms

Following are the alarms related to threshold system set.

- CPU threshold exceeded
- Memory threshold exceeded
- Disk usage threshold exceeded
- License threshold exceeded
- Rate limit for TOR surpassed
- The number of users exceeded its limit
- The number of devices exceeded its limit

CPU threshold exceeded

Table 92. CPU threshold exceeded alarm

Alarm	CPU threshold exceeded
Alarm Type	cpuThresholdExceeded
Alarm Code	950
Severity	Critical
Aggregation Policy	From the event code 950 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 953.
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	CPU threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the CPU usage exceeds the threshold limit as 60% to 90%.
Recommended Actions	Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to Ruckus Wireless support. Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.

Memory threshold exceeded

Table 93. Memory threshold exceeded alarm

Alarm	Memory threshold exceeded
Alarm Type	memoryThresholdExceeded
Alarm Code	951
Severity	Critical
Aggregation Policy	From the event code 951 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 954.
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the memory usage exceeds the threshold limit. The disk threshold value for SZ-100 is 85% and 90% for vSZ-E.
Recommended Actions	Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to Ruckus Wireless support. Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.

Disk usage threshold exceeded

Table 94. Disk usage threshold exceeded alarm

Alarm	Disk usage threshold exceeded
Alarm Type	diskUsageThresholdExceeded
Alarm Code	952
Severity	Critical
Aggregation Policy	From the event code 952 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 955.
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”

Table 94. Disk usage threshold exceeded alarm

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 Wireless support.

License threshold exceeded

Table 95. License threshold exceeded alarm

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

Rate limit for TOR surpassed

Table 96. 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.
Auto Clearance	The alarm code is auto cleared with the event code 1301.
Attribute	"mvnoId"="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 97. 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.

Table 97. The number of users exceeded its limit

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 98. 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.

NOTE: Refer toThreshold Events.

Tunnel Alarms - Access Point

Following are the alarms related to tunnel.

- AP softGRE gateway not reachable
- AP is disconnected from secure gateway
- AP secure gateway association failure

AP softGRE gateway not reachable

Table 99. 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”
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 100. 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 101. 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.

NOTE: Refer toTunnel Events - Access Point (AP) and Tunnel Events - Data Plane

Events Types

4

This chapter provides information on the following types of events that the controller generates:

- Accounting Events
- AP Communication Events
- AP LBS Events
- AP Mesh Events
- AP State Change Events
- AP Authentication Events
- AP USB Events
- Authentication Events
- Authorization Events
- Control and Data Plane Interface Events
- Client Events
- Cluster Events
- Configuration Events
- Data Plane Events
- IPMI Events
- Licensing Interface Events
- SCI Events
- Session Events
- System Events
- Threshold Events
- Tunnel Events - Access Point (AP)
- Tunnel Events - Data Plane

Accounting Events

Following are the events related to accounting.

- Accounting server not reachable
- AP accounting response while invalid config
- AP account message drop while no accounting start message
- Unauthorized COA/DM message dropped

Accounting server not reachable

Table 102. Accounting server not reachable event

Event	Accounting server not reachable
Event Type	accSrvrNotReachable
Event Code	1602
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.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 103. AP accounting response while invalid config event

Event	AP accounting response while invalid config
Event Type	apAcctRespWhileInvalidConfig
Event Code	1909
Severity	Debug
Attribute	mvnoId"=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 due to incorrect controller configuration.. 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 104. 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	mvnoId"=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 105. Unauthorized COA/DM message dropped event

Event	Unauthorized COA/DM message dropped
Event Type	unauthorizedCoaDmMessageDropped
Event Code	1911
Severity	Critical
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" “userName”=”abc@xyz.com", “radSrvrIp”=”7.7.7.7”,"SZMgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] Dropped CoA/DM Packet received from AAA [{radSrvrIp}] 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.

NOTE: Refer to Accounting Alarms.

AP Communication Events

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

AP discovery succeeded	AP managed	AP rejected
AP firmware updated	AP firmware update failed	Updating AP firmware
Updating AP configuration	AP configuration updated	AP configuration update failed
AP pre-provision model mismatched	AP swap model mismatched	AP WLAN oversubscribed
AP illegal to change country code	AP configuration get failed	Rogue AP
SSID-spoofing rogue AP	Mac-spoofing rogue AP	Same-network rogue AP
Ad-hoc network device	Rogue AP disappeared	

AP discovery succeeded

Table 106. AP discovery succeeded event

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

AP managed

Table 107. 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 108. 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 109. 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 its firmware.

AP firmware update failed

Table 110. 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 firmware update fails
Auto Clearance	This event triggers the alarm 107, which is auto cleared by the event code 106.

Updating AP firmware

Table 111. 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 the AP update is in progress.

Updating AP configuration

Table 112. 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 an AP configuration update is in progress.

AP configuration updated

Table 113. AP configuration updated event

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

AP configuration update failed

Table 114. 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 configuration update fails.
Auto Clearance	This event triggers the alarm 102, which is auto cleared by the event code 110.

AP pre-provision model mismatched

Table 115. 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 116. AP swap model mismatched event

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

AP WLAN oversubscribed

Table 117. AP WLAN oversubscribed event

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

AP illegal to change country code

Table 118. AP illegal to change country code event

Event	AP illegal to change country code
Event Type	apIllgalToChangeCountryCode
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 119. AP configuration get failed event

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

Rogue AP

Table 120. Rogue AP event

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

SSID-spoofing rogue AP

Table 121. SSID-spoofing rogue AP event

Event	SSID-spoofing rogue AP
Event Type	ssid-spoofingRogueAPDetected
Event Code	181
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxxxx", "channel"="xx"

Table 121. SSID-spoofing rogue AP event

Displayed on the web interface	Ssid-spoofing rogue [{rogueMac}] with [{ssid}] is detected by [{apName&&apMac}] on channel [{channel}]
Description	This event occurs when the AP detects a rogue AP with the same service set identifier (SSID).

Mac-spoofing rogue AP

Table 122. Mac-spoofing rogue AP event

Event	Mac-spoofing rogue AP
Event Type	mac-spoofingRogueAPDetected
Event Code	182
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac"="xxx.xxx.xxx.xxx", "ssid"="xxxxxxxxxx", "channel"="xx"
Displayed on the web interface	MAC-spoofing AP [{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}]
Description	This event occurs when the AP detects a rogue AP having the same basic service set identifier (BSSID).

Same-network rogue AP

Table 123. Same-network rogue AP event

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

Ad-hoc network device

Table 124. Ad-hoc network device event

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

Rogue AP disappeared

Table 125. 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.

NOTE: Refer to AP Communication Alarms.

AP LBS Events

Following are the events related to AP Location Based Service.

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

No LS responses

Table 126. 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.
Auto Clearance	This event triggers the alarm 701, which is auto cleared by the event code 703.

LS authentication failure

Table 127. 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 when the AP fails to connect to the location service.
Auto Clearance	This event triggers the alarm 702, which is auto cleared by the event code 703.

AP connected to LS

Table 128. 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 129. 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 130. 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 location service is started on an AP.

AP stopped location service

Table 131. 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 location service on an AP is stopped.

AP received passive calibration request

Table 132. AP received passive calibration request event

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

AP received passive footfall request

Table 133. 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 134. 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.

NOTE: Refer to AP LBS Alarms.

AP Mesh Events

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

EMAP downlink connected to MAP	EMAP downlink disconnected from MAP	EMAP uplink connected to MAP
EMAP uplink disconnected from MAP	MAP disconnected	MAP downlink connected
MAP downlink connected to EMAP	MAP downlink disconnected from EMAP	RAP downlink connected to MAP
MAP uplink connected to EMAP	MAP uplink disconnected from EMAP	MAP uplink connected to RAP
MAP uplink connected to MAP	Mesh state updated to MAP	Mesh state updated to MAP no channel
Mesh state updated to RAP	Mesh state update to RAP no channel	MAP downlink connected to MAP
MAP downlink disconnected from MAP	RAP downlink disconnected from MAP	

EMAP downlink connected to MAP

Table 135. 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 136. 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 137. 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 138. 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 139. 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 140. 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

Table 140. MAP downlink connected event

Description	This event occurs when the MAP downlink connects to the AP.

MAP downlink connected to EMAP

Table 141. MAP downlink connected to EMAP event

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

MAP downlink disconnected from EMAP

Table 142. MAP downlink disconnected from EMAP event

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

RAP downlink connected to MAP

Table 143. 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 144. MAP uplink connected to EMAP event

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

MAP uplink disconnected from EMAP

Table 145. 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 146. 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 147. 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 148. Mesh state updated to MAP event

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

Mesh state updated to MAP no channel

Table 149. 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's mesh state is changed to *Mesh AP* (MAP). The message also indicates the MAP's uplink AP, number of hops, and downlink state.

Mesh state updated to RAP

Table 150. 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 's mesh state changes to Root AP (RAP). The message also indicates the radio channel and downlink state.

Mesh state update to RAP no channel

Table 151. Mesh state update to RAP no channel event

Event	Mesh state update to RAP no channel
Event Type	meshStateUpdateToRapNoChannel
Event Code	424
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "newState"="xx", "downlinkState"="xx"
Displayed on the web interface	AP [{apName&&apMac}] state set to [{newState}] with downlink [{downlinkState}]
Description	This event occurs when the AP's state changes to Root AP. The message also indicates the downlink state.

MAP downlink connected to MAP

Table 152. 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 153. 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 154. 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	AP rebooted by system	AP disconnected
AP IP address updated	AP reset to factory default	AP channel updated
AP country code updated	AP channel updated because dynamic frequency selection (DFS) detected a radar	AP change control plane
AP connected	AP deleted	AP heartbeat lost
AP tagged as critical	AP cable modem interface down	AP brownout
AP cable modem power-cycled by user	AP smart monitor turn off WLAN	AP client load balancing limit reached
AP client load balancing limit recovered	AP WLAN state changed	AP capacity reached
AP capacity recovered	AP cable modem interface up	AP cable modem soft-rebooted by user
AP cable modem set to factory default by user	AP health high latency flag	AP health low capacity flag
AP health high connection failure flag	AP health high client count flag	AP health high latency clear
AP health low capacity clear	AP health high connection failure clear	AP health high client count clear
Primary DHCP AP is down	Primary DHCP AP is up	Primary or secondary DHCP AP detects 90% of the configured total IPs
Both primary and secondary DHCP server APs are down	AP NAT gateway IP failover detected for particular VLAN pool	AP NAT gateway IP fall back detected for particular VLAN pool
NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool	AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down	AP health high airtime utilization flag

AP health high airtime utilization clear		

AP rebooted by user

Table 155. 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 been power-cycled by the user.

AP rebooted by system

Table 156. 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 157. 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 158. 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 159. AP reset to factory default event

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

AP channel updated

Table 160. 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 161. 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 162. AP channel updated because dynamic frequency selection (DFS) detected a radar event

Event	AP channel updated because dynamic frequency selection (DFS) detected a radar
Event Type	apDfsRadarEvent
Event Code	308
Severity	Informational
Attribute	“apMac"="xx:xx:xx:xx:xx:xx", “radio”="xxx", “channel”="xx"
Displayed on the web interface	AP [{apName&&apMac}] detected radar burst on radio [{radio}] and channel [{channel}] went into non-occupancy period
Description	This event occurs when the AP detects a radar burst on the channel and the channel moves to a non-occupancy mode.

AP change control plane

Table 163. 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 164. 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 165. 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 166. 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 loss is detected.

AP tagged as critical

Table 167. 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

Table 167. AP tagged as critical event

Description	This event occurs when the AP is tagged critical.

AP cable modem interface down

Table 168. 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 169. AP brownout event

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

AP cable modem power-cycled by user

Table 170. 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 171. 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 172. AP client load balancing limit reached event

Event	AP client load balancing limit reached
Event Type	apCLBlimitReached
Event Code	320
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "bssid"="xx:xx:xx:xx:xx:xx", "clb-load-limit"="", "cur-load"="", "min-clbpartner-bssid"="", "min-clbpartner-load"="", "num-clbpartners"="", "low-clbpartners"=""
Displayed on the web interface	AP [{apname@apMac}] reached client load limit, [{cur-load}] / [{clb-load-limit}], on WLAN [{ssid}]
Description	This event occurs when the AP reaches the client loading balance (CLB) limit. The adjacent threshold limit value is 50 for 2.4GHz radio and 43 for 5GHz radio.

AP client load balancing limit recovered

Table 173. 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 174. 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 adminstrator"
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 175. 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.
Description	This event occurs when an AP rejects a client because the client association threshold has been reached.

AP capacity recovered

Table 176. 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 177. 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 178. 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 rebooted because the user executes the soft-reboot CLI command.

AP cable modem set to factory default by user

Table 179. 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 defaults because the user executes the set factory CLI command.

AP health high latency flag

Table 180. 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”, ”currentValue”=“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 181. 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”, ”currentValue”=“xxxxx”,”configuredThreshold”=“xxxxx”, "radio" = "X.XG"
Displayed on the web interface	AP [{apName&&apMac}] flagged {{radio}} capacity health [{currentValue}] because it crossed the threshold [{configuredThreshold}].
Description	This event occurs when the AP is flagged because the radio has crossed the capacity health threshold configured by the administrator.

AP health high connection failure flag

Table 182. 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”, ”currentValue”=“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 183. 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”, ”currentValue”=“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 184. 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”, ”currentValue”=“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 185. 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”, ”currentValue”=“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 186. 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 187. AP health high client count clear event

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

Primary DHCP AP is down

Table 188. 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 DHCP AP detects that the primary DHCP service has failed and starts the DHCP service.

Primary DHCP AP is up

Table 189. 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 190. Secondary DHCP AP is down event

Event	Secondary DHCP AP is down detected by primary DHCP AP.
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 191. 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 primary DHCP 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 192. 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	apDHCPIPPoolMaxThresholdReached
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 193. 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 194. AP NAT gateway IP failover detected for particular VLAN pool event

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

AP NAT gateway IP fall back detected for particular VLAN pool

Table 195. AP NAT gateway IP fall back detected for particular VLAN pool event

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

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

Table 196. NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool event

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

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

Table 197. NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up event

Event	NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up
Event Type	apNATVlanCapacityRestored
Event Code	345
Severity	Informational
Attribute	”natGatewayIP”=“192.168.10.2”, "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	NAT VLAN capacity restored detected by DHCP NAT AP [{apMac}] one of the NAT gateway IP [{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 198. AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down event

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

AP health high airtime utilization flag

Table 199. AP health high airtime utilization flag event

Event	AP health high airtime utilization flag
Event Type	apHealthAirUtilizationFlag
Event Code	347
Severity	Warning
Attribute	”apName”=“xxxxx”, ”apMac”=“xx:xx:xx:xx:xx:xx”, ”currentValue”=“xxxxx”,”configuredThreshold”=“xxxxx”, "radio" = "X.XG"
Displayed on the web interface	AP [{apName&&apMac}] flagged {{radio}} airtime utilization health [{currentValue}] because it crossed the threshold [{configuredThreshold}].
Description	This event occurs when an AP is flagged because the radio has crossed the latency health threshold configured by the administrator.

AP health high airtime utilization clear

Table 200. AP health high airtime utilization clear event

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

NOTE: Refer to AP State Change Alarms.

AP Authentication Events

Following are the events related to AP authentication.

- Radius server reachable
- Radius server unreachable
- LDAP server reachable
- LDAP server unreachable
- AD server reachable
- AD server unreachable
- Wechat ESP authentication server reachable
- WeChat ESP authentication server unreachable
- WeChat ESP authentication server resolvable
- WeChat ESP authentication server unresolvable
- WeChat ESP DNAT server reachable
- WeChat ESP DNAT server unreachable
- WeChat ESP DNAT server resolvable
- WeChat ESP DNAT server unresolvable

Radius server reachable

Table 201. 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 202. 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 an 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 203. LDAP server reachable event

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

LDAP server unreachable

Table 204. 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 205. 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 the AP is able to reach the active directory server successfully.

AD server unreachable

Table 206. AD server unreachable event

Event	AD server unreachable
Event Type	adServerUnreachable
Event Code	2142
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].
Description	This event occurs when the AP is unable 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 207. 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 the AP successfully reaches the WeChat ESP authentication server.

WeChat ESP authentication server unreachable

Table 208. 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 the AP fails to reach the 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 209. WeChat ESP authentication server resolvable event

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

WeChat ESP authentication server unresolvable

Table 210. 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 the AP fails to resolves the 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 211. 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 the AP successfully reaches the WeChat ESP DNAT server.

WeChat ESP DNAT server unreachable

Table 212. WeChat ESP DNAT server unreachable event

Event	WeChat ESP DNAT server unreachable
Event Type	espDNATServerUnreachable
Event Code	2162
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach WeChat ESP DNAT server [{ip}].
Description	This event occurs when the AP fails to reach the 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 213. 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 the AP successfully resolves the WeChat ESP DNAT server domain name.

WeChat ESP DNAT server unresolvable

Table 214. 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 the AP fails to resolve the WeChat ESP DNAT server domain name.
Auto Clearance	This event triggers the alarm 2164, which is auto cleared by the event code 2163.

NOTE: Refer to AP Authentication Alarms.

AP USB Events

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

- AP USB software package downloaded
- AP USB software package download failed

AP USB software package downloaded

Table 215. 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 an AP successfully downloads a USB software package.

AP USB software package download failed

Table 216. 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 the USB software package.

Authentication Events

The following are the events related to authentication.

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

Authentication server not reachable

Table 217. Authentication server not reachable event

Event	Authentication server not reachable
Event Type	authSrvrNotReachable
Event Code	1601
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “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 primary or secondary authentication servers are not reachable.

Authentication failed over to secondary

Table 218. Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "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 becomes available after the primary server becomes unreachable.

Authentication fallback to primary

Table 219. Authentication fallback to primary event

Event	Authentication fallback to primary
Event Type	authFallbackToPrimary
Event Code	1652
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "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 event occurs when the authentication server failover recovery has occurred.

AD/LDAP connected successfully

Table 220. 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”, “mvnoId”=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 the RADIUS connection to the AD/LDAP server is successful.

AD/LDAP connectivity failure

Table 221. AD/LDAP connectivity failure event

Event	AD/LDAP connectivity failure
Event Type	racADLDAPFail
Event Code	1752
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, "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 the RADIUS fails to connect to an AD/LDAP server.

Bind fails with AD/LDAP

Table 222. Bind fails with AD/LDAP event

Event	Bind fails with AD/LDAP
Event Type	racADLDAPBindFail
Event Code	1753
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”= “1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”=”Bind to AD/LDAP fails”
Displayed on the web interface	[{srcProcess}] Bind to AD/LDAP[{authSrvrIp}] fails from SCG[{SZMgmtIp}] for User[{userName}]
Description	This event occurs when the RADIUS binding to the AD/LDAP server fails.

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

Table 223. 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”, “mvnoId”=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 the LDAP using root credentials but the controller is unable to retrieve the clear text password for the user.

RADIUS fails to connect to AD NPS server

Table 224. 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”, “mvnoId”=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 an AD NPS server.

RADIUS fails to authenticate with AD NPS server

Table 225. RADIUS fails to authenticate with AD NPS server event

Event	RADIUS fails to authenticate with AD NPS server
Event Type	racADNPSFailToAuthenticate
Event Code	1756
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=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 the RADIUS fails to authenticate with an AD NPS server.

Successfully established the TLS tunnel with AD/LDAP

Table 226. 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”, “mvnoId”=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 227. 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”, “mvnoId”=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}] Establishs the TLS connection with AD/ LDAP[{authSrvrIp}] fails from SCG[{SCGMgmtIp}]
Description	This event occurs when the TLS connection between the controller and AD/LDAP fails.
Auto Clearance	This event triggers the alarm 1762, which is auto cleared by the event code 1761.

NOTE: Refer to Authentication Alarms.

Authorization Events

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

- DM received from AAA
- DM NACK sent to AAA
- DM sent to NAS
- DM NACK received from NAS
- CoA received from AAA
- CoA NACK sent to AAA
- CoA sent NAS
- CoA NAK received NAS
- CoA authorize only access reject
- CoA RWSG MWSG notification failure

DM received from AAA

Table 228. DM received from AAA event

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

DM NACK sent to AAA

Table 229. DM NACK sent to AAA event

Event	DM NACK sent to AAA
Event Type	dmNackSntAAA
Event Code	1642
Severity	Debug
Attribute	“mvnoId”=”2” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radius” “userName”=”user name" “radSrvrIp”=”7.7.7.7” "rmtRadSrvrIp"="40.40.40.40" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected not acknowledged message to the AAA server.

DM sent to NAS

Table 230. DM sent to NAS event

Event	DM sent to NAS
Event Type	dmSntNAS
Event Code	1643
Severity	Debug
Attribute	“mvnoId”=”2” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radius” “userName”=”user name" “radSrvrIp”=”7.7.7.7” "nasIp"="40.40.40.40" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS DM sent to NAS [{rmtRadSrvrIp}] by RAC [{radSrvrIp}] for [{userName}]
Description	This event occurs when RAC sends a disconnected message to the network access server [proxy of received disconnected message or the disconnected message as initiated by the controller].

DM NACK received from NAS

Table 231. DM NACK received from NAS event

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

CoA received from AAA

Table 232. CoA received from AAA event

Event	CoA received from AAA
Event Type	coaRcvdAAA
Event Code	1645
Severity	Debug
Attribute	“mvnoId”=”2” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radius” “userName”=”user name" “radSrvrIp”=”7.7.7.7” "rmtRadSrvrIp"="40.40.40.40" "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 233. CoA NACK sent to AAA event

Event	CoA NACK sent to AAA
Event Type	coaNackSntAAA
Event Code	1646
Severity	Debug
Attribute	“mvnoId”=”2” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radius” “userName”=”user name" “radSrvrIp”=”7.7.7.7” "rmtRadSrvrIp"="40.40.40.40" "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 234. CoA sent NAS event

Event	CoA sent NAS
Event Type	coaSentNas
Event Code	1647
Severity	Debug
Attribute	“mvnoId”=”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 235. CoA NAK received NAS event

Event	CoA NAK received NAS
Event Type	coaNakRcvdNas
Event Code	1648
Severity	Debug
Attribute	“mvnoId”=”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 NAK received from NAS(AP) for forwarded/proxied CoA [{radSrvrIp}]
Description	This event occurs when a change of authorization, not acknowledged is received from the NAS server.

CoA authorize only access reject

Table 236. CoA authorize only access reject event

Event	CoA authorize only access reject
Event Type	coaAuthorizeOnlyAccessReject
Event Code	1649
Severity	Critical
Attribute	“mvnoId”=”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” "rmtRadSrvrIp"="40.40.40.40"
Displayed on the web interface	CoA Authorize Only unsuccessful for AAA Server [rmtRadSrvrIp] for UE [ueMacAddr]
Description	This event occurs when the change of authorization is rejected.

CoA RWSG MWSG notification failure

Table 237. CoA RWSG MWSG notification failure event

Event	CoA RWSG MWSG notification failure
Event Type	coaRWSGMWSGNotifFailure
Event Code	1650
Severity	Major
Attribute	mvnoId"=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
- GtpManager (DP) disconnected
- Session updated at DP
- Session update at DP failed
- Session deleted at DP
- Session delete at DP failed
- C2d configuration failed

DP connected

Table 238. DP connected event

Event	DP connected
Event Type	connectedToDblade
Event Code	1201
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”NA” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	The connectivity between Control plane [{ctrlBladeIp}] and Data plane [{dataBladeIp}] is established at {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the control plane successfully completes the configuration procedure.

GtpManager (DP) disconnected

Table 239. GtpManager (DP) disconnected event

Event	GtpManager (DP) disconnected
Event Type	lostCnxnToDblade
Event Code	1202
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”NA” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "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 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 240. Session updated at DP event

Event	Session updated at DP
Event Type	sessUpdatedAtDblade
Event Code	1205
Severity	Debug
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”realm sent by UE” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2" “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “ueImsi”=”12345” “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been updated at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the session updates the request (C-D-SESS-UPD-REQ) successfully.

Session update at DP failed

Table 241. Session update at DP failed event

Event	Session update at DP failed
Event Type	sessUpdateErrAtDblade
Event Code	1206
Severity	Debug
Attribute	“mvnoId”=”12”, “wlanId”=”1”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, “zoneId”=”10”, “realm”=”realm sent by UE”, “ctrlBladeIp”=”1.1.1.1”, "dataBladeIp"="3.3.3.3", "{produce.short.name}MgmtIp"="2.2.2.2", “ueMacAddr”=”aa:bb:cc:gg:hh:ii”, “ueImsi”=”12345”, “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to update at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{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 242. Session deleted at DP event

Event	Session deleted at DP
Event Type	sessDeletedAtDblade
Event Code	1207
Severity	Debug
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”realm sent by UE” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2" “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “ueImsi”=”12345” “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been deleted from Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SZMgmtIp}]

Table 242. Session deleted at DP event

Description	This event occurs when the session delete request (C-D-SESS-DEL-REQ) is successfully acknowledged.

Session delete at DP failed

Table 243. Session delete at DP failed event

Event	Session delete at DP failed
Event Type	sessDeleteErrAtDblade
Event Code	1208
Severity	Debug
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”realm sent by UE” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2" “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “ueImsi”=”12345” “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to delete from Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SZMgmtIp}]
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 244. C2d configuration failed event

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

NOTE: Refer to Control and Data Plane Interface Alarms.

Client Events

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

- Client authentication failed
- Client joined
- Client failed to join
- Client disconnected
- Client connection timed out
- Client authorization successfully
- Client authorization failed
- Client session expired
- Client roaming
- Client logged out
- Client roaming disconnected
- Client blocked
- Client grace period
- Onboarding registration succeeded
- Onboarding registration failed
- Remediation succeeded
- Remediation failed
- Force DHCP disconnected
- WDS device joined
- WDS device left
- Client is blocked because of barring UE rule
- Client is unblocked because of barring UE rule
- Start CALEA mirroring client
- Stop CALEA mirroring client
- Wired client joined
- Wired client failed to join
- Wired client disconnected
- Wired client authorization successfully

- Wired client session expired

Client authentication failed

Table 245. Client authentication failed event

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

Client joined

Table 246. 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 a WLAN on an AP.

Client failed to join

Table 247. 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 a WLAN on an AP.

Client disconnected

Table 248. Client disconnected event

Event	Client disconnected
Event Type	clientDisconnect
Event Code	204
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", “ssid”=”xxxxx”, “assoicationTime"="600", “wlanId”=”xxxxx”, “userName”=”xxxxx”, “clientIP”=”x.x.x.x”, “apName”=””, “apLocation”=””, “username”=””, “osType”=””, “radio”=””, “vlanId”=””, “sessionDuration”=””, “txBytes”=””, “rxBytes”=””, “rssi”=””, “receivedSignalStrength”=””, “apGps”=””, “hostname”=””, “encryption”=””, “disconnectReason”=””, “bssid”=””, “userId”=”uuid"
Displayed on the web interface	Client [{userName||IP||clientMac}] disconnected from WLAN [{ssid}] on AP [{apName&&apMac}]
Description	This event occurs when the client disconnects from a WLAN on an AP.

Client connection timed out

Table 249. Client connection timed out event

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

Client authorization successfully

Table 250. 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 is authorized successfully.

Client authorization failed

Table 251. Client authorization failed event

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

Client session expired

Table 252. 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”, “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}] 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 253. 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 has roamed from one AP to another.

Client logged out

Table 254. Client logged out event

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

Client roaming disconnected

Table 255. Client roaming disconnected event

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

Client blocked

Table 256. 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 257. 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 reconnects to a WLAN within the grace period.

Onboarding registration succeeded

Table 258. 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 259. 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 260. 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 261. 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 262. 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 is disconnected from a WLAN due to a force-DHCP trigger.

WDS device joined

Table 263. WDS device joined event

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

WDS device left

Table 264. WDS device left event

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

Client is blocked because of barring UE rule

Table 265. 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 is blocked because of barring UE rule. Client [clientMac}] of WLAN [{ssid}] from AP [{apName&&apMac}] was blocked because of barring UE rule
Description	This event occurs when a client is blocked due to blocking of user equipment rule.

Client is unblocked because of barring UE rule

Table 266. Client is unblocked because of barring UE rule event

Event	Client is unblocked because of 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 allowed by the user equipment rule.

Start CALEA mirroring client

Table 267. 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 268. 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 269. Wired client joined event

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

Wired client failed to join

Table 270. 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 271. Wired client disconnected event

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

Wired client authorization successfully

Table 272. Wired client authorization successfully event

Event	Wired client authorization successfully
Event Type	wiredClientAuthorization
Event Code	2806
Severity	Informational
Attribute	apMac”=“xx:xx:xx:xx:xx:xx”, ”clientMac”=“xx:xx:xx:xx:xx:xx”, “ethProfileId”=“xxxxx”, "ethPort"="x", "iface"="xxxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx","apName"="xxxx","vlanId"="x","userName"="xxxx"
Displayed on the web interface	Client [{userName||IP||clientMac}] of LAN [{ethPort}] from AP [{apName&&apMac}] was authorized.
Description	This event occurs when a client on WLAN AP is authorized.

Wired client session expired

Table 273. Wired client session expired event

Event	Wired client session expired
Event Type	wiredClientSessionExpiration
Event Code	2808
Severity	Informational
Attribute	apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ethProfileId"="xxxxx", "ethPort"="x", "iface"="xxxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxxx","vlanId"="x","rxBytes"="x","txFrames"="x", "txBytes"="x","disconnectTime"="x","sessionDuration"="x", "disconnectReason"="x"
Displayed on the web interface	Client [{userName||IP||clientMac}] exceeded the session time limit. Session terminated.
Description	This event occurs when a client exceeds the session time limit, which results in a session termination.

Cluster Events

Following are the events related to clusters.

Cluster created successfully	New node joined successfully	New node failed to join
Node removal completed	Node removal failed	Node out of service
Cluster in maintenance state	Cluster back in service	Cluster backup completed
Cluster backup failed	Cluster restore completed	Cluster restore failed
Cluster node upgrade completed	Entire cluster upgraded successfully	Cluster upgrade failed
Cluster application stopped	Cluster application started	Cluster backup started
Cluster upgrade started	Cluster leader changed	Node bond interface down
Node bond interface up	Node IP address changed	Node physical interface down
Node physical interface up	Cluster node rebooted	NTP time synchronized
Cluster node shutdown	Cluster upload started	Cluster upload completed
Cluster upload failed	SSH tunnel switched	Cluster remove node started
Node back in service	Disk usage exceed threshold	Cluster out of service
Initiated moving APs in node to a new cluster	Cluster upload vSZ-D firmware started	Cluster upload vSZ-D firmware completed
Cluster upload vSZ-D firmware failed	Cluster upload AP firmware started	Cluster upload AP firmware completed
Cluster upload AP firmware failed	Cluster add AP firmware started	Cluster add AP firmware completed
Cluster add AP firmware failed	Cluster name is changed	Unsync NTP time
Cluster upload KSP file started	Cluster upload KSP file completed	Cluster upload KSP file failed
Configuration backup started	Configuration backup succeeded	Configuration backup failed
Configuration restore succeeded	Configuration restore failed	AP Certificate Expired
AP Certificate Updated	Configuration restore started	Upgrade SSTable failed
Reindex Elastic Search finished	Initiated APs contact APR	Node IPv6 address added
Node IPv6 address deleted		

Cluster created successfully

Table 274. 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 275. 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 276. 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 277. 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 278. 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 279. 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 280. Cluster in maintenance state event

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

Cluster back in service

Table 281. 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 282. Cluster backup completed event

Event	Cluster backup completed
Event Type	backupClusterSuccess
Event Code	809
Severity	Informational
Attribute	“clusterName”=”xxx”

Table 282. Cluster backup completed event

Displayed on the web interface	Cluster [{clusterName}] backup completed
Description	This event occurs when a cluster backup is complete.

Cluster backup failed

Table 283. Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810
Severity	Major
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason [{reason}].
Description	This event occurs when a cluster backup fails.
Auto Clearance	This event triggers the alarm 805, which is auto cleared by the event code 809.

Cluster restore completed

Table 284. 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 285. 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 286. Cluster node upgrade completed event

Event	Cluster node upgrade completed
Event Type	upgradeClusterNodeSuccess
Event Code	813
Severity	Informational
Attribute	clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”, "fromVersion"="x.x", "toVersion"="x.x"
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] upgraded from [{fromVersion}] to [{toVersion}]
Description	This event occurs when version upgrade of a node is successful.

Entire cluster upgraded successfully

Table 287. 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 288. 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 289. 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 290. Cluster application started event

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

Cluster backup started

Table 291. 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 292. 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 293. 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 294. 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 295. 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 296. 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 297. Node physical interface down event

Event	Node physical interface down
Event Type	nodePhyInterfaceDown
Event Code	824
Severity	Critical
Attribute	“nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”, “ifName”=”xxxx”
Displayed on the web interface	Physical network interface [{networkInterface||ifName}] on node [{nodeName}] is down.
Description	This event occurs when the node’s physical interface is down.
Auto Clearance	This event triggers the alarm 810, which is auto cleared by the event code 825.

Node physical interface up

Table 298. 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 299. 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.
Auto Clearance	This event triggers the alarm 811, which is auto cleared by the event code 826.

NTP time synchronized

Table 300. NTP time synchronized event

Event	NTP time synchronized
Event Type	ntpTimeSynched
Event Code	827
Severity	Informational
Attribute	“nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Date and time settings on node [{nodeName}] synchronized with NTP server
Description	This event occurs when the date and time settings of a node are synchronized with the NTP server.

Cluster node shutdown

Table 301. Cluster node shutdown event

Event	Cluster node shutdown
Event Type	nodeShutdown
Event Code	828
Severity	Major
Attribute	“nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] has been shut down
Description	This event occurs when the node is shut down.
Auto Clearance	This event triggers the alarm 813, which is auto cleared by the event code 826.

Cluster upload started

Table 302. 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 303. 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 304. 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 305. 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.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 306. 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 removal from a cluster is started.

Node back in service

Table 307. Node back in service event

Event	Node back in service
Event Type	nodeBackToInService
Event Code	835
Severity	Informational
Attribute	"clusterName"="xx", "nodeName" =”xxx”, "nodeMac"=”xx:xx:xx:xx:xx”
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is in service
Description	This event occurs when a node status changes to 'in service'.

Disk usage exceed threshold

Table 308. 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%.
Auto Clearance	This event triggers the alarm 834, which is auto cleared by the event code 838.

Cluster out of service

Table 309. 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 310. 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 tor SZ.

Cluster upload vSZ-D firmware started

Table 311. 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 312. 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 vSZ Data Plane firmware upload for a cluster is completed successfully.

Cluster upload vSZ-D firmware failed

Table 313. 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 314. 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 315. 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 316. Cluster upload AP firmware failed event

Event	Cluster upload AP firmware failed
Event Type	clusterUploadAPFirmwareFailed
Event Code	850
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] upload AP firmware failed. Reason:[{reason}].
Description	This event occurs when the cluster upload process to the AP firmware fails.
Auto Clearance	This event triggers the alarm 850, which is auto cleared by the event code 851.

Cluster add AP firmware started

Table 317. 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 318. 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	Cluster [{clusterName}] add AP firmware completed.
Description	This event occurs when the cluster add process to the AP firmware is successful.

Cluster add AP firmware failed

Table 319. 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.
Auto Clearance	This event triggers the alarm 853, which is auto cleared by the event code 852.

Cluster name is changed

Table 320. 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	This event occurs when the cluster node name is modified. By enabling email and SNMP notification in the controller user interface (**Configuration > System > Event Management**) of the event, SNMP trap and email will be generated on successful cluster-name modification. 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.

Unsync NTP time

Table 321. 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 322. 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	Starting upload KSP file in cluster [{clusterName}]
Description	This event occurs when the KSP file uploads to a cluster.

Cluster upload KSP file completed

Table 323. 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	Cluster [{clusterName}] upload KSP file completed.
Description	This event occurs when the KSP file upload is successful to the cluster.

Cluster upload KSP file failed

Table 324. 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.

Table 324. Cluster upload KSP file failed event

Description	This event occurs when the cluster fails to upload the *ksp* file.
Auto Clearance	This event triggers the alarm 858, which is auto cleared by the event code 857.

Configuration backup started

Table 325. Configuration backup started event

Event	Configuration backup started
Event Type	clusterCfgBackupStart
Event Code	860
Severity	Informational
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration backup is started.
Description	This event occurs when cluster configuration backup starts.

Configuration backup succeeded

Table 326. 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 327. 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 328. 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 329. Configuration restore failed event

Event	Configuration restore failed
Event Type	clusterCfgRestoreFailed
Event Code	864
Severity	Major
Attribute	"clusterName"="xxx"

Table 329. Configuration restore failed event

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 330. 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 331. 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 332. Configuration restore started event

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

Upgrade SSTable failed

Table 333. 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 SS table fails.

Reindex Elastic Search finished

Table 334. Reindex Elastic Search finished event

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

Initiated APs contact APR

Table 335. 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.

Node IPv6 address added

Table 336. 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 337. Node IPv6 address deleted event

Event	Node IPv6 address deleted
Event Type	nodeIPv6Deleted
Event Code	2502
Severity	Informational
Attribute	“nodeMac”=“xxx”, “ifName”=“ xx:xx:xx:xx:xx:xx”, “ip”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Network interface [{networkInterface||ifName}] on node [{nodeName}] deleted IPv6 address [{ip}].
Description	This event occurs when the node deletes the IPv6 address.

NOTE: Refer to Cluster Alarms.

Configuration Events

Following are events related to configuration.

- Configuration updated
- Configuration update failed
- Configuration receive failed
- Incorrect flat file configuration
- Zone configuration preparation failed
- AP configuration generation failed
- End-of-life AP model detected
- VLAN configuration mismatch on non-DHCP/NAT WLAN
- VLAN configuration mismatch on a DHCP/NAT WLAN

Configuration updated

Table 338. 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 339. Configuration update failed event

Event	Configuration update failed
Event Type	cfgUpdFailed
Event Code	1008

Table 339. Configuration update failed event

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 340. 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 341. Incorrect flat file configuration event

Event	Incorrect flat file configuration
Event Type	incorrectFlatFileCfg
Event Code	1012
Severity	Major

Table 341. Incorrect flat file configuration event

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 342. 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 343. 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}].

Table 343. AP configuration generation failed event

Description	This event occurs when the controller fails to generate the AP configuration under a particular zone.

End-of-life AP model detected

Table 344. 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 345. VLAN configuration mismatch on non-DHCP/NAT WLAN event

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

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on a non-DHCP/NAT WLAN
Event Type	apCfgDhcpNatWlanVlanConfigMismatch
Event Code	1025
Severity	Critical
Attribute	“ssid”=”xxxx”, “vlanID”=”xxxx”, “configuredVlan”=”5”, “vlanId”=”11”, "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [apMac}] detected VLAN configuration mismatch on DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This event occurs when the AP detects a DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

NOTE: Refer to Configuration Alarms.

Data Plane Events

Following are the events related to data plane.

Data plane discovered	Data plane discovery failed	Data plane configuration updated
Data plane configuration update failed	Data plane heartbeat lost	Data plane IP address updated
Data plane updated to a new control plane	Data plane status update failed	Data plane statistics update failed
Data plane connected	Data plane disconnected	Data plane physical interface down
Data plane physical interface up	Data plane packet pool is under low water mark	Data plane packet pool is under critical low water mark
Data plane packet pool is above high water mark	Data plane core dead	Data plane process restarted
Data plane discovery succeeded	Data plane managed	Data plane deleted
Data plane license is not enough	Data plane upgrade started	Data plane upgrading
Data plane upgrade succeeded	Data plane upgrade failed	Data plane of data center side successfully connects to the CALEA server
Data plane of data center side fails to connect to the CALEA server	Data plane successfully connects to the other data plane	Data plane fails to connects to the other data plane
Data plane disconnects to the other data plane	Start CALEA mirroring client	Stop CALEA mirroring client
Data plane DHCP IP pool usage rate is 100 percent	Data plane DHCP IP pool usage rate is 80 percent	

Data plane discovered

Table 347. 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 348. 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 349. 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"

Table 349. Data plane configuration updated event

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 350. Data plane configuration update failed event

Event	Data plane configuration update failed
Event Type	dpConfUpdateFailed
Event Code	505
Severity	Major
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “configID”=” 123456781234567”
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to update to configuration [{configID}]
Description	This event occurs when the data plane configuration update fails.
Auto Clearance	This event triggers the alarm 501, which is auto cleared by the event code 504.

Data plane rebooted

NOTE: This event is not applicable to SZ.

Table 351. 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”, "reason"="xxxxx"
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 352. 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 353. Data plane IP address updated event

Event	Data plane IP address updated
Event Type	dpIPChanged
Event Code	508
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”,
Displayed on the web interface	Data plane [{dpName&&dpKey}] IP address changed
Description	This event occurs when the IP address of the data plane is modified.

Data plane updated to a new control plane

Table 354. 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”

Table 354. Data plane updated to a new control plane event

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 355. 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 356. 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 357. 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 358. 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 359. 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 360. Data plane physical interface up event

Event	Data plane physical interface up
Event Type	dpPhyInterfaceUp
Event Code	515
Severity	Informational
Attribute	“portID”=”xx”, “dpKey”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName&&dpKey}] is up.
Description	This event occurs when the network link of the data plane is UP.

Data plane packet pool is under low water mark

Table 361. Data plane packet pool is under low water mark event

Event	Data plane packet pool is under low water mark
Event Type	dpPktPoolLow
Event Code	516
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName&&dpKey}] is under low-water mark.
Description	This event occurs when the data core packet pool is below the water mark level.
Auto Clearance	This event triggers the alarm 516, which is auto cleared by the event code 518.

Data plane packet pool is under critical low water mark

Table 362. Data plane's packet pool is under critical low water mark event

Event	Data plane packet pool is under critical low water mark
Event Type	dpPktPoolCriticalLow
Event Code	517
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName&&dpKey}] is under critical low-water mark.
Description	This event occurs when the data core packet pool falls below the critical water mark level.

Data plane packet pool is above high water mark

Table 363. Data plane packet pool is above high water mark event

Event	Data plane packet pool is above high water mark
Event Type	dpPktPoolRecover
Event Code	518
Severity	Informational
Attribute	dpKey="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName&&dpKey}] is above high-water mark
Description	This event occurs when the data plane's packet pool is above the high-water mark.

Data plane core dead

Table 364. Data plane core dead event

Event	Data plane core dead
Event Type	dpCoreDead
Event Code	519
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName&&dpKey}] has dead data core.
Description	This event occurs when one or multiple data core packet pool is lost / dead.

Data plane process restarted

Table 365. Data plane process restarted event

Event	Data plane process restarted
Event Type	dpProcessRestart
Event Code	520
Severity	Major
Attribute	dpKey="xx:xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	[{processName}] 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 to SZ.

Data plane discovery succeeded

Table 366. Data plane discovery succeeded event

Event	Data plane discovery succeeded
Event Type	dpDiscoverySuccess
Event Code	530
Severity	Informational
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, “wsgIP”=“xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] sent a discovery request to {produce.short.name} [{wsgIP}]
Description	This event occurs when data plane sends a discovery request to the controller successfully.

NOTE: Event 532 is not applicable to SZ.

Data plane managed

Table 367. 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 the data plane is approved by the controller.

NOTE: Events 537 to 553 are not applicable to SZ.

Data plane deleted

Table 368. 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 the data plane is deleted.

Data plane license is not enough

Table 369. 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 370. 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 the data plane starts the upgrade process.

Data plane upgrading

Table 371. 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 the data plane starts to upgrade programs and configuration.

Data plane upgrade succeeded

Table 372. 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 the data plane upgrade is successful.

Data plane upgrade failed

Table 373. Data plane upgrade failed event

Event	Data plane upgrade failed
Event Type	dpUpgradeFailed
Event Code	553
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to upgrade.
Description	This event occurs when the data plane upgrade fails.
Auto Clearance	This event triggers the alarm 553, which is auto cleared by the event code 552.

Data plane of data center side successfully connects to the CALEA server

Table 374. 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

Table 375. Data plane of data center side fails to connect to the CALEA server.event

Event	Data plane of data center side fails to connect to the CALEA server.
Event Type	dpDcToCaleaConnectFail
Event Code	1258
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, “caleaServerIP”=“xxx.xxx.xxx.xxx”, "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side[{dpName&&dpKey}] fails to connects to the CALEA server[{caleaServerIP}]
Description	This event occurs when the data plane fails to connect to the CALEA server.
Auto Clearance	This event triggers the alarm 1258, which is auto cleared by the event code 1257.

Data plane successfully connects to the other data plane

Table 376. 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 connects to the other data plane

Table 377. Data plane fails to connects to the other data plane event

Event	Data plane fails to connects 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

Table 378. 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	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}] 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

Table 379. Start CALEA mirroring client event

Event	Start CALEA mirroring client
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

Table 380. Stop CALEA mirroring client event

Event	Stop CALEA mirroring client
Event Type	dpStopMirroringClient
Event Code	1264
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	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

Table 381. Data plane DHCP IP pool usage rate is 100 percent event

Event	Data plane DHCP IP pool usage rate is 100 percent
Event Type	dpDhcpIpPoolUsageRate100
Event Code	1265
Severity	Critical
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane[{dpName&&dpKey}] DHCP IP Pool usage rate is 100 percent
Description	This event occurs when the data plane DHCP pool usage rate is 100%.

Data plane DHCP IP pool usage rate is 80 percent

Table 382. Data plane DHCP IP pool usage rate is 80 percent event

Event	Data plane DHCP IP pool usage rate is 80 percent
Event Type	dpDhcpIpPoolUsageRate80
Event Code	1266
Severity	Warning
Attribute	“dpName="xxxxxxxx", “dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane[{dpName&&dpKey}] DHCP IP Pool usage rate is 80 percent
Description	This event occurs when the data plane DHCP pool usage rate is 80%.

.

NOTE: Refer to Data Plane Alarms.

IPMI Events

NOTE: This section is not applicable to vSZ-E.

Following are the events related to IPMIs.

- ipmiThempBB
- ipmiThempP
- ipmiFan
- ipmiFanStatus
- ipmiREThempBB
- ipmiREThempP
- ipmiREFan
- ipmiREFanStatus

ipmiThempBB

Table 383. 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 10^0 Celsius to 61^0 Celsius. The default threshold is 61^0C.
Auto Clearance	This event triggers the alarm 902, which is auto cleared by the event code 927.

ipmiThempP

Table 384. ipmiThempP event

Event	ipmiThempP
Event Type	ipmiThempP
Event Code	907
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the processor temperature on the control plane reaches the threshold value. The threshold value is in the range of 1^0 to 11^0 Celsius. The default threshold is 11^0C.
Auto Clearance	This event triggers the alarm 907, which is auto cleared by the event code 932.

ipmiFan

Table 385. ipmiFan event

Event	ipmiFan
Event Type	ipmiFan
Event Code	909
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}]
Description	This event occurs when the system fan module status is sent.
Auto Clearance	This event triggers the alarm 909, which is auto cleared by the event code 934.

ipmiFanStatus

Table 386. ipmiFanStatus event

Event	ipmiFanStatus
Event Type	ipmiFanStatus
Event Code	912
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the fan module status is sent.
Auto Clearance	This event triggers the alarm 912, which is auto cleared by the event code 937.

ipmiREThempBB

Table 387. ipmiREThempBB event

Event	ipmiREThempBB
Event Type	ipmiREThempBB
Event Code	927
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the baseboard temperature comes back to the normal status.

ipmiREThempP

Table 388. ipmiREThempP event

Event	ipmiREThempP
Event Type	ipmiREThempP
Event Code	932
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the processor temperature comes back to the normal status.

ipmiREFan

Table 389. ipmiREFan event

Event	ipmiREFan
Event Type	ipmiREFan
Event Code	934
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}].
Description	This event occurs when the system fan module comes back to the normal status.

ipmiREFanStatus

Table 390. ipmiREFanStatus event

Event	ipmiREFanStatus
Event Type	ipmiREFanStatus
Event Code	937
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}].
Description	This event occurs when the fan module comes back to normal status.

NOTE: Refer to IPMI Alarms.

Licensing Interface Events

Following are the events related to licensing.

- License sync succeeded
- License sync failed
- License import succeeded
- License import failed
- License data changed
- License going to expire
- Insufficient license capacity

License sync succeeded

Table 391. License sync succeeded event

Event	License sync succeeded
Event Type	licenseSyncSuccess
Event Code	1250
Severity	Informational
Attribute	"nodeName"="xxxxxxxx", "licenseServerName"="ruckuswireless.flexeraoperation.com"
Displayed on the web interface	Node [{nodeName}] sync-up license with license server [{licenseServerName}] succeeded.
Description	This event occurs when the controller successfully synchronizes the license data with the license server.

License sync failed

Table 392. License sync failed event

Event	License sync failed
Event Type	licenseSyncFail
Event Code	1251
Severity	Warning
Attribute	"nodeName"="xxxxxxxx", "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 393. License import succeeded event

Event	License import succeeded
Event Type	licenseImportSuccess
Event Code	1252
Severity	Informational
Attribute	"nodeName"="xxxxxxxx",
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 394. License import failed event

Event	License import failed
Event Type	licenseImportFail
Event Code	1253
Severity	Warning
Attribute	"nodeName"="xxxxxxxx",
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 395. License data changed event

Event	License data changed
Event Type	licenseChanged
Event Code	1254
Severity	Informational
Attribute	"nodeName"="xxxxxxxx"
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 396. 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 397. Insufficient license capacity event

Event	Insufficient license capacity
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1256
Severity	Major
Attribute	"licenseType”=“ xxx”
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing AP connections to terminate.
Description	This event occurs when connected APs are rejected due to insufficient licenses.

NOTE: Refer to Licensing Interface Alarms.

SCI Events

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

- Connect to SCI
- Disconnect to SCI
- Connect to SCI failure
- SCI has been disabled
- SCI and FTP have been disabled

Connect to SCI

Table 398. Connect to SCI event

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

Disconnect to SCI

Table 399. Disconnect to SCI event

Event	Disconnect to SCI (Smart Cell Insight)
Event Type	disconnectedFromSci
Event Code	4002
Severity	Warning
Attribute	id="SCI Server","ip"="2.2.2.2","port"="8883","userName"="admin"
Displayed on the web interface	Disconnect to SCI with system id [{id}], address [{ip}:{port}] and login user [{userName}].
Description	This event occurs when the controller disconnects from SCI.

Connect to SCI failure

Table 400. Connect to SCI failure event

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

SCI has been disabled

Table 401. SCI has been disabled event

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

SCI and FTP have been disabled

Table 402. SCI and FTP have been disabled event

Event	SCI and FTP have been disabled
Event Type	disabledSciAndFtpDueToMutuallyExclusive
Event Code	4005
Severity	Warning
Displayed on the web interface	SCI and FTP have been disabled. It is recommended to enable SCI instead of FTP
Description	This event occurs when the SCI and FTP are disabled.

NOTE: Refer to SCI Alarms.

Session Events

Following event is related to user equipment TTG session.

Delete all sessions

Table 403. Delete all sessions event

Event	Delete all sessions
Event Type	delAllSess
Event Code	1237
Severity	Minor
Attribute	“mvnoId”=”NA” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”NA" "cause"="Admin Delete" "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, RWSG or CLI.

System Events

Following are the events related to system log severity.

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

No LS responses	LS authentication failure	{produce.short.name} connected to LS
{produce.short.name} failed to connect to LS	{produce.short.name} received passive request	{produce.short.name} sent controller information report
{produce.short.name} received management request	{produce.short.name} sent AP info by venue report	{produce.short.name} sent query venues report
{produce.short.name} sent associated client report	{produce.short.name} forwarded calibration request to AP	{produce.short.name} forwarded footfall request to AP
{produce.short.name} received unrecognized request	Syslog server reachable	Syslog server unreachable
Syslog server switched	Generate AP config for plane load rebalance succeeded	Generate AP config for plane load rebalance failed
FTP transfer	FTP transfer error	File upload
Email sent successfully	Email sent failed	SMS sent successfully
SMS sent failed	Process restart	Service unavailable
Keepalive failure	Resource unavailable	Data plane of data center side successfully connects to the CALEA server
Data plane of data center side fails to connect to the CALEA server	Data plane successfully connects to the other data plane	Data plane successfully connects to the other data plane
Data plane fails to connects to the other data plane	Data plane disconnects to the other data plane	Start CALEA mirroring client in data plane
Stop CALEA mirroring client in data plane	Data plane DHCP IP pool usage rate is 100 percent	Data plane DHCP IP pool usage rate is 80 percent

All data planes in the zone affinity profile are disconnected	CALEA UE Matched	ZD AP migrating
ZD AP migrated	ZD AP rejected	ZD AP migration failed
Database error	Database error	

No LS responses

Table 404. 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 405. 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 when SmartZone tries connecting to the location based service.

{produce.short.name} connected to LS

Table 406. {produce.short.name} connected to LS event

Event	{produce.short.name} connected to LS
Event Type	scgLBSConnectSuccess
Event Code	723
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “url”=““, “port”=““, “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 407. {produce.short.name} failed to connect to LS event

Event	{produce.short.name} failed to connect to LS
Event Type	scgLBSConnectFailed
Event Code	724
Severity	Major
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “url”=““, “port”=““, “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 408. {produce.short.name} received passive request event

Event	{produce.short.name} received passive request
Event Type	scgLBSStartLocationService
Event Code	725
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx:”, “type”=““, “venue”=““, “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 409. {produce.short.name} sent controller information report event

Event	{produce.short.name} sent controller information report
Event Type	scgLBSSentControllerInfo
Event Code	727
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “api”=““, “sw”=““, “clusterName”=““,”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 410. {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 411. {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 412. {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 413. {produce.short.name} sent associated client report event

Event	{produce.short.name} sent associated client report
Event Type	scgLBSSendClientInfo
Event Code	731
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “count”=““, “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 414. {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 415. {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 416. {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 417. 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 418. 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 419. Syslog server switched event

Event	Syslog server switched
Event Type	syslogServerSwitched
Event Code	752
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, "srcAddress"="xxx.xxx.xxx.xxx”, "destAddress"="xxx.xxx.xxx.xxx”
Displayed on the web interface	Syslog server is switched from [{srcAddress}] to [{destAddress}] on {produce.short.name}.
Description	This event occurs when the syslog server is switched.

Generate AP config for plane load rebalance succeeded

Table 420. 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 421. Generate AP config for plane load rebalance failed event

Event	Generate AP config for plane load rebalance failed
Event Type	planeLoadingRebalancingFailed
Event Code	771
Severity	Informational
Attribute	
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing failed.
Description	This event occurs when the user executes the load of data plane for re-balancing and generation of a new AP configuration fails.

FTP transfer

Table 422. 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 423. 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 424. 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

Table 424. File upload event

Description	This event occurs when the backup file upload fails.

Email sent successfully

Table 425. 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 the system sends mail successfully.

Email sent failed

Table 426. 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 427. 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 SMS successfully.

SMS sent failed

Table 428. SMS sent failed event

Event	SMS sent failed
Event Type	smsSendFailed
Event Code	984
Severity	Warning
Attribute	"srcProcess"="xxxxx","receiver"= "xxxxx", "reason"="xxxxx","nodeMac"="xxxxx","nodeName"="xxxxx","tenantUUID"="xxxxx"
Displayed on the web interface	[{srcProcess}] sent short message to [{receiver}] failed, reason: [{reason}].
Description	This event occurs when system fails to send the SMS.

Process restart

Table 429. 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 430. 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 431. 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"
Displayed on the web interface	[{srcProcess}] on {produce.short.name} [{SZMgmtIp}] restarted [{processName}] process
Description	This event occurs when the *mon/nc* restarts the process due to a keep alive failure.

Resource unavailable

Table 432. 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.

NOTE: Events 1257 to 1267 are not applicable for SCG.

Data plane of data center side successfully connects to the CALEA server

Table 433. 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 data plane successfully connects to the CALEA server.

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

Table 434. Data plane of data center side fails to connect to the CALEA server event

Event	Data plane of data center side fails to connect to the CALEA server.
Event Type	dpDcToCaleaConnectFail
Event Code	1258
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, “caleaServerIP”=“xxx.xxx.xxx.xxx”, "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side[{dpName&&dpKey}] fails to connects to the CALEA server[{caleaServerIP}]
Description	This event occurs when the data plane fails to connect to the CALEA server.

Table 434. Data plane of data center side fails to connect to the CALEA server event

Auto Clearance	This event triggers the alarm 1258, which is auto cleared by the event code 1257.

Data Plane of data center side disconnects to CALEA server

Table 435. Data Plane of data center side disconnects to CALEA server event

Event	Data Plane of data center side disconnects to CALEA server.
Event Type	dpDcToCaleaDisconnected
Event Code	1259
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side[{dpName&&dpKey}] fails to connects to the CALEA server[{caleaServerIP}]
Description	This event occurs when the data plane disconnects from the CALEA server.

Data plane successfully connects to the other data plane

Table 436. 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 connect to another data plane.

Data plane fails to connects to the other data plane

Table 437. Data plane fails to connects to the other data plane event

Event	Data plane fails to connects 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

Table 438. 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

Table 439. 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

Table 440. 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

Table 441. Data plane DHCP IP pool usage rate is 100 percent event

Event	Data plane DHCP IP pool usage rate is 100 percent
Event Type	dpDhcpIpPoolUsageRate100
Event Code	1265
Severity	Critical
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane[{dpName&&dpKey}] DHCP IP Pool usage rate is 100 percent
Description	This event occurs when the data plane DHCP pool usage rate is 100%.

Data plane DHCP IP pool usage rate is 80 percent

Table 442. Data plane DHCP IP pool usage rate is 80 percent event

Event	Data plane DHCP IP pool usage rate is 80 percent
Event Type	dpDhcpIpPoolUsageRate80
Event Code	1266
Severity	Warning
Attribute	“dpName="xxxxxxxx", “dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane[{dpName&&dpKey}] DHCP IP Pool usage rate is 80 percent
Description	This event occurs when the data plane DHCP pool usage rate is 80%.

All data planes in the zone affinity profile are disconnected

Table 443. 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="xxxxxxxx",“dpKey”=“xx:xx:xx:xx:xx:xx”, "zoneAffinityProfileId"="xxxxxxxx"
Displayed on the web interface	The Last one Data Plane[{dpName&&dpKey}] is disconnected Zone Affinity profile[{zoneAffinityProfileId}] .
Description	This event occurs when all the data planes disconnect from the zone affinity profile.

CALEA UE Matched

Table 444. 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 data plane CALEA user equipment and client matches.

ZD AP migrating

Table 445. 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 being upgraded to a SmartZone firmware image.

ZD AP migrated

Table 446. 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 successfully completed upgrading its firmware to SmartZone controller firmware.

ZD AP rejected

Table 447. 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 has not been upgraded with the SmartZone controller AP firmware because of an ACL setting.

ZD AP migration failed

Table 448. 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 the ZoneDirector AP fails to upgrade to the SmartZone AP firmware image.

Database error

Table 449. 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 450. Database error event

Event	Database error
Event Type	recoverCassandraError
Event Code	3011
Severity	Informational
Attribute	“nodeName”=“xxx”,”reason”=“recovery reason”
Displayed on the web interface	Recover database error on node [{nodeName}], reason : [].
Description	This event occurs when the internal errors on the database are fixed.

NOTE: Refer to System Alarms.

Threshold Events

Following are the events related to threshold limits.

- CPU threshold exceeded
- Memory threshold exceeded
- Disk usage threshold exceeded
- CPU threshold back to normal
- Memory threshold back to normal
- Disk threshold back to normal
- License threshold exceeded
- Rate limit threshold surpassed
- Rate limit threshold restored
- Rate limit for TOR surpassed
- The number of users exceed its limit
- The number of devices exceeded its limit

CPU threshold exceeded

Table 451. 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 as 60% to 90%.
Auto Clearance	This event triggers the alarm 950, which is auto cleared by the event code 953.

Memory threshold exceeded

Table 452. 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. The disk threshold value for SZ-100 is 85% and 90% for vSZ-E.
Auto Clearance	This event triggers the alarm 951, which is auto cleared by the event code 954.

Disk usage threshold exceeded

Table 453. 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 454. 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 455. 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 456. 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].

Table 456. Disk threshold back to normal event

Description	This event occurs when the disk usage comes back to normal.

License threshold exceeded

Table 457. License threshold exceeded event

Event	License threshold exceeded
Event Type	licenseThresholdExceeded
Event Code	960
Severity	Critical 90%; Major 80%; Informational 70%;
Attribute	"perc"="xxx", "nodeName"="", "nodeMac"="xx:xx:xx:xx:xx:xx", licenseType="SG00"
Displayed on the web interface	[{licenseType}] limit reached at [{perc}%]
Description	This event occurs when the number of user equipment attached to the system have exceeded the license limit.

Rate limit threshold surpassed

Table 458. Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major
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 [{aaaSrvrIp}] 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 459. 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" “aaaSrvrIp”=”1.1.1.1” “AAAServerType”=”Auth/Acct” “MOR”=1000 “THRESHOLD”=”500” “TOR”=”501”
Displayed on the web interface	Threshold restored for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is restored. The threshold limit for this event is dependent 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 460. 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" “aaaSrvrIp”=”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 [{aaaSrvrIp}] 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 461. 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 SZ-100 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 462. 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 SZ-100 is 342000 and 152000 for vSZ-E.

NOTE: Refer to Threshold Alarms.

Tunnel Events - Access Point (AP)

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

- Data plane accepted a tunnel request
- Data plane rejected a tunnel request
- Data plane terminated a tunnel
- AP created a tunnel
- AP tunnel disconnected
- AP SoftGRE tunnel fails over primary to secondary
- AP SoftGRE tunnel fails over secondary to primary
- AP SoftGRE gateway reachable
- AP SoftGRE gateway not reachable
- Data plane set up a tunnel
- AP secure gateway association success
- AP is disconnected from secure gateway
- AP secure gateway association failure

Data plane accepted a tunnel request

Table 463. Data plane accepted a tunnel request event

Event	Data plane accepted a tunnel request
Event Type	dpAcceptTunnelRequest
Event Code	601
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “apMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] accepted a tunnel request from AP [{apName&&apMac}].
Description	This event occurs when the data plane accepts a tunnel request from the AP.

Data plane rejected a tunnel request

Table 464. Data plane rejected a tunnel request event

Event	Data plane rejected a tunnel request
Event Type	dpRejectTunnelRequest
Event Code	602
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “apMac”=”xx:xx:xx:xx:xx:xx”, “reason”=”xxxxxxxxxxxxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] rejected a tunnel request from AP [{apName&&apMac}] because of reason [{reason}].
Description	This event occurs when the data plane rejects a tunnel request from the AP.

Data plane terminated a tunnel

Table 465. Data plane terminated a tunnel event

Event	Data plane terminated a tunnel
Event Type	dpTearDownTunnel
Event Code	603
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “apMac”=”xx:xx:xx:xx:xx:xx”, “reason”=”xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] terminated a tunnel from AP [{apName&&apMac}]. Reason: [{reason}]
Description	This event occurs when the data plane terminates a tunnel from the AP.

AP created a tunnel

Table 466. AP created a tunnel event

Event	AP created a tunnel
Event Type	apBuildTunnelSuccess
Event Code	608
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "dpIP"="xxx.xxx.xxx.xxx",
Displayed on the web interface	AP [{apName&&apMac}] created a tunnel to data plane [{dpIP}].
Description	This event occurs when AP creates a tunnel to the data plane.

AP tunnel disconnected

Table 467. 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 468. 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 an AP moves from a primary to a secondary GRE.

AP SoftGRE tunnel fails over secondary to primary

Table 469. AP SoftGRE tunnel fails over secondary to primary event

Event	AP SoftGRE tunnel fails over secondary to primary
Event Type	apSoftGRETunnelFailoverStoP
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 an AP moves from a secondary to a primary GRE.

AP SoftGRE gateway reachable

Table 470. 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 an AP builds a soft GRE tunnel successfully.

AP SoftGRE gateway not reachable

Table 471. 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 an 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 to vSZ-E.

Table 472. 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 473. 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 474. 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 the secure gateway.

AP secure gateway association failure

Table 475. AP secure gateway association failure event

Event	AP secure gateway association failure
Event Type	ipsecTunnelAssociateFailed
Event Code	662
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is unable to establish secure gateway with [{ipsecGWAddress}].
Description	This event occurs when the AP is unable to reach the secure gateway.
Auto Clearance	This event triggers the alarm 662, which is auto cleared by the event code 660.

NOTE: Refer to Tunnel Alarms - Access Point.

Tunnel Events - Data Plane

NOTE: Events 618, 619 and 623 are applicable to SZ-100.

Following are the events related to tunnel events on the data plane.

- DP Core GW unreachable
- DPs GRE keep alive timeout
- DP Core GW inactive
- DP DHCPRelay no response
- DP DHCPRelay failover
- DP sGRE new tunnel
- DP sGRE keepalive recovery
- DP DHCPRelay response recovery
- DP Core GW reachable
- DP Core GW active

DP Core GW unreachable

Table 476. DP Core GW unreachable event

Event	DP Core GW unreachable
Event Type	dpSgreGWUnreachable
Event Code	615
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected Core Gateway [{GatewayIP}] is unreachable.
Description	This event occurs when the data plane detects that a core network gateway is unreachable.

DPs GRE keep alive timeout

Table 477. DPs GRE keep alive timeout event

Event	DPs GRE 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 Core GW inactive

Table 478. DP Core GW inactive event

Event	DP Core 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 479. 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 a response from the DHCP server.

DP DHCPRelay failover

Table 480. DP DHCPRelay failover event

Event	DP DHCPRelay failover
Event Type	dpDhcpRelayFailOver
Event Code	619
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "preDhcpIP"="x.x.x.x", "curDhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected DHCP server fail-over from [preDhcpIP}] to [{curDhcpIP}]
Description	This event occurs when the data plane detects a DHCP server relay failure.

DP sGRE new tunnel

Table 481. DP sGRE new tunnel event

Event	DP sGRE new tunnel
Event Type	dpSgreNewTunnel
Event Code	620
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "greType"="L2oGRE, L3oGRE", "apIpAddress"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] established a [{greType}] tunnel with AP[{apIP}].
Description	This event occurs when the data plane establishes a tunnel with an AP.

DP sGRE keepalive recovery

Table 482. 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 483. 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 Core GW reachable

Table 484. DP Core GW reachable event

Event	DP Core 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 Core GW active

Table 485. DP Core GW active event

Event	DP Core 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 the core gateway changes to active mode.

NOTE: Refer to Tunnel Alarms - Access Point.

Index

A

accounting alarms 50
accounting server not reachable 50, 128
accSrvrNotReachable 50, 128
ad server unreachable 52
ad/LDAP connected successfully 194
ad/ldap connectivity failure 70
ad-hoc network device 142
ad-hoc-networkRogueAPDetecte 142
adServerUnreachable 52
alarm 44, 45
alarm and event management 44
AP 173
ap account message drop while no accounting start message 130
ap accounting response while invalid config 129
AP Brownout 165
ap cable modem interface down 66, 165
ap cable modem power-cycled by user 166
ap cable modem set to factory default by user 170
ap cable modem soft-rebooted by user 170
ap capacity reached 168
ap capacity recovered 169
ap certificate expired 92, 254
ap certificate updated 254
ap change control plane 163
ap channel updated 161
ap channel updated dfs detected a radar 162
ap client load balancing limit reached 167
ap client load balancing limit recovered 167
ap communication alarms 56
ap communication events 132, 191
ap configuration generation failed 94, 260
AP configuration get failed 139
ap configuration update failed 57, 136
ap configuration updated 136
ap connected 163
ap connected to ls 144
ap country code updated 162
ap created a tunnel 330
ap deleted 65, 164
AP disconnected 160
ap disconnected 65
ap discovery succeeded 132
aP failed to connect to LS 63
ap failed to connect to ls 145
ap firmware update failed 59, 134
ap firmware updated 134
AP health high airtime utilization clear 182
AP health high airtime utilization flag 181
AP health high client count clear 174
AP health high client count flag 172
AP health high connection failure clear 174
AP health high connection failure flag 172
AP health high latency clear 173
AP health high latency flag 171
AP health low capacity clear 173
AP health low capacity flag 171
ap heartbeat lost 164
ap illegal to change country code 138
ap ip address updated 160
ap is disconnected from secure gateway 125, 334
ap managed 133
ap mesh events 148
AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down 181
AP NAT gateway IP failover detected for particular VLAN pool 178
AP NAT gateway IP fall back detected for particular VLAN pool 178
ap pre-provision model mismatched 58, 137
ap rebooted by system 64, 159
ap rebooted by user 159
ap received passive calibration request 146
ap received passive footfall request 147
AP received unrecognized request 147
ap rejected 56, 133
ap reset to factory default settings 161

ap secure gateway association failure 334
ap secure gateway association success 333
ap smart monitor turn off wlan 166
ap softgre gateway not reachable 124, 332
ap softgre gateway reachable 332
ap softgre tunnel fails over primary to secondary 331
ap softgre tunnel fails over secondary to primary 331
ap started location service 145
ap state change alarms 64
ap state change events 158
ap stopped location service 146
ap swap model mismatched 57, 137
ap tagged as critical 164
ap tunnel disconnected 330
ap USB software package download failed 191
ap USB software package downloaded 191
ap WLAN oversubscribed 60
ap wlan oversubscribed 138
ap wlan state changed 168
apAcctMsgDropNoAcctStartMsg 130
apAcctRespWhileInvalidConfig 129
apBrownout 165
apBuildTunnelSuccess 330
apCapacityReached 168
apCapacityRecovered 169
apCertificateExpire 92, 254
apCertificateExpireClear 254
apCfgDhcpNatWlanVlanConfigMismatch 26, 27, 97, 263
apCfgGenFailed 94, 260
apCfgNonDhcpNatWlanVlanConfigMismatch 26, 27, 96, 262
apChangeControlBlade 163
apChannelChanged 161
apCLBlimitReached 167
apCLBlimitRecovered 167
apConfApplying 135
apConfUpdated 136
apConfUpdateFailed 57, 136
apConnected 163
apConnectionTerminatedDueToInsufficientLicense 291
apCountryCodeChanged 162
apDeleted 164
apDfsRadarEvent 162
apDHCPFailoverDetected 26, 175
apDHCPFallbackDetected 26, 175
apDHCPIPPoolMaxThresholdReached 27, 177
apDHCPServiceFailure 25, 27, 66, 177
apDiscoverySuccess 132
apFirmwareApplying 135
apFirmwareUpdated 134
apFirmwareUpdateFailed 59, 134
apGetConfigFailed 26, 139
apHealthAirUtilizationClear 27, 182
apHealthAirUtilizationFlag 27, 181
apHealthCapacityClear 26, 173
apHealthCapacityFlag 26, 171
apHealthClientCountClear 26, 174
apHealthClientCountFlag 26, 172
apHealthConnectionFailureClear 26, 174
apHealthConnectionFailureFlag 26, 172
apHealthLatencyClear 26, 173
apHealthLatencyFlag 26, 171
apHeartbeatLost 164
apIPChanged 160
apLBSAuthFailed 62, 144
apLBSConnectFailed 63, 145
apLBSConnectSuccess 144
apLBSNoResponses 61, 143
apLBSRcvdPassiveCalReq 146
apLBSRcvdPassiveFFReq 147
apLBSRcvdUnrecognizedRequest 147
apLBSStartLocationService 145
apLBSStopLocationService 146
apModelDiffWithPreProvConfig 58, 80, 137, 230
apModelDiffWithSwapOutAP 57, 137
apNATFailoverDetected 27, 178
apNATFailureDetectedbySZ 25, 27, 67, 181
apNATFallbackDetected 27, 178
apNATVlanCapacityAffected 27, 179
apNATVlanCapacityRestored 27
apP cable modem interface up 169
apRebootBySystem 64, 159
apSecondaryDHCPAPDown 26, 176
apSecondaryDHCPAPUp 27, 176
apSoftGREGatewayNotReachable 124, 332
apSoftGREGatewayReachable 332
apSoftGRETunnelFailoverPtoS 331
apSoftGRETunnelFailoverStoP 331

apStatusManaged 133
apStatusRejected 56, 133
apTaggedAsCritical 164
apTunnelDisconnected 330
apUsbSoftwarePackageDownloaded 191
apUsbSoftwarePackageDownloadFailed 191
apWlanOversubscribed 60, 138
apWLANStateChanged 168
authentication alarms 68
authentication events 192
authentication failed over to secondary 69, 193
authentication fallback to primary 69, 193
authentication server not reachable 68, 192
authFailedOverToSecondary 69, 193
authFallbackToPrimary 69, 193
authorization events 199
authSrvrNotReachable 68, 192
auto cleared 51, 52, 53, 54, 55, 56, 57, 59, 63, 65, 66, 76, 78, 79, 80, 81, 82, 83, 84, 85, 86, 88, 89, 90, 91, 92, 98, 99, 105, 106, 107, 113, 114, 119, 120, 122, 124, 126, 133, 134, 136, 143, 144, 145, 160, 165, 184, 185, 186, 187, 188, 189, 190, 198, 206, 228, 229, 230, 231, 232, 233, 234, 236, 238, 239, 240, 244, 248, 249, 252, 253, 254, 267, 270, 271, 272, 278, 279, 280, 283, 284, 285, 293, 298, 304, 312, 313, 321, 322, 326, 332, 334
aystem alarms 112

B

backupClusterFailed 81, 231
backupClusterSuccess 230
bind fails with AD/LDAP 71
bind success with LDAP 72, 195
Both primary and secondary DHCP server APs are down 66, 177

C

c2d configuration failed 209
c2dCfgFailed 209
cableModemDown 165
cableModemUp 169
CALEA UE Matched 316
caleaMirroringStart 222
caleaMirroringStop 222
cassandraError 319
cfgGenSkippedDueToEolAp 262
cfgRcvFailed 259
cfgUpdFailed 258
cfgUpdSuccess 258
client authentication failed 211
client authorization failed 214
client authorization successfully 213
client blocked 216
client connection timed out 213
client disconnected 212
client events 210
client failed to join 212
client grace period 217
client is blocked because of barring UE rule 221
client is unblocked because of barring UE rule 221
client joined 211
client logged out 215
client roaming 215
client roaming disconnected 216
client session expired 214
clientAuthFailure 211
clientAuthorization 213
clientAuthorizationFailure 214
clientBlockByBarringUERule 26, 221
clientBlockByDeviceType 216
clientDisconnect 212
clientGracePeriod 217
clientInactivityTimeout 213
clientJoin 211
clientJoinFailure 212
clientRoaming 215
clientSessionExpiration 214
clientSessionLogout 215
clientUnblockByBarringUERule 26, 221
cluster add AP firmware completed 249
Cluster add AP firmware failed 89
cluster add AP firmware failed 249
cluster add AP firmware started 248
cluster application started 234
cluster application stopped 84, 234
cluster back in service 230
cluster backup completed 230
cluster backup failed 81, 231
cluster backup started 235

cluster created successfully 227
cluster events 226
cluster in maintenance state 80, 230
cluster leader changed 236
cluster name is changed 250
cluster node rebooted 86, 239
cluster node shut down 86
cluster node shutdown 240
cluster node upgrade completed 232
cluster out of service 88, 244
cluster remove node started 243
cluster restore completed 231
cluster restore failed 82, 232
Cluster upgrade failed 83
cluster upgrade failed 233
cluster upgrade started 235
cluster upload AP firmware completed 247
cluster upload AP firmware failed 88, 248
cluster upload AP firmware started 247
cluster upload completed 241
cluster upload failed 242
cluster upload KSP file completed 251
Cluster upload KSP file failed 89
cluster upload KSP file failed 251
cluster upload KSP file started 251
cluster upload started 241
cluster upload vSZ-D firmware failed 246
clusterAddAPFirmwareFailed 89, 249
clusterAddAPFirmwareStart 248
clusterAddAPFirmwareSuccess 249
clusterAppStart 234
clusterAppStop 84, 234
clusterBackToInService 230
clusterBackupStart 235
clusterCfgBackupFailed 90, 253
clusterCfgBackupStart 252
clusterCfgBackupSuccess 252
clusterCfgRestoreFailed 91, 253
clusterCfgRestoreStarted 255
clusterCfgRestoreSuccess 253
clusterCreatedSuccess 227
clusterInitContactApr 27, 256
clusterLeaderChanged 236
clusterNameChanged 250
clusterOutOfService 88, 244
clusterUpgradeStart 235
clusterUploadAPFirmwareFailed 88, 248
clusterUploadAPFirmwareStart 247
clusterUploadAPFirmwareSuccess 247
clusterUploadKspFileFailed 25, 90, 251
clusterUploadKspFileStart 251
clusterUploadKspFileSuccess 251
cmRebootByUser 166
cmResetByUser 170
cmResetFactoryByUser 170
coA authorize only access reject 203
coA nack sent to AAA 202
coA NAK received NAS 203
coA received from AAA 201
coA RWSG MWSG notification failure 204
coA sent NAS 202
coaAuthorizeOnlyAccessReject 203
coaNackSntAAA 202
coaNakRcvdNas 203
coaRcvdAAA 201
coaRWSGMWSGNotifFailure 204
coaSentNas 202
configuration 93
Configuration backup failed 90
configuration backup failed 253
configuration backup started 252
configuration backup succeeded 252
configuration events 258
configuration receive failed 259
configuration restore failed 90, 253
configuration restore started 255
configuration restore succeeded 253
configuration update failed 258
configuration update success 258
configuration-change events 44
connect to SCI 292
Connect to SCI failure 110
connect to SCI failure 293
connectedToDblade 205
connectedToSci 28, 292
connectToSciFailure 110, 293
control and data plane 76, 205
cpu threshold back to normal 323
cpu threshold exceeded 119, 321
cpuThresholdBackToNormal 323
cpuThresholdExceeded 119, 321
csvDiskMaxCapacityReached 26, 27
csvDiskThreshholdExceeded 25, 27
csvFtpTransferMaxRetryReached 25, 27

D

data plane 98, 264
data plane accepted a tunnel request 328

data plane configuration update failed 98, 267
data plane configuration updated 265
data plane connected 270
data plane core dead 273
data plane deleted 275
data plane disconnected 99, 270
data plane discovered 265
data plane discovery failed 265
data plane discovery succeeded 274
Data Plane fails to connects to the other Data Plane 103
data plane heartbeat lost 268
data plane ip address updated 268
data plane license is not enough 100, 276
data plane managed 275
data plane of data center side disconnects to CALEA server. 312
data plane of data center side fails to connect to the CALEA server 102
Data plane of data center side fails to connect to the CALEA server. 279
data plane packet pool is above high water mark 273
data plane packet pool is under critical low water mark 272
data plane packet pool is under low water mark 272
data plane physical interface down 99, 271
data plane physical interface up 271
data plane process restarted 100, 274
data plane rebooted 267
data plane rejected a tunnel request 329
data plane set up a tunnel 333
data plane statistics update failed 269
data plane status update failed 269
data plane terminated a tunnel 329
data plane updated to a new control plane 268
data plane upgrade failed 101, 278
data plane upgrade started 276
data plane upgrade succeeded 277
data plane upgrading 277
database error 319
datablade alarms 98
debug 45
delAllSess 295
delete all sessions 295
disabledSciAndFtpDueToMutuallyExclusive 26, 28, 294
disabledSciDueToUpgrade 26, 28, 293
disconnect to SCI 292
disconnectedFromSc 292
disconnectedFromSci 28
disk threshold back to normal 323
disk usage exceed threshold 87, 244
disk usage threshold exceeded 120, 322
diskUsageExceed 87, 244
diskUsageThresholdExceeded 120, 322
dm nack received from NAS 201
dm nack sent to AAA 200
dm received from AAA 199
dm sent to NAS 200
dmNackRcvdNAS 201
dmNackSntAAA 200
dmRcvdAAA 199
dmSntNAS 200
dp connected 205
dp DHCPRelay failover 337
dp DHCPRelay no response 337
dp dhcprelay response recovery 339
dp sGRE keep alive timeout 336
dp sGRE new tunnel 338
dpAcceptTunnelRequest 328
dpCaleaUeInterimMatched 27, 316
dpCoreDead 273
dpDcToCaleaConnected 27
dpDcToCaleaConnectFail 26, 27, 102, 279
dpDcToCaleaDisconnected 27, 312
dpDeleted 275
dpDhcpIpPoolUsageRate100 26, 28
dpDhcpIpPoolUsageRate80 28
dpDhcpRelayFailOver 337
dpDhcpRelayNoResp 337
dpDhcpRelayRespRecovery 339
dpDisconnected 99
dpDiscoverySuccess 274
dpLicenseInsufficient 100, 101, 276
dpP sGRE keepalive recovery 338
dpP2PTunnelConnected 27
dpP2PTunnelConnectFail 26, 27
dpP2PTunnelDisconnected 27
dpPhyInterfaceDown 99
dpPktPoolCriticalLow 272
dpPktPoolLow 272
dpPktPoolRecover 273
dpProcessRestart 100, 274

dpRejectTunnelRequest 329
dpSetUpTunnel 333
dpSgreGWAct 340
dpSgreGWInact 336
dpSgreGWReachable 339
dpSgreKeepAliveRecovery 338
dpSgreKeepAliveTimeout 336
dpSgreNewTunnel 338
dpStartMirroringClient 28, 314
dpStatusManaged 275
dpStopMirroringClient 28, 314
dpTearDownTunnel 329
dpUpdateStatisticFailed 269
dpUpgradeFailed 278
dpUpgradeStart 276
dpUpgradeSuccess 277
dpUpgrading 277

E

email sent failed 307
email sent successfully 307
emapDlinkConnectWithMap 148
emapDlinkDisconnectWithMap 149
emapUlinkConnectWithMap 149
emapUlinkDisconnectWithMap 150
end -of-life AP model detected 95, 262
entire cluster upgraded successfully 233
espAuthServerReachable 186
espAuthServerResolvable 187
espAuthServerUnreachable 53, 187
espAuthServerUnResolvable 54, 188
espDNATServerReachable 188
espDNATServerResolvable 189
espDNATServerUnreachable 54, 189
espDNATServerUnresolvable 190
event 45
event attributes 45
event categories 44
event detail information 45
event severity 45
event source 45
event type 45

F

failed to connect to LS 113
fails to establish TLS tunnel with AD/LDAP 75, 198
file upload 306
fileUpload 306
force DHCP disconnected 219
forceDHCPDisconnect 219
ftp transfer 306
ftp transfer error 306
ftpTransfer 306
ftpTransferError 306

G

generate AP config for plane load rebalance failed 305
generate AP config for plane load rebalance succeeded 305
generation of event and alarm 45
gtpManager (DP) disconnected 76, 206

H

hIP failed over 117
hipFailover 117

I

incorrect flat file configuration 259
informational 45
Initiated APs contact APR 256
insufficient license capacity 291
ipmi alarms 105
ipmi events 283
ipmiFan 106, 284
ipmiFanStatus 107, 285
ipmiREFan 286
ipmiREFanStatus 287
ipmiREThempBB 285
ipmiREThempP 286
ipmiThempBB 105, 283
ipmiThempP 106, 284
ipsecTunnelAssociated 333
ipsecTunnelAssociateFailed 334
ipsecTunnelDisassociated 125, 334

K

keepalive failure 115, 310
keepAliveFailure 115, 310

L

ldap server unreachable 52
ldapServerUnreachable 52

license data changed 290
license going to expire 108, 291
license import failed 290
license import succeeded 289
license sync failed 289
license sync succeeded 288
license threshold exceeded 121, 324
licenseChanged 290
licenseGoingToExpire 108, 291
licenseImportFail 290
licenseImportSuccess 289
licenseSyncFail 289
licenseSyncSuccess 288
licenseThresholdExceeded 121, 324
licensing alarms 108
licensing interface events 288
logging events 44
lostCnxnToDblade 76, 206
LS authentication failure 113
lS authentication failure 62
ls authentication failure 144, 297

M

mac-spoofing rogue ap 141
mac-spoofingRogueAPDetected 141
mailSendFailed 307
mailSendSuccess 307
map disconnected 150
map downlink connected 150
map downlink connected to emap 151
map downlink connected to map 156
map downlink disconnected from emap 151
map downlink disconnected from map 157
map uplink connected to emap 152
map uplink connected to map 154
map uplink connected to rap 153
map uplink disconnected from emap 153
mapDisconnected 150
mapDlinkConnected 150
mapDlinkConnectWitheMap 151
mapDlinkConnectWithMap 156
mapDlinkDisconnectWitheMap 151
mapDlinkDisconnectWithMap 157
mapUlinkConnectToeMap 152
mapUlinkConnectToMap 154
mapUlinkConnectToRap 153
mapUlinkDisconnectToeMap 153
memory threshold back to normal 323
memory threshold exceeded 120, 322
memoryThresholdBackToNormal 323
memoryThresholdExceeded 120, 322
Mesh state update to rap no channel 156
mesh state updated to map 154
mesh state updated to map no channel 155
mesh state updated to rap 155
meshStateUpdateToMap 154
meshStateUpdateToMapNoChannel 155
meshStateUpdateToRap 155
meshStateUpdateToRapNoChannel 156

N

new node failed to join 78, 228
new node joined successfully 227
newNodeJoinFailed 78, 228
newNodeJoinSuccess 227
No LS responses 143
no LS responses 61, 112
no ls responses 297
node back in service 243
node bond interface down 84, 236
node bond interface up 237
Node ip address changed 237
node out of service 79, 229
node physical interface down 85, 238
node physical interface up 239
node removal completed 228
node removal failed 79, 229
nodeBondInterfaceDown 84, 236
nodeBondInterfaceUp 237
nodeIPChanged 237
nodeOutOfService 79, 229
nodePhyInterfaceUp 239
nodeShutdown 86, 240
ntp time synchronized 240
ntpTimeSynched 240
number of devices exceeded it’s limit 123
number of users exceeded it’s limit 122

O

onboarding registration failed 218
onboarding registration succeeded 217
onboardingRegistrationFailure 218
onboardingRegistrationSuccess 217
overview 44

P

planeLoadingRebalancingFailed 305
planeLoadingRebalancingSucceeded 305
Primary DHCP AP is down detected by secondary DHCP AP. Starting DHCP service on secondary 175
Primary DHCP AP is up detected by secondary DHCP AP. Stopping DHCP service on secondary. 175
Primary or secondary DHCP AP detects 90% of the configured total IPs 177
process restart 114, 309
processRestart 114, 309

R

racADLDAPBindFail 71
racADLDAPFail 70
racADLDAPSuccess 194
racADLDAPTLSFailed 26, 28, 75, 198
racADLDAPTLSSuccess 28
racADNPSFail 73, 196
racADNPSFailToAuthenticate 74, 196, 197
racLDAPFailToFindPassword 72, 195
radius fails to authenticate with AD NPS server 74, 196
radius fails to connect to AD NPS server 73, 196
radius server reachable 183
radius server unreachable 51, 184
radiusServerUnreachable 51
rap downlink connected to map 152
rap downlink disconnected from map 157
rapDlinkDisconnectWithMap 157
rate limit for MOR surpassed 326
rate limit for TOR surpassed 122
rate limit threshold restored 325
rate limit threshold surpassed 324
rateLimitMORSurpassed 122
rateLimitThresholdRestored 325
rateLimitThresholdSurpassed 324
rateLimitTORSurpassed 326
recoverCassandraError 319
Reindex ElasticSearch finished 27
remediation failed 219
remediation succeeded 218
remediationFailure 219
remediationSuccess 218
removeNodeFailed 79, 229
removeNodeSuccess 228
resource unavailable 116, 310
resourceUnavailable 116, 310
restoreClusterFailed 82, 232
restoreClusterSuccess 231
resyncNTPTime 35
rmapDlinkConnectWithMap 152
Rogue AP 139
rogue AP disappeared 142

S

same network rogue ap 141
same-networkRogueAPDetected 141
scgLBSAuthFailed 113, 297
scgLBSConnectFailed 113, 298
scgLBSConnectSuccess 298
scgLBSFwdPassiveCalReq 302
scgLBSFwdPassiveFFReq 302
scgLBSNoResponse 112, 297
scgLBSRcvdMgmtRequest 300
scgLBSRcvdUnrecognizedRequest 303
scgLBSSendAPInfobyVenueReport 300
scgLBSSendClientInfo 301
scgLBSSendVenuesReport 301
scgLBSStartLocationService 299
SCI and FTP have been disabled 111, 294
SCI has been disabled 110, 293
Secondary DHCP AP is down detected by primary DHCP AP 176
Secondary DHCP AP is up detected by primary DHCP AP 176
service unavailable 115, 309
serviceUnavailable 115, 309
sessDeletedAtDblade 207
sessDeleteErrAtDblade 208
session delete at DP failed 208
session deleted at DP 207
session interface events 110, 292, 295
session update at DP failed 207
session updated at DP 206
sessUpdatedAtDblade 206
sessUpdateErrAtDblade 207
smartMonitorTurnOffWLAN 166
smartRoamDisconnect 216
SmartZone 301
SmartZone connected to LS 298
SmartZone failed to connect to LS 298

SmartZone forwarded calibration request to AP 302
SmartZone forwarded footfall request to AP 302
SmartZone received management request 300
SmartZone received passive request 299
SmartZone received unrecognized request 303
SmartZone sent AP info by venue report 300
SmartZone sent associated client report 301
SmartZone sent controller information report 299
sms sent failed 308
sms sent successfully 308
smsSendFailed 308
smsSendSuccess 308
ssid-spoofing rogue AP 139
ssid-spoofingRogueAPDetected 139
start CALEA mirroring client 222
Start CALEA mirroring client in data plane 314
stop CALEA mirroring client 222
Stop CALEA mirroring client in data plane 314
successfully established the TLS tunnel with AD/LDAP 197
syslog server reachable 303
syslog server switched 304
syslog server unreachable 114, 304
syslogServerReachable 303
syslogServerSwitched 304
syslogServerUnreachable 114, 304
system interface events 296

T

threshold alarms 119
threshold events 321
threshold-crossing alerts 44
timestamp 45
tooManyUsers 122
tunnel alarms 124
tunnel events - datablade 335

U

unauthorized COA/DM message dropped 131
unauthorizedCoaDmMessageDropped 131
Unsync NTP time 89, 250
unsyncNTPTime 89, 250
updating ap configuration 135
updating ap firmware 135
upgrade SSTable failed 255
upgradeClusterFailed 83, 233
upgradeClusterNodeSuccess 232
upgradeEntireClusterSuccess 233
upgradeSSTableFailed 255
uploadClusterVDPFirmwareFailed 246

W

wds device joined 220
wds device left 220
wdsDeviceJoin 220
wdsDeviceLeave 220
wechat ESP authentication server reachable 186
weChat ESP authentication server resolvable 187
WeChat ESP authentication server unreachable 187
weChat ESP authentication server unreachable 53
weChat ESP authentication server unresolvable 54, 188
weChat ESP DNAT server reachable 188
weChat ESP DNAT server resolvable 189
weChat ESP DNAT server unreachable 54, 189
weChat ESP DNAT server unresolvable 190
wired client authorization successfully 224
wired client disconnected 224
wired client failed to join 223
wired client joined 223
wired client session expired 225
wiredClientAuthorization 25, 224
wiredClientDisconnect 25, 224
wiredClientJoin 25, 223
wiredClientJoinFailure 25, 223
wiredClientSessionExpiration 25, 225

Z

zD AP Migrated 317

ZD AP Migrating 317
ZD AP Migration Failed 318
zD AP Rejected 318
zdAPMigrated 317
zdAPMigrating 317
zdAPMigrationFailed 318
zdAPRejected 318
zone configuration preparation failed 93, 260
zoneAffinityLastDpDisconnected 26
zoneCfgPrepareFailed 93, 94, 260

Ruckus®
Simply Better Wireless.

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com