Ruckus Wireless™ SmartCell Gateway™ 200 and Virtualized SmartZone High-Scale™

Alarm and Event Reference Guide for SmartZone 3.1.2

Part Number 800-71109-001 Rev A
Published December 2015

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Copyright 2015. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. (“Ruckus”), or as expressly provided by under license from Ruckus.

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

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, Channelfly, Smartcell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Guide

Document Conventions 22
Terminology 23
Revision History 27
Alarm 27
New Alarm 27
Event 27
New Event 27
Re-added Event 28
Renamed Event 28
Related Documentation 28
Online Training Resources 28
Documentation Feedback 29

1 Revision History

RuckOS Version 3.0 31
New Alarm 31
Deprecated Alarm 32
Renamed Alarm Type 33
Modification of Alarm Severity 33
Renamed Alarm 34
New Event 35
Deprecated Event 38
Re-added Event 38
Modifications to Event Severity 38
Renamed Event Type 39
Renamed Event 40
RuckOS Version 3.1 43
New Alarm 43
Deprecated Alarm 44
Renamed Alarm 44
New Event 45
Modified Event Severity 47

Renamed Event 48
SmartZone Version 3.1.1 52
New Alarm 52
New Event 52
Re-added Event 53
Renamed Event 53
SmartZone Version 3.1.2 54
New Alarm 54
New Event 54

1 Alarm and Event Management
Overview 56
Alarm and Event Management 56
Event Categories 56
Event Attributes 57
Generation of Alarm and Event 57

2 Alarm Types
Accounting Alarms 62
Accounting server not reachable 62
Accounting failover to secondary 63
Accounting fallback to primary 63
AP accounting message mandatory parameter missing 64
AP accounting message decode failed 65
AP account message drop while no accounting start message 66
Unauthorized CoA/DM message dropped 67
AP Communication Alarms 68
AP rejected 68
AP configuration update failed 69
AP swap model mismatched 69
AP pre-provision model mismatched 70
AP firmware update failed 70
AP WLAN oversubscribed 71
AP join zone failed 72
AP LBS Alarms 73
No LS responses 73
LS authentication failure 73
AP failed to connect to LS 74
AP State Change Alarms 75

AP rebooted by system . . . 75
AP disconnected . . . 76
AP deleted . . . 76
AP cable modem interface down . . . 77
Authentication Alarms . . . 78
Authentication server not reachable . . . 78
Authentication failed over to secondary . . . 79
Authentication fallback to primary . . . 80
Control and Data Plane Interface Alarms . . . 81
DP disconnected . . . 81
Cluster Alarms . . . 82
New node failed to join . . . 82
Node removal failed . . . 83
Node out of service . . . 84
Cluster in maintenance state . . . 84
Cluster backup failed . . . 85
Cluster restore failed . . . 86
Cluster upgrade failed . . . 86
Cluster application stopped . . . 87
Node bond interface down . . . 88
Node physical interface down . . . 88
Cluster node rebooted . . . 89
Cluster node shut down . . . 90
Disk usage exceed threshold . . . 90
Cluster out of service . . . 91
Configuration backup failed . . . 91
Configuration restore failed . . . 92
AP Certificate Expired . . . 93
Data Plane Alarms . . . 94
Data plane configuration update failed . . . 94
Data plane disconnected . . . 95
Data plane physical interface down . . . 95
Data plane rebooted . . . 96
Data plane packet pool is under low water mark . . . 96
Data plane packet pool is under critical low water mark . . . 97
Data plane core dead . . . 97
Data plane process restarted . . . 98
GA Interface Alarms . . . 99
Connection to CGF failed . . . 99

CDR transfer failed . . . 100
CDR generation failed . . . 101
Gn/S2a Interface Alarms . . . 102
GGSN restarted . . . 102
GGSN not reachable . . . 103
GGSN not resolved . . . 103
PDNGW could not be resolved . . . 104
PDNGW version not supported . . . 105
Associated PDNGW down . . . 105
Create session response failed . . . 106
Decode failed . . . 107
Modify bearer response failed . . . 107
Delete session response failed . . . 108
Delete bearer request failed . . . 109
Update bearer request failed . . . 109
CGF server not configured . . . 110
GR Interface Alarms . . . 111
Destination not reachable . . . 111
App server down . . . 112
App server inactive . . . 112
Association establishment failed . . . 113
Association down . . . 114
Outbound routing failure . . . 114
Did allocation failure . . . 115
IPMI Alarms . . . 116
ipmiVoltage . . . 117
ipmiThempBB . . . 118
ipmiThempFP . . . 119
ipmiThempIOH . . . 119
ipmiThempMemP . . . 120
ipmiThempPS . . . 121
ipmiThempP . . . 122
ipmiThempHSBP . . . 122
ipmiFan . . . 123
ipmiPower . . . 123
ipmiCurrent . . . 124
ipmiFanStatus . . . 124
ipmiPsStatus . . . 125
ipmiDrvStatus . . . 126

Licensing Alarms . . . 127
TTG session critical threshold . . . 127
TTG session license exhausted . . . 128
PMIPv6 Alarms . . . 129
Config update failed . . . 129
LMA ICMP unreachable . . . 130
LMA failed over . . . 130
DHCP connection lost . . . 131
Session Alarms . . . 132
Binding failed . . . 132
STA Interface Alarms . . . 133
STA authentication failed transport down . . . 133
STA authentication failed failure response . . . 134
STA authentication failed decode failure . . . 135
STA re-authorization failed . . . 135
STA response timer expired . . . 136
Retransmission exhausted . . . 137
System Alarms . . . 138
No LS responses . . . 139
LS authentication failure . . . 139
{produce.short.name} failed to connect to LS . . . 140
Process restart . . . 140
Service unavailable . . . 141
Keepalive failure . . . 141
Resource unavailable . . . 142
HIP failed over . . . 142
Diameter initialization error . . . 143
Diameter peer transport failure . . . 144
Diameter CER error . . . 144
Diameter peer add error . . . 145
Diameter peer remove successful . . . 146
Diameter realm entry error . . . 146
Diameter fail over to alternate peer . . . 147
Diameter fail back to peer . . . 148
Diameter CEA unknown peer . . . 149
Diameter no common application . . . 149
Process initiated . . . 150
PMIPv6 unavailable . . . 151
Memory allocation failed . . . 152

Threshold Alarms . . . 153
CPU threshold exceeded . . . 153
Memory threshold exceeded . . . 154
Disk usage threshold exceeded . . . 154
License threshold exceeded . . . 155
Rate limit for TOR surpassed . . . 156
The number of users exceeded its limit . . . 156
The number of devices exceeded its limit . . . 157
Tunnel Alarms - Access Point . . . 158
AP softGRE gateway not reachable . . . 158
AP is disconnected from secure gateway . . . 158
AP secure gateway association failure . . . 159

3 Events Types

3rd Party Access Point Events . . . 161
3rd party AP connected . . . 161
Accounting Events . . . 162
Accounting session started . . . 162
Accounting session start failed . . . 163
Accounting session disabled . . . 164
Accounting session stopped successfully . . . 164
Accounting session stopped failed . . . 165
Accounting session interim failed . . . 166
Accounting server not reachable . . . 166
Accounting failed over to secondary . . . 167
Accounting fallback to primary . . . 168
AP accounting message mandatory parameter missing . . . 169
Unknown realm . . . 170
AP accounting message decode failed . . . 170
AP accounting retransmission message dropped . . . 171
AP accounting response while invalid config . . . 172
AP account message drop while no accounting start message . . . 173
Unauthorized COA/DM message dropped . . . 174
AP Authentication Events . . . 175
Radius server reachable . . . 175
Radius server unreachable . . . 175
LDAP server reachable . . . 176
LDAP server unreachable . . . 176
AD server reachable . . . 177

AD server unreachable . . . 177
AP Communication Events . . . 178
AP discovery succeeded . . . 179
AP managed . . . 179
AP rejected . . . 180
AP firmware updated . . . 180
AP firmware update failed . . . 181
Updating AP firmware . . . 181
Updating AP configuration . . . 182
AP configuration updated . . . 182
AP configuration update failed . . . 183
AP pre-provision model mismatched . . . 183
AP swap model mismatched . . . 184
AP WLAN oversubscribed . . . 184
AP join zone failed . . . 185
AP illegal to change country code . . . 185
Rogue AP . . . 186
SSID-spoofing rogue AP . . . 186
MAC-spoofing rogue AP . . . 187
Same-network rogue AP . . . 187
Ad-hoc network device . . . 188
Rogue AP disappeared . . . 188
AP LBS Events . . . 189
No LS responses . . . 189
LS authentication failure . . . 190
AP connected to LS . . . 190
AP failed to connect to LS . . . 191
AP started location service . . . 191
AP stopped location service . . . 192
AP received passive calibration request . . . 192
AP received passive footfall request . . . 193
AP received unrecognized request . . . 193
AP Mesh Events . . . 194
EMAP downlink connected to MAP . . . 194
EMAP downlink disconnected from MAP . . . 195
EMAP uplink connected to MAP . . . 195
EMAP uplink disconnected from MAP . . . 196
MAP disconnected . . . 196
MAP downlink connected . . . 196

MAP downlink connected to EMAP 197
MAP downlink disconnected from EMAP 197
RAP downlink connected to MAP 198
MAP uplink connected to EMAP 198
MAP uplink disconnected from EMAP 199
MAP uplink connected to RAP 199
MAP uplink connected to MAP 200
Mesh state updated to MAP 200
Mesh state updated to MAP no channel 201
Mesh state updated to RAP 201
Mesh state update to RAP no channel 202
MAP downlink connected to MAP 202
MAP downlink disconnected from MAP 203
RAP downlink disconnected from MAP 203
AP State Change Events 204
AP rebooted by user 204
AP rebooted by system 205
AP disconnected 205
AP IP address updated 206
AP reset to factory default 206
AP channel updated 206
AP country code updated 207
AP channel updated because dynamic frequency selection (DFS) detected a radar . . 207
AP change control plane 208
AP connected 208
AP deleted 208
AP heartbeat lost 209
AP tagged as critical 209
AP cable modem interface down 210
AP brownout 210
AP cable modem power-cycled by user 210
AP smart monitor turn off WLAN 211
AP CLB limit reached 211
AP CLB limit recovered 212
AP WLAN state changed 212
AP capacity reached 213
AP capacity recovered 213
AP cable modem interface up 214
AP cable modem soft-rebooted by user 214

AP cable modem set to factory default by user . . . 215
AP USB Events . . . 216
AP USB software package downloaded . . . 216
AP USB software package download failed . . . 216
Authentication Events . . . 217
Authentication server not reachable . . . 217
Unknown realm . . . 218
Authentication succeeded . . . 218
Authentication failed . . . 219
Pseudonym authentication succeeded . . . 219
Pseudonym authentication failed . . . 220
Fast re-authentication succeeded . . . 221
Fast re-authentication failed . . . 222
Authentication failed over to secondary . . . 222
Authentication fallback to primary . . . 223
Authorization Events . . . 224
DM received from AAA . . . 224
DM NACK sent to AAA . . . 225
DM sent to NAS . . . 225
DM NACK received from NAS . . . 226
CoA received from AAA . . . 226
CoA NACK sent to AAA . . . 227
CoA sent NAS . . . 227
CoA NAK received NAS . . . 228
CoA authorize only access reject . . . 228
CoA RWSG MWSG notification failure . . . 229
Control and Data Plane Interface . . . 230
DP connected . . . 230
DP disconnected . . . 231
Session updated at DP . . . 231
Session update at DP failed . . . 232
Session deleted at DP . . . 232
Session delete at DP failed . . . 233
C2d configuration failed . . . 234
Client Events . . . 235
Client authentication failed . . . 236
Client joined . . . 236
Client failed to join . . . 237
Client disconnected . . . 237

Client connection timed out 238
Client authorization successfully 238
Client authorization failed 239
Client session expired 239
Client roaming 240
Client logged out 240
3rd party client join 241
3rd party client inactivity timeout 241
3rd party client authorization 242
3rd party client authorization failure 242
3rd party client session expiration 243
3rd party client roaming 243
3rd party client session logout 244
Client roaming disconnected 244
Client blocked 245
Client grace period 245
Onboarding registration succeeded 246
Onboarding registration failed 246
Remediation succeeded 247
Remediation failed 247
Force DHCP disconnected 248
Cluster Events 249
Cluster created successfully 249
New node joined successfully 250
New node failed to join 250
Node removal completed 251
Node removal failed 251
Node out of service 252
Cluster in maintenance state 252
Cluster back in service 253
Cluster backup completed 253
Cluster backup failed 253
Cluster restore completed 254
Cluster restore failed 254
Cluster node upgrade completed 255
Entire cluster upgraded successfully 255
Cluster upgrade failed 256
Cluster application stopped 256
Cluster application started 257

Cluster backup started . . . 257
Cluster upgrade started . . . 258
Cluster leader changed . . . 258
Node bond interface down . . . 259
Node bond interface up . . . 259
Node IP address changed . . . 260
Node physical interface down . . . 260
Node physical interface up . . . 261
Cluster node rebooted . . . 261
NTP time synchronized . . . 262
Cluster node shutdown . . . 262
Cluster upload started . . . 263
Cluster upload completed . . . 263
Cluster upload failed . . . 264
SSH tunnel switched . . . 264
Cluster remove node started . . . 264
Node back in service . . . 265
Resync NTP Time . . . 265
Disk usage exceed threshold . . . 266
Cluster out of service . . . 266
Initiated moving APs in node to a new cluster . . . 267
Configuration backup started . . . 267
Configuration backup succeeded . . . 268
Configuration backup failed . . . 268
Configuration restore succeeded . . . 268
Configuration restore failed . . . 269
AP Certificate Expired . . . 269
AP Certificate Updated . . . 270
Node IPv6 address added . . . 270
Node IPv6 address deleted . . . 271
Configuration Events . . . 272
Configuration updated . . . 272
Configuration update failed . . . 272
Configuration receive failed . . . 273
Incorrect flat file configuration . . . 274
Data Plane Events . . . 275
Data plane discovered . . . 275
Data plane discovery failed . . . 276
Data plane configuration updated . . . 276

Data plane configuration update failed . . . 277
Data plane rebooted . . . 277
Data plane heartbeat lost . . . 277
Data plane IP address updated . . . 278
Data plane updated to a new control plane . . . 278
Data plane status update failed . . . 279
Data plane statistics update failed . . . 279
Data plane connected . . . 280
Data plane disconnected . . . 280
Data plane physical interface down . . . 281
Data plane physical interface up . . . 281
Data plane packet pool is under low water mark . . . 282
Data plane packet pool is under critical low water mark . . . 282
Data plane packet pool is above high water mark . . . 283
Data plane core dead . . . 283
Data plane process restarted . . . 284
DHCP Events . . . 285
DHCP inform received . . . 285
DHCP dcln received . . . 286
GA Interface Events . . . 287
Connection to CGF failed . . . 287
CGF keep alive not responded . . . 288
CDR transfer succeeded . . . 288
CDR transfer failed . . . 289
CDR generation failed . . . 289
Gn/S2a Interface Events . . . 290
GGSN restarted . . . 290
GGSN not reachable . . . 291
Echo response not received . . . 291
GGSN not resolved . . . 292
PDP context established . . . 292
PDP create failed . . . 293
PDP update by HLR succeeded . . . 293
PDP update by HLR failed . . . 294
PDP update by roaming succeeded . . . 294
PDP update by roaming failed . . . 295
PDP update by GGSN succeeded . . . 296
PDP update by GGSN failed . . . 296
PDP delete by TTG succeeded . . . 297

PDP delete by TTG failed . . . 297
PDP delete by GGSN succeeded . . . 298
PDP delete by GGSN failed . . . 298
IP assigned . . . 299
IP not assigned . . . 299
Unknown UE . . . 300
PDP update success COA . . . 300
PDP update fail COA . . . 301
PDNGW could not be resolved . . . 301
PDNGW version not supported . . . 302
Associated PDNGW down . . . 302
Create session response failed . . . 303
Decode failed . . . 304
Modify bearer response failed . . . 304
Delete session response failed . . . 305
Delete bearer request failed . . . 305
Update bearer request failed . . . 306
CGF server not configured . . . 307
Gr Interface Event . . . 308
Destination not reachable . . . 309
Destination available . . . 309
App server down . . . 310
App server inactive . . . 310
App server active . . . 311
Association establishment failed . . . 311
Association down . . . 312
Association up . . . 312
Send auth info success . . . 313
Auth info sending failed . . . 313
GPRS location update succeeded . . . 314
GPRS location update failed . . . 314
Insert sub data success . . . 315
Insert sub data failed . . . 315
Outbound routing failure . . . 316
Did allocation failure . . . 316
Restore data success . . . 317
Restore data failed . . . 317
IPMI Events . . . 318
ipmiVoltage . . . 318

ipmiThempBB . . . 319
ipmiThempFP . . . 319
ipmiThempIOH . . . 320
ipmiThempMemP . . . 320
ipmiThempPS . . . 321
ipmiThempP . . . 321
ipmiThempHSBP . . . 322
ipmiFan . . . 322
ipmiPower . . . 323
ipmiCurrent . . . 323
ipmiFanStatus . . . 324
ipmiPsStatus . . . 324
ipmiDrvStatus . . . 325
ipmiREVotage . . . 325
ipmiREThempBB . . . 326
ipmiREThempFP . . . 326
ipmiREThempIOH . . . 326
ipmiREThempMemP . . . 327
ipmiREThempPS . . . 327
ipmiREThempP . . . 328
ipmiREThempHSBP . . . 328
ipmiREFan . . . 328
ipmiREPower . . . 329
ipmiRECurrent . . . 329
ipmiREFanStatus . . . 330
ipmiREPsStatus . . . 330
ipmiREDrvStatus . . . 331
Licensing Interface Events . . . 332
TTG session warning threshold . . . 332
TTG session major threshold . . . 333
TTG session critical threshold . . . 333
TTG session license exhausted . . . 334
License sync succeeded . . . 334
License sync failed . . . 335
License import succeeded . . . 335
License import failed . . . 336
License data changed . . . 336
Location Delivery Events . . . 337
Unavailable location info requested . . . 337

Incapable location info requested . . . 338
Unsupported location delivery request . . . 338
PMIPv6 Events . . . 339
Config update failed . . . 339
LMA ICMP reachable . . . 339
LMA ICMP unreachable . . . 340
LMA server unreachable . . . 340
LMA failed over . . . 341
Connect To DHCP . . . 341
DHCP connection lost . . . 342
Session Events . . . 343
Session timeout . . . 343
Delete all . . . 344
Binding succeeded . . . 344
Binding failed . . . 345
Binding time expired . . . 345
Binding revoked . . . 346
Binding released . . . 346
STA Interface Events . . . 347
STA successful authentication . . . 347
STA authentication failed transport down . . . 348
STA authentication failed failure response . . . 348
STA authentication failed decode failure . . . 349
STA session termination {produce.short.name} initiated success . . . 349
STA session termination AAA initiated success . . . 350
STA session termination AAA initiated failed . . . 351
STA re-authorization successful . . . 351
STA re-authorization failed . . . 352
STA response timer expired . . . 352
Retransmission exhausted . . . 353
System Events . . . 354
No LS responses . . . 355
LS authentication failure . . . 355
{produce.short.name} connected to LS . . . 355
{produce.short.name} failed to connect to LS . . . 356
{produce.short.name} received passive request . . . 357
{produce.short.name} sent controller information report . . . 357
{produce.short.name} received management request . . . 358
{produce.short.name} sent AP info by venue report . . . 358

{produce.short.name} sent query venues report . . . 359
{produce.short.name} sent associated client report . . . 359
{produce.short.name} forwarded calibration request to AP . . . 360
{produce.short.name} forwarded footfall request to AP . . . 360
{produce.short.name} received unrecognized request . . . 361
FTP transfer . . . 361
FTP transfer error . . . 361
File upload . . . 362
Email sent successfully . . . 362
Email sent failed . . . 363
SMS sent successfully . . . 363
SMS sent failed . . . 364
Process restart . . . 364
Service unavailable . . . 365
Keepalive failure . . . 365
Resource unavailable . . . 366
HIP started . . . 366
HIP stopped . . . 367
HIP failed over . . . 367
Standby HIP restarted . . . 368
HIP cache cleaned . . . 368
Diameter initialization error . . . 369
Diameter initialization . . . 369
Diameter peer transport failure . . . 370
Diameter CER error . . . 370
Diameter CER success . . . 371
Diameter invalid version . . . 372
Diameter peer add error . . . 372
Diameter peer add successful . . . 373
Diameter peer remove successful . . . 374
Diameter realm entry error . . . 374
Diameter failover to alternate peer . . . 375
Diameter fail back to peer . . . 376
Diameter CEA unknown peer . . . 376
Diameter no common application . . . 377
ZD AP migrating . . . 378
ZD AP migrated . . . 378
ZD AP rejected . . . 379
ZD AP migration failed . . . 379

Database error . . . 380
Process initiated . . . 380
PMIPv6 unavailable . . . 381
Memory allocation failed . . . 381
Process stopped . . . 382
Threshold Events . . . 383
CPU threshold exceeded . . . 383
Memory threshold exceeded . . . 384
Disk usage threshold exceeded . . . 384
CPU threshold back to normal . . . 385
Memory threshold back to normal . . . 385
Disk threshold back to normal . . . 385
License threshold exceeded . . . 386
Rate limit threshold surpassed . . . 386
Rate limit threshold restored . . . 387
Rate limit for TOR surpassed . . . 388
The number of users exceed its limit . . . 388
The number of devices exceeded its limit . . . 389
Tunnel Events - Access Point (AP) . . . 390
Data plane accepted a tunnel request . . . 390
Data plane rejected a tunnel request . . . 391
Data plane terminated a tunnel . . . 391
AP created a tunnel . . . 392
AP tunnel disconnected . . . 392
AP softGRE tunnel fails over primary to secondary . . . 393
AP softGRE tunnel fails over secondary to primary . . . 393
AP softGRE gateway reachable . . . 394
AP softGRE gateway not reachable . . . 394
Data plane set up a tunnel . . . 395
AP secure gateway association success . . . 395
AP is disconnected from secure gateway . . . 396
AP secure gateway association failure . . . 396
Tunnel Events - Data Plane . . . 397
DP softGRE GW unreachable . . . 397
DP softGRE keepalive timeout . . . 398
DP softGRE GW inactive . . . 398
DP DHCPRelay no resp . . . 399
DP DHCPRelay failOver . . . 399
DP softGRE new tunnel . . . 400

DP softGRE del tunnel 400
DP softGRE keepalive recovery 401
DP DHCPRelay response recovery 401
DP softGRE GW reachable 402
DP softGRE GW active 402
DP softGRE GW failover. 403

Index

About This Guide

This *SmartZone ™ Alarm and Event Reference Guide* describes the various types of alarms and events that the controller (SCG-200 or vSZ-H) 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
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AD	Active Directory
AMBR	Aggregate Maximum Bit Rate
AP	Access Point
APN	Access Point Name
ASP	Application Service Provider
ASPDN	ASP Down
ASPDN ACK	ASP Down Acknowledgment
ASR	Abort Session Request
AVP	Ruckus Vendor specific attribute Pair
BMD	Billing Mediation Device is a network component in a telecommunications network that receives, processes, reformats and sends information to other formats between network elements.
BSSID	Basic Service Set Identifier
CDF	Charging Data Function
CDR	Call Detail Record. A formatted collection of information on chargeable events used for accounting and billing. For example, call set-up, call duration and amount of data transferred.
CEA	Capabilities Exchange Answer
CER	Capabilities Exchange Request
CGF	Charging Gateway Function
CHAP	Challenge Handshake Authentication Protocol
CIP	Channel Interface Processor
CLB	Client Load Balance

Table 3. Terms used

Term	Description
CNN	Configuration Change Notifier
CNR	Configuration Notification Receiver
CoA	Change of Authorization
Controller	Refers to either SCG-200 or vSZ-H as the case may be.
CTF	Charging Trigger Function
DEA	Diameter-EAP-Answer
DER	Diameter-EAP-Request
DHCP	Dynamic Host Configuration Protocol
DM	Dynamic Multipoint
DNS	Domain Name System
DPR	Diameter Disconnect Peer Request
DRT	Data Record Transfer
EAP	Extensible Authentication Protocol
EBI	EPS Bearer ID
EMAP	Ethernet Mesh AP
EPC	Evolved Packet Core
EPS	Evolved Packet System
F-TEID	Fully Qualified Tunnel Endpoint Identifier
FTP	File Transfer Protocol
Ga	Reference point between a CDF and the CGF for CDR transfer
GGSN	Gateway GPRS Support Node
GPDU	GTP Packet Data Unit
GPRS	General Packet Radio Service
GSN	GPRS Support Node
GSN APN	GPRS serving node, is application module in the SCG handling GTP messages
GTP	GPRS Tunneling Protocol
GTP-C	GTP control plane

Table 3. Terms used

Term	Description
GTP-U	GTP user plane
GTP'	GPRS protocol, used for CDR transport. It is derived from GTP with enhancements to improve transport reliability necessary for CDRs
GTPP	GPRS Tunneling Protocol Prime
GTPv1-U	GTP version 1, user plane
GTPv2-C	GTP version 2, control plane
HIP	Host Identity Protocol
HLR	Home Location Register
ICMP	Internet Control Message Protocol
IE	Information Element
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IPSP	IP Signalling Protocol
LBS	Location Based Service
LCS	Location Services
LDAP	Lightweight Directory Access Protocol
LMA	Local Mobility Anchor
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MOR	Maximum Outstanding Requests
MS-ISDN	Mobile Subscriber Integrated Services Digital Network Number
MTU	Maximum Transmission Unit
MWSG	Metro Wireless Security Gateway
NAS	Network Access Server
NTP	Network Time Protocol)
P-GW	Packet Data Network Gateway

Table 3. Terms used

Term	Description
PAA	PDN Address Allocation
PCN	Packet switched Core network Node (SGSN, GGSN, S–GW, P–GW)
PCO	Protocol Configuration Options
PDN	Packet Data Network
PDP	Packet Data Protocol
PGW	PDN Gateway
produce.short.name	Refers to either SCG or vSZ-H
R-WSG/WSG	Ruckus Wireless Security Gateway
RAC	Radio Access Controller
RAP	Root Access Point
RAR	Re-Auth Request
RSSI	Received Signal Strength Indicator
S-CDR	SGSN Call Detail Record
SCG	Ruckus Wireless Smart Cell Gateway
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
SG	Signalling Gateway
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SSID	Service Set Identifier (SSID)
STR	STR (Session Termination-Request)
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TEID	Tunnel End Point Identifier
UDP	User Datagram Protocol
UE	User Equipment
UI	Web User Interface

Revision History

The following are the additions/ modifications/deletions of alarm and event in this guide from SCG-200 version 2.1.3 to SZ 3.1.1

- Alarm
- Event

Alarm

- New Alarm

New Alarm

Table 4. New Alarm

Alarm Code	Alarm
661	ipsecTunnelDisAssociated
662	ipsecTunnelAssociateFailed

Event

- New Event
- Re-added Event
- Renamed Event

New Event

Table 5. New Events

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

Table 5. New Events

Event Code	Event
2121	ldapServerReachable
2122	ldapServerUnreachable
2141	adServerReachable
2142	adServerUnreachable
2201	zoneInitiatedMovingAp
2501	nodeIPv6Added
2502	nodeIPv6Deleted

Re-added Event

Table 6. Re-added Event

Event Code	Event
101	apDiscoverySuccess

Renamed Event

The following is the renamed event on the SCG web interface

Table 7. Renamed Events

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

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:

- Ruckus Wireless SmartZone Administrator Guide (Release 3.1.1)
- Part number: 800-70917-001
- Page 88

Revision History

1

This chapter contains revision history for:

- RuckOS Version 3.0
- RuckOS Version 3.1
- SmartZone Version 3.1.1
- SmartZone Version 3.1.2

RuckOS Version 3.0

The following is the revision history from SCG version 2.6 to RuckOS 3.0.

New Alarm

Table 8. New Alarm

Alarm Code	Alarm
115	apJoinZoneFailed
510	dpReboot
614	apSoftGREGatewayNotReachable
701	apLBSNoResponses
702	apLBSAuthFailed
704	apLBSConnectFailed
721	scgLBSNoResponse
722	scgLBSAuthFailed
724	scgLBSConnectFailed
834	diskUsageExceed
1008	cfgUpdFailed
1302	rateLimitMORSurpassed
5001	processInit
5002	pmipUnavailable
5003	unallocatedMemory
5004	updateCfgFailed
5006	lmaIcmpUnreachable
5008	lmaFailOver
5010	bindingFailure
5102	lostCnxnToDHCP

Deprecated Alarm

Table 9. Deprecated Alarm

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

Table 9. Deprecated Alarm

Alarm Code	Alarm
821	clusterAppStart
822	removeNodeSuccess
823	restoreClusterSuccess
824	nodeBackToInService
833	sshTunnelSwitched
971	ftpTransferError
1010	smfRegFailed

Renamed Alarm Type

Table 10. Renamed Alarm Type

Alarm Code	Alarm Type	Renamed To
108	apWlanMismatched	apWlanOversubscribed
1242	sessionCriticalThreshold	ttgSessionCriticalThreshold
1243	sessionLicenseExausted	ttgSessionLicenseExausted
1302	rateLimitTORSurpassed	rateLimitMORSurpassed
1626	assocCantStart	assocEstbFailed
1960	CGFServerNotConfigured	cgfServerNotConfigured
5004	updateCgfFailed	updateCfgFailed

Modification of Alarm Severity

Table 11. Modification of Alarm Severity

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

Renamed Alarm

Table 12. Renamed Alarm

Code	Alarm Name	Renamed To
104	AP model different with swap AP configuration	AP swap model mismatched
105	AP model different with pre-provision configuration	AP pre-provision model mismatched
108	AP WLAN mismatched	AP WLAN oversubscribed
809	Control plane interface down	Node bond interface down
810	Control plane physical interface down	Node physical interface down
952	Disk Usage threshold exceeded	Disk usage threshold exceeded
1003	Keep alive failure	Keepalive failure
1016	HIP Failover	HIP failed over
1202	Lost connection to Data plane	DP disconnected
1302	Rate Limit for Total Outstanding Requests (TOR) Surpassed	Rate Limit for MOR surpassed
1618	Destination Not reachable	Destination not reachable
1626	Association cannot Start	Association establishment failed
1902	Unknown realm accounting	Unknown realm
1909	apAcctRespWhileInvalidConfig	AP accounting response while invalid config
1910	apAcctMsgDropNoAcctStartMsg	AP account message drop while no accounting start message
1911	unauthorizedCoaDmMessageDropped	Unauthorized CoA/DM message dropped
1960	CGFServerNotConfigured	CGF Server Not Configured
5001	Initial Process	Process initiated
5002	PMIPv6 is Unavailable	PMIPv6 unavailable
5004	Update config failed	Config update failed
5006	LMA ICMP is unreachable	LMA ICMP unreachable
5008	LMA failover	LMA failed over

Table 12. Renamed Alarm

Code	Alarm Name	Renamed To
5010	Binding failure	Binding failed
5102	Lost DHCP connection	DHCP connection lost

New Event

Table 13. New Event

Event Code	Event
115	apJoinZoneFailed
116	apIllgalToChangeCountryCode
180	genericRogueAPDetected
181	ssid-spoofingRogueAPDetected
182	mac-spoofingRogueAPDetected
183	same-networkRogueAPDetected
184	ad-hoc-networkRogueAPDetected
185	maliciousRogueAPTimeout
218	smartRoamDisconnect
219	clientBlockByDeviceType
220	clientGracePeriod
221	onboardingRegistrationSuccess
222	onboardingRegistrationFailure
225	forceDHCPDisconnect
319	319##smartMonitorTurnOffWLAN
320	apCLBlimitReached
321	apCLBlimitRecovered
322	apWLANStateChanged
323	apCapacityReached
324	apCapacityRecovered
516	dpPktPoolLow
517	dpPktPoolCriticalLow

Table 13. New Event

Event Code	Event
518	dpPktPoolRecover
519	dpCoreDead
611	apSoftGRETunnelFailoverPtoS
612	apSoftGRETunnelFailoverStoP
613	apSoftGREGatewayReachable
614	apSoftGREGatewayNotReachable
701	apLBSNoResponses
702	apLBSAuthFailed
703	apLBSConnectSuccess
704	apLBSConnectFailed
705	apLBSStartLocationService
706	apLBSStopLocationService
707	apLBSRcvdPassiveCalReq
708	apLBSRcvdPassiveFFReq
709	apLBSRcvdUnrecognizedRequest
721	scgLBSNoResponse
722	scgLBSAuthFailed
723	scgLBSConnectSuccess
724	scgLBSConnectFailed
725	scgLBSStartLocationService
726	scgLBSRcvdNoPayload
727	scgLBSSentControllerInfo
728	scgLBSRcvdMgmtRequest
729	scgLBSSendAPInfobyVenueReport
730	scgLBSSendVenuesReport
731	scgLBSSendClientInfo
732	scgLBSFwdPassiveCalReq
733	scgLBSFwdPassiveFFReq

Table 13. New Event

Event Code	Event
734	scgLBSRcvdUnrecognizedRequest
837	resyncNTPTime
838	diskUsageExceed
981	mailSendSuccess
982	mailSendFailed
983	smsSendSuccess
984	smsSendFailed
1250	licenseSyncSuccess
1251	licenseSyncFail
1252	licenseImportSuccess
1253	licenseImportFail
1254	licenseChanged
1300	rateLimitThresholdSurpassed
1301	rateLimitThresholdRestored
1302	rateLimitMORSurpassed
2001	zdAPMigrating
2002	zdAPMigrated
2003	zdAPRejected
2004	zdAPMigrationFailed
5001	processInit
5002	pmipUnavailable
5003	unallocatedMemory
5004	updateCfgFailed
5005	lmaIcmpReachable
5006	lmaIcmpUnreachable
5007	lmaHbUnreachable
5008	lmaFailOver
5009	bindingSuccess

Table 13. New Event

Event Code	Event
5010	bindingFailure
5011	bindingExpired
5012	bindingRevoked
5013	bindingReleased
5100	processTerminated
5101	connectedToDHCP
5102	lostCnxnToDHCP

Deprecated Event

Table 14. Deprecated Event

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

Re-added Event

Table 15. Re-added Event

Event Code	Event
827	ntpTimeSynched

Modifications to Event Severity

Table 16. Event Severity Modifications

Event Code	Event Code	Severity	Changed To
114	apWlanOversubscribed	Informational	Major
320	apCLBlimitReached	Informational	Warning

Table 16. Event Severity Modifications

Event Code	Event Code	Severity	Changed To
835	nodeBackToInService	Major	Informational
960	licenseThresholdExceeded	Informational	Warning
1007	cfgUpdSuccess	Debug	Informational
1008	cfgUpdFailed	Major	Debug
1009	cfgRcvFailed	Major	Debug
1201	connectedToDblade	Debug	Informational
1209	c2dCfgFailed	Informational	Warning
1301	rateLimitThresholdRestored	Major	Informational
1603	unknownRealm	Major	Debug
1908	apAcctRetransmittedMsgDropped	Major	Debug
1910	apAcctMsgDropNoAcctStartMsg	Major	Critical
1911	unauthorizedCoaDmMessageDropped	Major	Critical
1952	pdnGwVersionNotSupportedMsgReceived	Critical	Major
5006	lmaIcmpUnreachable	Debug	Major

Renamed Event Type

Table 17. Renamed Event Type

Event Code	Event Name	Renamed To
114	apWlanMismatched	apWlanOversubscribed
416	rmapDlinkConnectWithMap	rapDlinkConnectWithMap
511	dpUpdateStatisticFalied	dpUpdateStatisticFailed
1017	standbyHipRestart	hipStandbyRestart
1240	sessionWarningThreshold	ttgSessionWarningThreshold
1241	sessionMajorThreshold	ttgSessionMajorThreshold
1242	sessionCriticalThreshold	ttgSessionCriticalThreshold
1243	sessionLicenseExausted	ttgSessionLicenseExausted
1302	rateLimitTORSurpassed	rateLimitMORSurpassed

Table 17. Renamed Event Type

Event Code	Event Name	Renamed To
1626	assocCantStart	assocEstbFailed
1960	CGFServerNotConfigured	cgfServerNotConfigured

Renamed Event

Table 18. Renamed Event

Code	Event Name	Renamed To
103	AP status changed to Managed	AP managed
112	AP model different with pre-provision configuration	AP pre-provision model mismatched
113	AP model different with swap AP configuration	AP swap model mismatched
114	AP WLAN mismatched	AP WLAN oversubscribed
202	Client joined successfully	Client joined
205	Client connection timed out due to inactivity	Client connection timed out
210	Client session logout	Client logged out
218	Client Roaming Disconnect	Client roaming disconnected
303	AP connection lost	AP disconnected
305	AP reset to factory default settings, new:	AP reset to factory default
311	AP change control plane	AP changed control plane
501	Data plane discovered successfully	Data plane discovered
620	DP Softgre New Tunnel	DP SoftGRE New Tunnel
621	DP Softgre Del Tunnel	DP SoftGRE Del Tunnel
622	DP Softgre KeepAlive Recovery	DP SoftGRE Keepalive Recovery
624	DP SoftgreGW Reachable	DP SoftGRE GW Reachable
625	DP SoftgreGW Active	DP SoftGRE GW Active
826	Cluster Node rebooted	Cluster node rebooted
828	Cluster node shutdown	Cluster node shut down

Table 18. Renamed Event

Code	Event Name	Renamed To
1003	Keep alive failure	Keepalive failure
1014	HIP Started	HIP started
1015	HIP Stopped	HIP stopped
1016	HIP Failover	HIP failed over
1017	Hip Restart	Standby HIP restarted
1018	HIP Cache Cleanup	HIP cache cleaned
1007	Configuration update success	Configuration updated
1201	Connected to Data plane	DP connected
1202	Lost connection to Data plane	DP disconnected
1205	Session updated at Data plane	Session updated at DP
1206	Session update error at Data plane	Session update at DP failed
1207	Session deleted at Data plane	Session deleted at DP
1208	Session delete error at Data plane	Session delete at DP failed
1217	Create PDP Failed	PDP create failed
1218	Initial PDP updated successfully HLR	PDP update by HLR succeeded
1219	Initial PDP updated fail HLR	PDP update by HLR failed
1220	Initial PDP updated successfully Roam	PDP update by Roaming succeeded
1221	Initial PDP updated fail Roam	PDP update by Roaming failed
1222	Received PDP update successfully GGSN	PDP update by GGSN succeeded
1223	Received PDP update fail GGSN	PDP update by GGSN failed
1224	Initial PDP deleted successfully	PDP delete by TTG succeeded
1225	Initial PDP deleted fail	PDP delete by TTG failed
1226	Received PDP deleted successfully	PDP delete by GGSN succeeded
1227	Received PDP deleted fail	PDP delete by GGSN failed
1229	ipAssigned	IP assigned
1300	Rate Limit Threshold Surpassed	Rate limit threshold surpassed

Table 18. Renamed Event

Code	Event Name	Renamed To
1301	Rate Limit Threshold Restored	Rate limit threshold restored
1302	Rate Limit for Total Outstanding Requests (TOR) Surpassed	Rate Limit for TOR surpassed
1604	Authentication success	Authentication succeeded
1606	Pseudonym authentication success	Pseudonym authentication succeeded
1608	Fast re-authentication success	Fast re-authentication succeeded
1612	CGF keep alive not responded	CGF keepalive not responded
1613	CDR transfer successful	CDR transfer succeeded
1618	Destination Not Reachable	Destination not reachable
1623	AppServer Down	App Server Down
1624	AppServer Inactive	App Server Inactive
1625	AppServer Active	App Server Active
1626	Association can not Start	Association establishment failed
1631	send Auth Info Failed	Auth info sending failed
1632	Update GPRS Location Success	GPRS location update succeeded
1633	Update GPRS Location Failed	GPRS location update failed
1902	Unknown realm accounting	Unknown realm
5001	Initial Process	Process initiated
5002	PMIPv6 is Unavailable	PMIPv6 unavailable
5004	Update config failed	Config update failed
5005	LMA ICMP is reachable	LMA ICMP reachable
5006	LMA ICMP is unreachable	LMA ICMP unreachable
5007	LMA server is unreachable	LMA server unreachable
5008	LMA failover	LMA failed over
5009	Binding success	Binding succeeded
5010	Binding failure	Binding failed

Table 18. Renamed Event

Code	Event Name	Renamed To
5012	Revoke binding	Binding revoked
5013	Release binding	Binding released
5100	Stop process	Process stopped
5101	Connect To DHCP	DHCP connected
5102	Lost DHCP connection	DHCP connection lost

RuckOS Version 3.1

The following is the revision history of alarm and event from RuckOS version 3.0 to version 3.1.

New Alarm

Table 19. New Alarm

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

Table 19. New Alarm

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

Deprecated Alarm

Table 20. Deprecated Alarm

Alarm Code	Alarm
1008	cfgUpdFailed
1902	unknownRealmAccounting
1909	apAcctRespWhileInvalidConfig

Renamed Alarm

Table 21. Renamed Alarm Type

Alarm Code	Alarm Type	Renamed To
701	No LS Responses	No LS responses
721	No LS Responses	No LS responses
1623	App Server Down	App server down
1624	App Server Inactive	App server inactive
1627	Association Down	Association down
1636	Outbound Routing Failure	Outbound routing failure

Table 21. Renamed Alarm Type

Alarm Code	Alarm Type	Renamed To
1637	Did Allocation Failure	Did allocation failure
1960	CGF Server Not Configured	CGF server not configured
1242	TTG Session Critical Threshold	TTG session critical threshold
1243	TTG Session License Exhausted	TTG session license exhausted
1302	Rate Limit for TOR surpassed	Rate limit for TOR surpassed
1911	Unauthorized CoA/DM message dropped	Unauthorized COA/DM message dropped

New Event

Table 22. New Event

Event Code	Event
223	remediationSuccess
224	remediationFailure
325	cableModemUp
520	dpProcessRestart
626	dpSgreGWFailOver
627	dpSetUpTunnel
860	clusterCfgBackupStart
861	clusterCfgBackupSuccess
862	clusterCfgBackupFailed
863	clusterCfgRestoreSuccess
864	clusterCfgRestoreSuccess
926	ipmiREVotage
927	ipmiREThempBB
928	ipmiREThempFP
929	ipmiREThempIOH
930	ipmiREThempMemP
931	ipmiREThempPS
932	ipmiREThempP

Table 22. New Event

Event Code	Event
933	ipmiREThempHSBP
934	ipmiREFan
935	ipmiREPower
936	ipmiRECurrent
937	ipmiREFanStatus
938	ipmiREPsStatus
939	ipmiREDrvStatus
953	cpuThresholdBackToNormal
954	memoryThresholdBackToNormal
955	diskUsageThresholdBackToNormal
1401	diaInitilizeErr
1402	diaInitialization
1403	diaPeerTransportFailure
1404	diaCERError
1405	diaCERSuccess
1406	diaInvalidVer
1407	diaPeerAddError
1408	diaPeerAddSuccess
1409	diaPeerRemoveSuccess
1410	diaRealmEntryErr
1411	diaFailOverToAltPeer
1412	diaFailbackToPeer
1414	diaCEAUnknownPeer
1415	diaNoCommonApp
1550	staSucessfulAuthentication
1551	staAuthFailedTransDown
1552	staAuthFailedFailureResp
1553	staAuthFailedDecodeFailure

Table 22. New Event

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

Modified Event Severity

Table 23. Modification of Event Severity

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

Renamed Event

Table 24. Renamed Event

Event Code	Event Name	Renamed To
181	Ssid-spoofing rogue AP	SSID-spoofing rogue AP
209	Client Roaming	Client roaming
211	3rd Party Client Join	3rd party client join
212	3rd Party Client Inactivity Timeout	3rd party client inactivity timeout
213	3rd Party Client Authorization	3rd party client authorization
214	3rd Party Client Authorization Failure	3rd party client authorization failure
215	3rd Party Client Session Expiration	3rd party client session expiration
216	3rd Party Client Roaming	3rd party client roaming
217	3rd Party Client Session Logout	3rd party client session logout
220	Client Grace Period	Client grace period
308	AP channel updated because Dynamic Frequency Selection (DFS) detected a radar event	AP channel updated because dynamic frequency selection (DFS) detected a radar event
317	AP Brownout	AP brownout
323	AP capacity Reached	AP capacity reached
405	eMAP downlink connected to MAP	EMAP downlink connected to MAP
406	eMAP downlink disconnected from MAP	EMAP downlink disconnected from MAP
407	eMAP uplink connected to MAP	EMAP uplink connected to MAP
408	eMAP uplink disconnected from MAP	EMAP uplink disconnected from MAP
422	Mesh state updated to MAP No Channel	Mesh state updated to MAP no channel
424	Mesh state update to RAP No Channel	Mesh state update to RAP no channel
515	Data plane physical Interface Up	Data plane physical interface up

Table 24. Renamed Event

Event Code	Event Name	Renamed To
615	DP SoftgreGW Unreachable	DP softGRE GW unreachable
616	DP Softgre Keep Alive Timeout	DP softGRE keep alive timeout
617	DP SoftgreGW Inact	DP softGRE GW inactive
618	DP DhcpRelay No Resp	DP DHCPRelay no response
619	DP DhcpRelay FailOver	DP DHCPRelay failOver
620	DP SoftGRE New Tunnel	DP softGRE new tunnel
621	DP SoftGRE Del Tunnel	DP softGRE del tunnel
622	DP SoftGRE Keepalive Recovery	DP softGRE keepalive recovery
623	DP DhcpRelay Resp Recovery	DP DHCPRelay response recovery
624	DP SoftGRE GW Reachable	DP softGRE GW reachable
625	DP SoftGRE GW Active	DP softGRE GW active
701	No LS Responses	No LS responses
707	AP received Passive Calibration Request	AP received passive calibration request
708	AP received Passive Footfall Request	AP received passive footfall request
709	AP received Unrecognized Request	AP received unrecognized request
721	No LS Responses	No LS responses
725	SCG received Passive Request	SCG received passive request
727	SCG sent Controller Information report	SCG sent controller information report
728	SCG received Management Request	SCG received management request
729	SCG sent AP Info by Venue Report	SCG sent AP info by venue report
730	SCG sent Query Venues Report	SCG sent query venues report

Table 24. Renamed Event

Event Code	Event Name	Renamed To
731	SCG sent Associated Client Report	SCG sent associated client report
732	SCG forwarded Calibration Request to AP	SCG forwarded calibration request to AP
733	SCG forwarded Footfall Request to AP	SCG forwarded footfall request to AP
734	SCG received Unrecognized Request	SCG received unrecognized request
833	SSH Tunnel Switched	SSH tunnel switched
970	FTP Transfer	FTP transfer
971	FTP Transfer Error	FTP transfer error
980	File Upload	File upload
981	Email Sent Successfully	Email sent successfully
982	Email Sent Failed	Email sent failed
983	SMS Sent Successfully	SMS sent successfully
984	SMS Sent Failed	SMS sent failed
1012	Incorrect Flat File Configuration	Incorrect flat file configuration
1220	PDP update by Roaming succeeded	PDP update by roaming succeeded
1221	PDP update by Roaming failed	PDP update by roaming failed
1244	PDP Update Success COA	PDP update success COA
1245	PDP Update Fail COA	PDP update fail COA
1647	CoA Sent NAS	CoA sent NAS
1648	CoA NAK Received NAS	CoA NAK received NAS
1649	CoA Authorize Only Access Reject	CoA authorize only access reject
1650	CoA RWSG MWSG Notification Failure	CoA RWSG MWSG notification failure
1960	CGF Server Not Configured	CGF server not configured
2001	ZD AP Migrating	ZD AP migrating

Table 24. Renamed Event

Event Code	Event Name	Renamed To
2002	ZD AP Migrated	ZD AP migrated
2003	ZD AP Rejected	ZD AP rejected
2004	ZD AP Migration Failed	ZD AP migration failed
1302	Rate Limit for TOR surpassed	Rate limit for TOR surpassed
1911	Unauthorized CoA/DM message dropped	Unauthorized COA/DM message dropped
1238	DHCP Inform Received	DHCP inform received
1239	DHCP Dcln Received	DHCP decline received
1240	TTG Session Warning Threshold	TTG session warning threshold
1241	TTG Session Major Threshold	TTG session major threshold
1242	TTG Session Critical Threshold	TTG session critical threshold
1243	TTG Session License Exhausted	TTG session license exhausted
1620	Destination Available	Destination available
1623	App Server Down	App server down
1624	App Server Inactive	App server inactive
1625	App Server Active	App server active
1627	Association Down	Association down
1628	Association Up	Association up
1630	Send Auth Info Success	Send auth info success
1634	Insert Sub Data Success	Insert sub data success
1635	Insert Sub Data Failed	Insert sub data failed
1636	Outbound Routing Failure	Outbound routing failure
1637	Did Allocation Failure	Did allocation failure
1639	Restore Data Success	Restore data success
1640	Restore Data Failed	Restore data failed
1641	DM Received from AAA	DM received from AAA
1643	DM Sent to NAS	DM sent to NAS
1644	DM NACK Received from NAS	DM NACK received from NAS

Table 24. Renamed Event

Event Code	Event Name	Renamed To
1645	CoA Received from AAA	CoA received from AAA
1801	3rdParty AP Connected	3rd party AP connected

SmartZone Version 3.1.1

The following is the revision history of alarm and event from RuckOS version 3.1 to SmartZone version 3.1.1.

New Alarm

Table 25. New Alarm

Alarm Code	Alarm
661	ipsecTunnelDisAssociated
662	ipsecTunnelAssociateFailed

New Event

Table 26. New Event

Event Code	Event
326	cmResetByUser
327	cmResetFactoryByUser
660	ipsecTunnelAssociated
661	ipsecTunnelDisassociated
662	ipsecTunnelAssociateFailed
844	clusterInitiatedMovingAp
2101	radiusServerReachable
2102	radiusServerUnreachable
2121	ldapServerReachable
2122	ldapServerUnreachable
2141	adServerReachable
2142	adServerUnreachable

Table 26. New Event

Event Code	Event
2201	zoneInitiatedMovingAp
2501	nodeIPv6Added
2502	nodeIPv6Deleted

Re-added Event

Table 27. Re-added Event

Event Code	Event
101	apDiscoverySuccess

Renamed Event

Table 28. Renamed Event

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

SmartZone Version 3.1.2

The following is the revision history of alarm and event from SmartZone version 3.1.1 to 3.1.2.

New Alarm

Table 29. New Alarm

Alarm Code	Alarm
865	apCertificateExpire

New Event

Table 30. New Event

Event Code	Event
370	apUsbSoftwarePackageDownloaded
371	apUsbSoftwarePackageDownloadFailed
865	apCertificateExpire
866	apCertificateExpireClear

Alarm and Event Management

1

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

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

Event Categories

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

- Alarms: These are unexpected events indicating a condition that typically requires management attention
- Configuration Change Events: Configuration change events are events that inform of a configuration change effect on the device.
- Threshold Crossing Alerts: These are events that inform of a performance-related state variable that has exceeded a certain value. These events point to conditions that might require management attention to prevent network and service degradation.
- Logging Events: These are events that occur regularly and are expected to occur during the operation of a network, that indicate what is currently going on in the network. Some examples of these events include:
  - Activity on the network and service
  - Operator activity
  - System activity
  - Informational events – Any other kind of event.

- Debug and Informational events - All the debug and informational events pertaining to TTG modules like RADIUS proxy, HIP, CIP and AUT are not displayed on the Web Interface. This is because it reduces the performance of the system since it's large in numbers. Enabling display of these events on the Web Interface is possible through CLI but it is not recommended.

Event Attributes

An event always includes the following attributes:

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

Generation of Alarm and Event

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

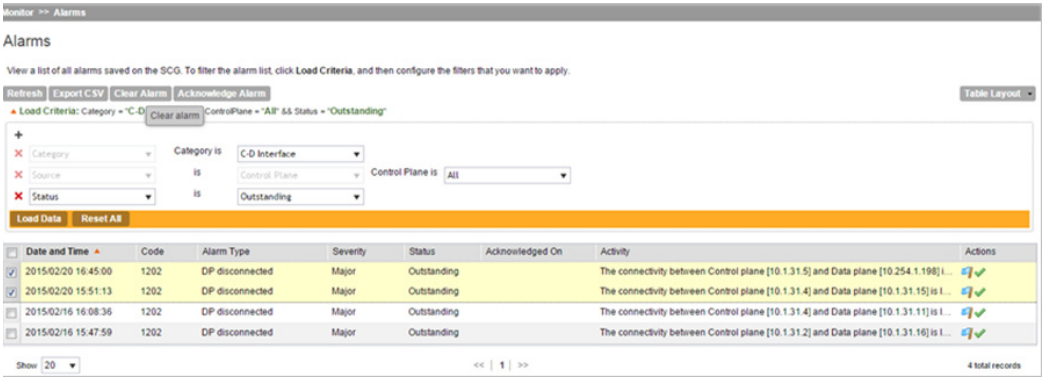
1 Alarm
   a An alarm is a persistent indication of a fault that clears only when the triggering condition had been resolved.
   b An alarm can be filtered in the controller Web Interface based on:
      - Alarm Category - Alarm classifications
      - Alarm Source: Source of the alarm
      - Alarm Status: Could either be outstanding or cleared
      - Acknowledge Time: The time when the alarm is acknowledged
      - Date and Time - Date and time when the alarm is acknowledged
      - Severity: Severity is classified as critical, major or minor
      - Status - Could either be cleared or outstanding
      - Type - Alarm type
   c Display of alarm information in the controller Web Interface is:
      - Date and Time
      - Code

- Alarm Type
- Severity
- Status
- Acknowledged on
- Activity
- Actions

d On an alarm generation, the controller web interface Monitor > Alarms 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.
- Filtering features based on the alarm attributes.
- You may clear an alarm or a set of alarms to let other administrators know that you have already resolved the issue. When you select a group of alarms, the Clear Alarms button is activated. Click this button. A text box appears where you can enter comments or notes about the resolved issue. Click Apply when done. To view the cleared alarms, select the cleared option.

Figure 1. Alarm



2 Event - On an event generation the:

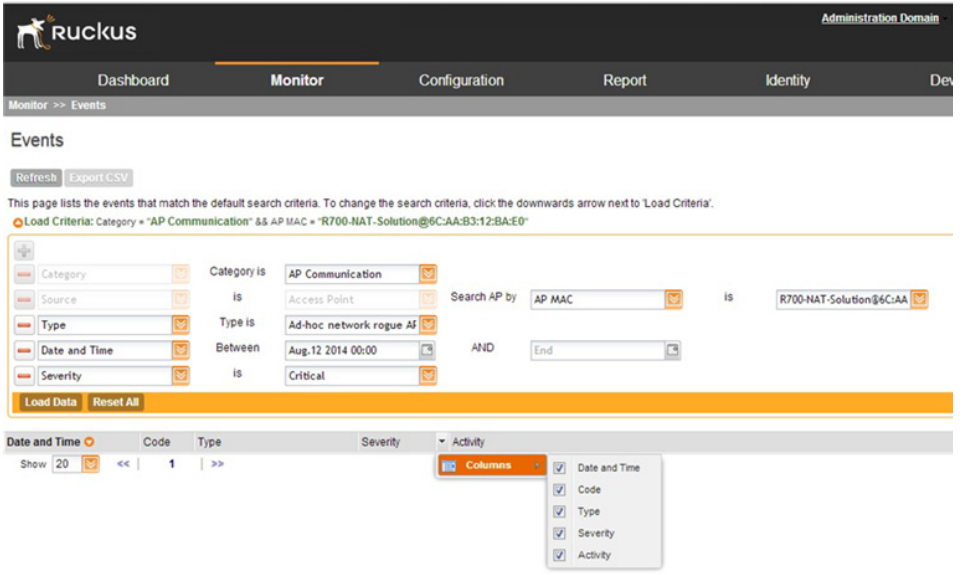
a The controller collects, receives, and maintains the raw events from the managed entities (control plane, data plane, access points, etc.). These raw events are kept in the database, and are automatically purged.

b The controller allows users to enable/disable certain event types from the managed entities.

- 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 web interface provides event log window as seen in Figure 2 for users to visualize and analyze the events. Users are able to perform various operations on the events, such as filtration, aggregation and counting.

Figure 2. Event



NOTE: Refer to Alarm Types and Events Types for the list of alarm and event that the SCG and vSZ-H generates.

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

NOTE: Refer to Administrator Guide for Viewing of Alarms and Events.

Alarm Types

2

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

In this chapter:

- Accounting Alarms
- AP Communication Alarms
- AP LBS Alarms
- AP State Change Alarms
- Authentication Alarms
- Control and Data Plane Interface Alarms
- Cluster Alarms
- Data Plane Alarms
- GA Interface Alarms
- Gn/S2a Interface Alarms
- GR Interface Alarms
- IPMI Alarms
- Licensing Alarms
- PMIPv6 Alarms
- Session Alarms
- STA Interface Alarms
- System Alarms
- Threshold Alarms
- Tunnel Alarms - Access Point

Accounting Alarms

The following are the alarms related to accounting.

- Accounting server not reachable
- Accounting failover to secondary
- Accounting fallback to primary
- AP accounting message mandatory parameter missing
- AP accounting message decode failed
- AP account message drop while no accounting start message
- Unauthorized CoA/DM message dropped

Accounting server not reachable

Table 31. 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”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the accounting server cannot be reached.
Recommended Actions	Manual intervention is required. Check the web interface for the connection to the AAA interface. Also, check if the RADIUS server can reach the AAA server interface.

Accounting failover to secondary

NOTE: This alarm is not applicable for vSZ-H.

Table 32. Accounting failover to secondary alarm

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

Accounting fallback to primary

NOTE: This alarm is not applicable for vSZ-H.

Table 33. Accounting fallback to primary alarm

Alarm	Accounting fallback to primary
Alarm Type	accFallbackToPrimary
Alarm Code	1654
Severity	Major
Aggregation Policy	An alarm is raised for every event from the event code 1654. A single event triggers a single alarm.

Table 33. Accounting fallback to primary 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”
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the automatic fallback is enabled. The accounting failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.
Recommended Actions	No action is required.

AP accounting message mandatory parameter missing

NOTE: This alarm is not applicable for vSZ-H.

Table 34. AP accounting message mandatory parameter missing alarm

Alarm	AP accounting message mandatory parameter missing
Alarm Type	apAcctMsgMandatoryPrmMissing
Alarm Code	1901
Severity	Critical
Aggregation Policy	From the event code 1901 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=”12”,“wlanId”=1, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, “realm”=”wlan.3gppnetwork.org","SCGMgmtIp"="2.2.2.2", “ueMacAddr”=”aa:bb:cc:gg:hh:ii”,“ueImsi”=”12345”, “ueMsisdn”=”98787”
Displayed on the web interface	[{srcProcess}] Mandatory attribute missing in Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}], with username [{ueImsi}@{realm}]

Table 34. AP accounting message mandatory parameter missing alarm

Description	This alarm is triggered when the controller fails to the find the mandatory parameter in the RADIUS accounting message received from the AP. This mandatory parameter is required for generating the WAN-CDR.
Recommended Action	Download the RADIUS log file from the web interface to check the error cause.

AP accounting message decode failed

NOTE: This alarm is not applicable for vSZ-H.

Table 35. AP accounting message decode failed alarm

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

AP account message drop while no accounting start message

NOTE: This alarm is not applicable for vSZ-H.

Table 36. AP account message drop while no accounting start message alarm

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

Unauthorized CoA/DM message dropped

NOTE: This alarm is not applicable for vSZ-H.

Table 37. Unauthorized CoA/DM message dropped alarm

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

NOTE: Refer to Accounting Events.

AP Communication Alarms

The following are the alarms related to access point communications.

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

AP rejected

Table 38. 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	controller name [{wsgIP}] rejected AP [{apName&&apMac}] because of [{reason}]
Description	This alarm is triggered when the AP is rejected.
Recommended Actions	Check if the number of licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses.

AP configuration update failed

Table 39. AP configuration update failed alarm

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

AP swap model mismatched

Table 40. 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.

Table 40. AP swap model mismatched alarm

Recommended Actions	If the model is incorrect delete and rejoin the AP.

AP pre-provision model mismatched

Table 41. 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.
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”, “configModel”=”xxx.xxx.xxx.xxx”. “model”=”xxx.xxx.xxx.xxx”
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from per-provision configuration model [{configModel}]
Description	This alarm is triggered when the AP model differs from the pre-provision configuration model.
Recommended Actions	If the model is incorrect delete the AP for the AP to rejoin to get the proper AP configuration.

AP firmware update failed

Table 42. 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"

Table 42. AP firmware update failed alarm

Displayed on the web interface	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}].
Description	This alarm is triggered when the AP fails to update its firmware details.
Recommended Actions	Retrieve the AP support text. Reboot the AP and trigger another configuration change for upgrading the AP. If it fails revert to the previous zone firmware.

AP WLAN oversubscribed

Table 43. AP WLAN oversubscribed alarm

Alarm	AP WLAN oversubscribed
Alarm Type	apWlanOversubscribed
Alarm Code	1081
Severity	Major
Aggregation Policy	From the event code 114 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	AP [{apName&&apMac}] does not have enough capacity to deploy all wlans. Only maximum wlan number of the AP can be deployed
Description	This alarm is triggered when the AP exceeds the maximum capacity for deploying all WLANs.
Recommended Actions	Any of the following are the recommended actions. • Create a new WLAN group with WLANs. Ensure that it is not more than the AP's WLAN capacity. Apply the new WLAN group to either the AP or the AP's AP Group. • Find the WLAN group used by the AP and reduce the number of WLAN

AP join zone failed

NOTE: This alarm is not applicable for vSZ-H.

Table 44. AP join zone failed alarm

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

NOTE: Refer to AP Communication Events.

AP LBS Alarms

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

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

No LS responses

Table 45. No LS responses alarm

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

LS authentication failure

Table 46. 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”=““

Table 46. LS authentication failure alarm

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

AP failed to connect to LS

Table 47. AP failed to connect to LS alarm

Alarm	AP failed to connect to LS
Alarm Type	apLBSConnectFailed
Alarm Code	704
Severity	Major
Aggregation Policy	From the event code 704 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 703.
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx“, “url”=““,”port”=““
Displayed on the SmartZone web interface	AP [{apName&&apMac}] connection failed to LS: url=[{url}], port=[{port}]
Description	This alarm is triggered when the AP fails to connect to the location based service.
Recommended Actions	This alarm is triggered either when the location server is unreachable or the network connection is unstable or the Domain Named System (DNS) configuration is incorrect. It is recommended to check all the three possible errors.

NOTE: Refer to AP LBS Events.

AP State Change Alarms

The following are the alarms related to access point state changes.

- AP rebooted by system
- AP disconnected
- AP deleted
- AP cable modem interface down

AP rebooted by system

Table 48. AP rebooted by system alarm

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

AP disconnected

Table 49. AP disconnected alarm

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

AP deleted

Table 50. AP deleted alarm

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

AP cable modem interface down

Table 51. 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 is rebooted.
Recommended Actions	Check cable modem. Try rebooting the cable modem.

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

Authentication server not reachable

Table 52. 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” "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}].
Description	This alarm is triggered when the authentication fails since the primary or secondary servers are not reachable.
Recommended Actions	Manual intervention is required. Check the web interface for the interface from the controller to AAA server. Also check if the AAA server can be reached from the RADIUS server. Ensure that the AAA server is UP.

Authentication failed over to secondary

Table 53. 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” "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]a
Description	This alarm is triggered when the secondary RADIUS server is available after the primary server becomes zombie or dead.
Recommended Actions	No operator action is required.

Authentication fallback to primary

Table 54. 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” "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when automatic fallback is enabled. Consequently, the authentication failover to the secondary server occurs and the revival timer for the primary server expires, and the requests falls back to the primary server.
Recommended Actions	No action is required.

NOTE: Refer to Authentication Events.

Control and Data Plane Interface Alarms

NOTE: This section is not applicable for vSZ-H.

The following alarm is related to control and data plane.

- DP disconnected

DP disconnected

Table 55. DP disconnected alarm

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

NOTE: Refer to Control and Data Plane Interface.

Cluster Alarms

The 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
- Configuration backup failed
- Configuration restore failed
- AP Certificate Expired

New node failed to join

Table 56. 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”

Table 56. New node failed to join alarm

Displayed on the web interface	New node [{nodeMac}] ([{nodeName}]) failed to join cluster [{clusterName}]
Description	This alarm is triggered when a node fails to join a cluster session. The web interface displays the error message.
Recommended Actions	When the operation fails, the user can run the *join process*. If it continues to fail, please send the complete log files (stored in the path - */opt/ ruckuswireless/controller/log/system)* for analysis to Ruckus support. 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 57. 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.

Table 57. Node removal failed alarm

Recommended Actions	In general, this alarm should rarely occur. If it occurs, restore to the previous backup file and please send the log files (stored in the path - */opt/ ruckuswireless/controller/log/system)* for analysis to Ruckus support.

Node out of service

Table 58. Node out of service alarm

Alarm	Node out of service
Alarm Type	nodeOutOfService
Alarm Code	803
Severity	Critical
Aggregation Policy	From the event code 806 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 835.
Attribute	“clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service
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 59. 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”

Table 59. Cluster in maintenance state alarm

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 (stored in the path - */opt/ ruckuswireless/controller/log/system)* to Ruckus support for analysis.

Cluster backup failed

Table 60. 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 failing or in case of Python script errors, please collect the complete log files (stored in the path - */opt/ ruckuswireless/controller/log/system)* to Ruckus support for analysis. Possible causes: • Insufficient disk space. • Communication between nodes may be broken. • Errors due to the underlying Python script.

Cluster restore failed

Table 61. 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	If the backup restore continues failing, please send the complete log files to Ruckus support. Download the log file by logging to the controller system. Navigate to Administration > Application Status & Logs. 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 62. 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"

Table 62. Cluster upgrade failed alarm

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 log file by logging to the controller system. Navigate to Administration > Application Status & Logs. Possible causes: • Insufficient disk space • Communication between nodes might be broken. • Errors due to the underlying Python script.

Cluster application stopped

Table 63. 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 64. 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}] down.
Description	This alarm is triggered when the network interface of a node is down.
Recommended Actions	Check if the network cables of both the physical interfaces are broken. Alternatively, check if the physical interfaces for this bond interface 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 65. 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"

Table 65. Node physical interface down alarm

Displayed on the web interface	Physical network interface [{networkInterface||ifName}] on node [{nodeName}] 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 66. 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 67. Cluster node shut down alarm

Alarm	Cluster node shut down
Alarm Type	nodeShutdown
Alarm Code	813
Severity	Major
Aggregation Policy	From the event code 828 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 826.
Attribute	"nodeName"="xxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Node [{nodeName}] has been shut down
Description	This alarm is triggered when the node shutdowns.
Recommended Actions	This usually occurs due to a user action. Please send the 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 68. 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%.

Table 68. Disk usage exceed threshold alarm

Recommended Actions	It is recommended that the user moves the backup files to the FTP server and deletes the moved backup files.

Cluster out of service

Table 69. Cluster out of service alarm

Alarm	Cluster out of service
Alarm Type	clusterOutOfService
Alarm Code	843
Severity	Critical
Aggregation Policy	From the event code 843 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 808.
Attribute	"clusterName"="xx"
Displayed on the web interface	Cluster [{clusterName}] is out of service.
Description	This alarm is triggered when the cluster service fails.
Recommended Actions	It is recommended that the operator/user checks the out of service node to locate the reason.

Configuration backup failed

Table 70. Configuration backup failed alarm

Alarm	Configuration backup failed
Alarm Type	clusterCfgBackupFailed
Alarm Code	862
Severity	Major
Aggregation Policy	From the event code 862 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 861.
Attribute	"clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] configuration backup failed.

Table 70. Configuration backup failed alarm

Description	This alarm is triggered when the configuration backup fails.
Recommended Actions	Download the web log file from the web interface to check for errors.

Configuration restore failed

Table 71. Configuration restore failed alarm

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

AP Certificate Expired

Table 72. 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.

Data Plane Alarms

The following are the alarms related to data plane.

- Data plane configuration update failed
- Data plane disconnected
- Data plane physical interface down
- Data plane rebooted
- Data plane packet pool is under low water mark
- Data plane packet pool is under critical low water mark
- Data plane core dead
- Data plane process restarted

Data plane configuration update failed

Table 73. 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	“dpMac”=”xx:xx:xx:xx:xx:xx”, “configID”=” 123456781234567”
Displayed on the web interface	Data plane [{dpName||dpMac}] failed to update to configuration [{configID}].
Description	This alarm is triggered when the data plane configuration update fails since it was unable to transfer the configuration update from the control plane to the data plane.
Recommended Actions	Check the data plane configuration and the CPU utilization of the control plane. The possible cause could be of the server being busy at that particular moment. Check to see if the event is persistent.

Data plane disconnected

Table 74. 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	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] disconnected from {produce.short.name} [{cpName||wsgIP}]
Description	This alarm is triggered when the data plane gets disconnected from the controller since it fails to update its status to the control plane.
Recommended Actions	Check if the communicator is still alive and if the cluster interface is working.

Data plane physical interface down

Table 75. 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”, “dpMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName||dpMac}] 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 75. 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 rebooted

Table 76. Data plane rebooted alarm

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

Data plane packet pool is under low water mark

Table 77. Data plane packet pool is under low water mark alarm

Alarm	Data plane packet pool is under low water mark
Alarm Type	dpPktPoolLow
Alarm Code	516
Severity	Major
Aggregation Policy	From the event code 516 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 518.
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName||dpMac}] is under low-water mark.

Table 77. Data plane packet pool is under low water mark alarm

Description	This alarm is triggered when the data core packet pool is below the water mark level.
Recommended Actions	The operator needs to check for network looping.

Data plane packet pool is under critical low water mark

Table 78. Data plane's packet pool is under critical low water mark alarm

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

Data plane core dead

Table 79. Data plane core dead alarm

Alarm	Data plane core dead
Alarm Type	dpCoreDead
Alarm Code	519
Severity	Critical
Aggregation Policy	From the event code 519 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpMac="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName||dpMac}] has dead data core.

Table 79. Data plane core dead alarm

Description	This alarm is triggered when one or multiple data core packet pool is lost /dead.
Recommended Actions	No action required.

Data plane process restarted

Table 80. Data plane process restarted alarm

Alarm	Data plane process restarted
Alarm Type	dpProcessRestart
Alarm Code	520
Severity	Major
Aggregation Policy	From the event code 519 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpMac="xx:xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	[{processName}] on data plane [{dpMac}] is restarted.
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.

NOTE: Refer to Data Plane Events.

GA Interface Alarms

NOTE: This section is not applicable for vSZ-H.

The following are the alarms related to GA interface.

- Connection to CGF failed
- CDR transfer failed
- CDR generation failed

Connection to CGF failed

Table 81. Connection to CGF failed alarm

Alarm	Connection to CGF failed
Alarm Type	cnxnToCgfFailed
Alarm Code	1610
Severity	Major
Aggregation Policy	From the event code 1610 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 1613.
Attribute	“mvnoId”=”2”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”cip”, “realm”=”NA”, “radSrvrIp”=”7.7.7.7”, "cgfSrvrIp"="40.40.40.40", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Connection with CGF [{cgfSrvrIp}] from RADServerIP [{radSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the channel interface processor (CIP) or GPRS tunneling protocol prime (GTPP) stack detects a connection loss to the charging gateway function (CGF server.
Recommended Actions	Manual intervention is required. Refer to GA Interface Events code 1613. The attribute cgfSrvIp should match.

CDR transfer failed

Table 82. CDR transfer failed alarm

Alarm	CDR transfer failed
Alarm Type	cdrTxfrFailed
Alarm Code	1614
Severity	Major
Aggregation Policy	From the event code 1614 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=”2”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”cip”, “realm”=”wlan.3gppnetwork.org", “radSrvrIp”=”7.7.7.7”, "cgfSrvrIp"="40.40.40.40", "CGF Serv Intf"="2.2.2.2",“cause”=”<reason for failure>”
Displayed on the web interface	CDR transfer failed from RAD Server [{radSrvrIp}] to CGF [{cgfSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the call detail record transfer over Gn' fails.
Recommended Actions	Manual intervention is required. Check the web interface for the home location register (HLR) configuration and also if the HLR can be reached from the controller.

CDR generation failed

Table 83. CDR generation failed alarm

Alarm	CDR generation failed
Alarm Type	cdrGenerationFailed
Alarm Code	1615
Severity	Major
Aggregation Policy	From the event code 1615 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=”2”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”cip”, “realm”=”wlan.3gppnetwork.org", “radSrvrIp”=”7.7.7.7”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Failed to generate CDR by RAD Server [{radSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the controller is unable to format or generate certain CDRs.
Recommended Actions	Manual intervention is required. Download the CIP process log file to check the cause of the error.

NOTE: Refer to GA Interface Events.

Gn/S2a Interface Alarms

NOTE: This section is not applicable for vSZ-H.

The following are the alarms related to Gn/S2a interface.

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

GGSN restarted

Table 84. GGSN restarted alarms

Alarm	GGSN restarted
Alarm Type	ggsnRestarted
Alarm Code	1210
Severity	Major
Aggregation Policy	From the event code 1210 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=”12”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”sm”, “realm”=”NA”, “gtpcIp”=”5.5.5.5”, "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2",
Displayed on the web interface	GGSN [{ggsnIp}] connected to {produce.short.name} [{SCGMgmtIp}] (GTPC-IP [{gtpcIp}]) is restarted.

Table 84. GGSN restarted alarms

Description	This alarm is triggered when the GTP control plane (GTP-C) receives a new recovery value.
Recommended Actions	Refer to the log file for Gateway GPRS Support Node (GGSN) restart.

GGSN not reachable

Table 85. GGSN not reachable alarms

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

GGSN not resolved

Table 86. GGSN not resolved alarm

Alarm	GGSN not resolved
Alarm Type	ggsnNotResolved
Alarm Code	1215
Severity	Major
Aggregation Policy	From the event code 1215 an alarm is raised for every event. A single event triggers a single alarm.

Table 86. GGSN not resolved alarm

Attribute	“mvnoId”=”12”,“wlanId”=”1”, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, “realm”=”wlan.3gppnetwork.org", “gtpcIp”=”5.5.5.5”, "apn"="ruckuswireless.com", "SCGMgmtIp"="2.2.2.2", “ueMacAddr”=”aa:bb:cc:gg:hh:ii”, “ueImsi”=”12345”, “ueMsisdn”=”98787”,
Displayed on the web interface	Failed to resolve GGSN from APN [{apn}] for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]
Description	This alarm is triggered when the access point name (APN) fails at GGSN.
Recommended Actions	Manual intervention is required. Correct the DNS configuration in the controller web interface.

PDNGW could not be resolved

Table 87. PDNGW could not be resolved alarm

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

PDNGW version not supported

Table 88. PDNGW version not supported alarm

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

Associated PDNGW down

Table 89. Associated PDNGW down alarm

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

Table 89. Associated PDNGW down alarm

Recommended Actions	Check the interface from the controller to PDN GW in the web interface to ensure it is reachable.

Create session response failed

Table 90. Create session response failed alarm

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

Decode failed

Table 91. Decode failed alarm

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

Modify bearer response failed

Table 92. Modify bearer response failed alarm

Alarm	Modify bearer response failed
Alarm Type	modifyBearerResponseFailed
Alarm Code	1956
Severity	Major
Aggregation Policy	From the event code 1956 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “gtpcIp”=”5.5.5.5” “pgwIp”=”1.1.1.1” "SCGMgmtIp"="2.2.2.2" “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “ueImsi”=”12345” “ueMsisdn”=”98787” “apn”=”ruckus.com” “cause”=”<reason for failure>”

Table 92. Modify bearer response failed alarm

Displayed on the web interface	[{srcProcess}] Modify Bearer Response from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	This alarm is reported when the modify bearer response from PDN GW fails as per the specified cause.
Recommended Actions	Download the SM log to check the cause of the error.

Delete session response failed

Table 93. Delete session response failed alarm

Alarm	Delete session response failed
Alarm Type	deleteSessionResponseFailed
Alarm Code	1957
Severity	Major
Aggregation Policy	From the event code 1957 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “gtpcIp”=”5.5.5.5” “pgwIp”=”1.1.1.1” "SCGMgmtIp"="2.2.2.2" “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “ueImsi”=”12345” “ueMsisdn”=”98787” “apn”=”ruckus.com” “cause”=”<reason for failure>”
Displayed on the web interface	[{srcProcess}] Delete Session response from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	Delete session response from PDN GW fails due to the specified cause.
Recommended Actions	Download the SM log to check the cause of the error.

Delete bearer request failed

Table 94. Delete bearer request failed alarm

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

Update bearer request failed

Table 95. Update bearer request failed alarm

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

Table 95. Update bearer request failed alarm

Recommended Actions	Download the SM log to check the cause of the error.

CGF server not configured

Table 96. CGF server not configured alarm

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

NOTE: Refer to Gn/S2a Interface Events.

GR Interface Alarms

NOTE: This section is not applicable for vSZ-H.

The following are the alarms related to GR interface.

- Destination not reachable
- App server down
- App server inactive
- Association establishment failed
- Association down
- Outbound routing failure
- Did allocation failure

Destination not reachable

Table 97. Destination not reachable alarm

Alarm	Destination not reachable
Alarm Type	destNotReacheable
Alarm Code	1618
Severity	Critical
Aggregation Policy	From the event code 1618 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1620.
Attribute	“mvnoId”=”2”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”hip”,“pointCode”=”1.1.1”
Displayed on the web interface	Remote Point Code [{pointCode}] is unavailable
Description	This alarm is triggered when the point code is unreachable due to a pause indicator.
Recommended Actions	Manual intervention is required.

App server down

Table 98. App server down alarm

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

App server inactive

Table 99. App server inactive alarm

Alarm	App server inactive
Alarm Type	appServerInactive
Alarm Code	1624
Severity	Critical
Aggregation Policy	From the event code 1624 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1625.
Attribute	“mvnoId”=”2”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”hip”, “routingContext” =”1”, “pointCode”=”1.1.1”, “SSN” = “7”

Table 99. App server inactive alarm

Displayed on the web interface	Application Server Inactive, Routing Context [{routingContext}], Ipcal Point Code [{pointCode}], local SSN [{SSN}]
Description	This alarm is triggered when the local application server is inactive due to application service provider inactive (ASP_INACTIVE) or application service provider inactive acknowledgment (ASP_INACTIVE_ACK) from remote IP security protocol (IPSP) or signalling gateway (SG).
Recommended Actions	Manual intervention is required.

Association establishment failed

Table 100. Association establishment failed alarm

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

Association down

Table 101. Association down alarm

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

Outbound routing failure

Table 102. Outbound routing failure alarm

Alarm	Outbound routing failure
Alarm Type	outboundRoutingFailure
Alarm Code	1636
Severity	Critical
Aggregation Policy	From the event code 1636 an alarm is raised for every 10 events. Alarm is raised for 10 or more events or events occurring within a span of 60 seconds.
Attribute	“mvnoId”=”2”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”hip”, “operation”=”updateGprsLocationReq”, “hlrInstance”=” Operator_HLR”, “ueImsi ”=” 04844624203918”
Displayed on the web interface	Unable to route [{operation}] for IMSI [{ueImsi}] to HLR [{hlrInstance}]

Table 102. Outbound routing failure alarm

Description	This alarm is triggered when a transaction capabilities application part (TCAP) message is unable to route to its destination.
Recommended Actions	Manual intervention is required.

Did allocation failure

Table 103. Did allocation failure alarm

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

NOTE: Refer to Gr Interface Event.

IPMI Alarms

NOTE: This section is not applicable for vSZ-H.

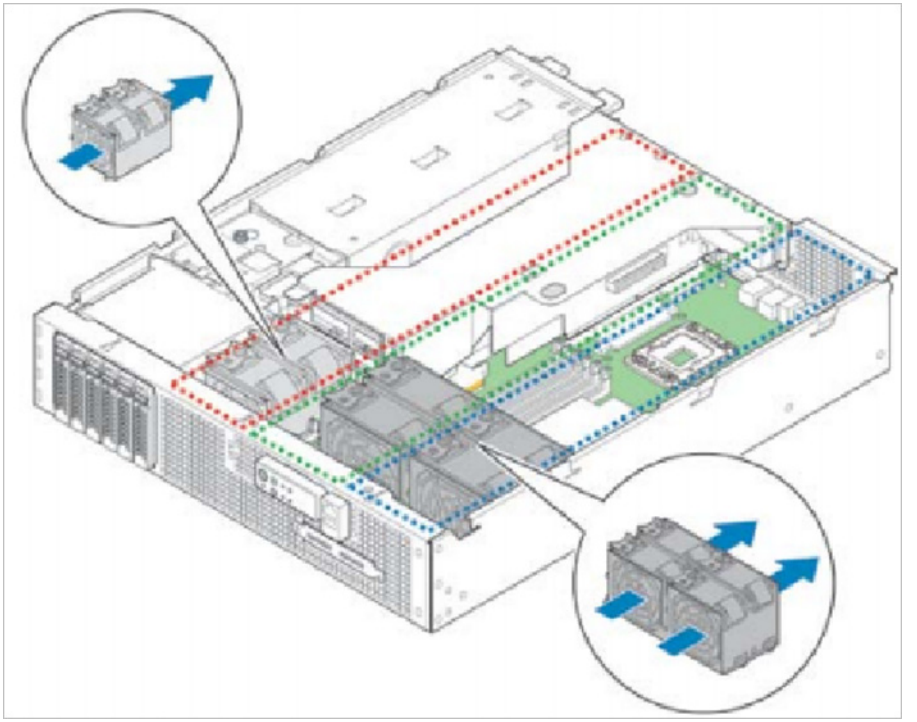
The following are the alarms related to IPMIs.

- ipmiVoltage
- ipmiThempBB
- ipmiThempFP
- ipmiThempIOH
- ipmiThempMemP
- ipmiThempPS
- ipmiThempP
- ipmiThempHSBP
- ipmiFan
- ipmiPower
- ipmiCurrent
- ipmiFanStatus
- ipmiPsStatus
- ipmiDrvStatus

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

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

Figure 3. Server Cooling Areas



ipmiVoltage

Table 104. ipmiVoltage alarm

Alarm	ipmiVoltage
Alarm Type	ipmiVotage
Alarm Code	901
Severity	Major
Aggregation Policy	From the event code 901 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 926.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard voltage [{status}] on control plane [{nodeMac}]

Table 104. ipmiVoltage alarm

Description	This alarm is triggered due to under/over voltage on the control plane. Baseboard threshold temperatures are: • Critical high - 66^0 C • Non critical high - 61^0 C • Non critical low - 10^0 C • Critical low - 5^0 C
Recommended Actions	Replace the power supply cord. If it does not work, the motherboard needs replacement.

ipmiThempBB

Table 105. 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.

ipmiThempFP

Table 106. ipmiThempFP alarm

Alarm	ipmiThempFP
Alarm Type	ipmiThempFP
Alarm Code	903
Severity	Major
Aggregation Policy	From the event code 903 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 928.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered due to increase/decrease of the front panel temperature status of the control plane. Front panel threshold temperatures are in the range of 5^0 Celsius to 44^0 Celsius. The default threshold is 44^0C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiThempIOH

Table 107. ipmiThempIOH alarm

Alarm	ipmiThempIOH
Alarm Type	ipmiThempIOH
Alarm Code	904
Severity	Major
Aggregation Policy	From the event code 904 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 929.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Chipset temperature [{status}] on control plane [{nodeMac}]

Table 107. ipmiThempIOH alarm

Description	This alarm is triggered when the chip set temperature status on the control plane increases/decreases. IOH thermal margin threshold temperatures are in the range of -20^0 Celsius to 5^0 Celsius. The default threshold is 5^0C.
Recommended Actions	Check the fan module. Decrease the ambient temperature if the fan module is working.

ipmiThempMemP

Table 108. ipmiThempMemP alarm

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

ipmiThempPS

Table 109. ipmiThempPS alarm

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

ipmiThempP

Table 110. ipmiThempP alarm

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

ipmiThempHSBP

Table 111. ipmiThempHSBP alarm

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

Table 111. ipmiThempHSBP alarm

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

ipmiFan

Table 112. ipmiFan alarm

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

ipmiPower

Table 113. ipmiPower alarm

Alarm	ipmiPower
Alarm Type	ipmiPower
Alarm Code	910
Severity	Major
Aggregation Policy	From the event code 910 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 935.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}]

Table 113. ipmiPower alarm

Description	This alarm is triggered when the control plane's power supply status is shown as a low/high input.
Recommended Actions	Replace the power supply cord.

ipmiCurrent

Table 114. ipmiCurrent alarm

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

ipmiFanStatus

Table 115. 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"

Table 115. ipmiFanStatus alarm

Displayed on the web interface	Fan module [{id}] [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's fan module shows the status as not working.
Recommended Actions	Replace the fan module.

ipmiPsStatus

Table 116. ipmiPsStatus alarm

Alarm	ipmiPsStatus
Alarm Type	ipmiPsStatus
Alarm Code	913
Severity	Major
Aggregation Policy	From the event code 913 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 938.
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's power supply status is shown as a low/high input.
Recommended Actions	Check the power supply cord. If the problem persists, replace the power supply cord.

ipmiDrvStatus

Table 117. ipmiDrvStatus alarm

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

NOTE: Refer to IPMI Events.

Licensing Alarms

NOTE: This section is not applicable for vSZ-H.

The following are the alarms related to licensing.

- TTG session critical threshold
- TTG session license exhausted

TTG session critical threshold

Table 118. TTG session critical threshold alarm

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

TTG session license exhausted

Table 119. TTG session license exhausted alarm

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

NOTE: Refer to Licensing Interface Events.

PMIPv6 Alarms

NOTE: This section is not applicable for vSZ-H.

The following are the alarms related to PMIPv6.

- Config update failed
- LMA ICMP unreachable
- LMA failed over
- DHCP connection lost

Config update failed

Table 120. Config update failed alarm

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

LMA ICMP unreachable

Table 121. LMA ICMP unreachable alarm

Alarm	LMA ICMP unreachable
Alarm Type	lmaIcmpUnreachable
Alarm Code	5006
Severity	Major
Aggregation Policy	From the event code 5006 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 5005.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, "SCGMgmtIp"="2.2.2.2", "lmaIp"="1.1.1.1"
Displayed on the web interface	[{lmaIp}] ICMP unreachable on {produce.short.name} [{SCGMgmtIp}].
Description	This alarm is triggered when the PMIPv6 daemon cannot connect to the LMA server through the internet control message protocol (ICMP) packet.
Recommended Actions	Check the network connectivity between local mobility anchor (LMA) and data plane. Also check the LMA server status from the LMA connectivity page on the controller web interface.

LMA failed over

Table 122. LMA failed over alarm

Alarm	LMA failed over
Alarm Type	lmaFailOver
Alarm Code	5008
Severity	Major
Aggregation Policy	From the event code 5008 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac"="aa:bb:cc:dd:ee:ff”, "SCGMgmtIp"="2.2.2.2", “lmaIp”=”1.1.1.1”
Displayed on the web interface	[{lmaIp}] Failover on {produce.short.name} [{ctrlBladeMac}]

Table 122. LMA failed over alarm

Description	This alarm is logged when the standby LMA transits to an active mode. This includes the control plane identifier of the newly active LMA.
Recommended Actions	Check the LMA server status from the LMA connectivity page.

DHCP connection lost

NOTE: This alarm is not applicable for vSZ-H.

Table 123. DHCP connection lost alarm

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

NOTE: Refer to PMIPv6 Events.

Session Alarms

NOTE: This section is not applicable for vSZ-H.

The following is the alarms related to session.

- Binding failed

Binding failed

Table 124. Binding failed alarm

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

NOTE: Refer to Session Events.

STA Interface Alarms

NOTE: This section is not applicable for vSZ-H.

The following is the alarms related to STA interface.

- STA authentication failed transport down
- STA authentication failed failure responsef
- STA authentication failed decode failure
- STA re-authorization failed
- STA response timer expired
- Retransmission exhausted

STA authentication failed transport down

Table 125. STA authentication failed transport down alarm

Alarm	STA authentication failed transport down
Alarm Type	staAuthFailedTransDown
Alarm Code	1551
Severity	Major
Aggregation Policy	From the event code 1551 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”=”STA”, “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with AAA [{aaaSrvrIp}] failed as Transport is down
Description	This alarm is triggered when the authentication procedure with external AAA server failed and the STA interface transport is down.
Recommended Actions	The operator should check the interfaces from the controller to 3rd generation partnership project (3GPP) AAA server. Alternatively, check if the 3GPP AAA server is down.

STA authentication failed failure response

Table 126. STA authentication failed failure response alarm

Alarm	STA authentication failed failure response
Alarm Type	staAuthFailedFailureResp
Alarm Code	1552
Severity	Major
Aggregation Policy	From the event code 1552 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”=”STA”, “realm”= “wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345” “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”, “resultCode” =”Decode Failed”
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with 3GPP AAA [{aaaSrvrIp}] failed, DEA with failure code [{resultCode}]
Description	This alarm is triggered when the authentication procedure with external AAA server failed. The diameter EAP answer (DEA) received from 3GPP AAA server failed with result code.
Recommended Actions	The operator should check the STA application logs. This could be a temporary failure response from the 3GPP AAA server.

STA authentication failed decode failure

Table 127. STA authentication failed decode failure alarm

Alarm	STA authentication failed decode failure
Alarm Type	staAuthFailedDecodeFailure
Alarm Code	1553
Severity	Major
Aggregation Policy	From the event code 1553 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”=”STA” “realm”=”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”, “resultCode” =”Decode Failed”
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with 3GPP AAA [{aaaSrvrIp}] failed, DEA decode failed
Description	This alarm is triggered when the authentication procedure with external AAA server failed. The DEA received from 3GPP AAA server failed with result code.
Recommended Actions	The operator should check the STA application logs. This could be a temporary failure response from the 3GPP AAA server.

STA re-authorization failed

Table 128. STA re-authorization failed alarm

Alarm	STA re-authorization failed
Alarm Type	staReAuthFailed
Alarm Code	1558
Severity	Major
Aggregation Policy	From the event code 1558 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”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”

Table 128. STA re-authorization failed alarm

Displayed on the web interface	[{srcProcess}] Re-Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] failed
Description	This alarm is triggered when the 3GPP AAA server initiated reauthorization re-auth request (RAR) fails.
Recommended Actions	The operator should check the STA application logs. Also check the version of 3GPP specifications supported by 3GPP AAA server.

STA response timer expired

Table 129. STA response timer expired alarm

Alarm	STA response timer expired
Alarm Type	staResponseTimerExpired
Alarm Code	1559
Severity	Major
Aggregation Policy	From the event code 1559 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”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Tx timer expired no response received from 3GPP AAA [{aaaSrvrIp}]
Description	This alarm is triggered when the 3GPP AAA server initiated reauthorization RAR fails.
Recommended Actions	The operator should check the interfaces from the controller to 3GPP AAA server. Alternatively, check if the 3GPP AAA server is down.

Retransmission exhausted

Table 130. Retransmission exhausted alarm

Alarm	Retransmission exhausted
Alarm Type	retransmitExausted
Alarm Code	1560
Severity	Major
Aggregation Policy	From the event code 1560 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 1550.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Retransmission for [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] to 3GPP AAA [{aaaSrvrIp}] failed. Retransmission of messages to 3GPP
Description	This alarm is triggered when the 3GPP AAA server initiated reauthorization RAR fails.
Recommended Actions	The operator should check the interfaces from the controller to 3GPP AAA server. Alternatively, check if the 3GPP AAA server is down.

NOTE: Refer to STA Interface Events.

System Alarms

The following are the alarms with the system log severity.

NOTE: {produce.short.name} refers to SCG or vSZ-H

- No LS responses
- LS authentication failure
- {produce.short.name} failed to connect to LS
- Process restart
- Service unavailable
- Keepalive failure
- Resource unavailable
- HIP failed over
- Diameter initialization error
- Diameter peer transport failure
- Diameter CER error
- Diameter peer add error
- Diameter peer remove successful
- Diameter realm entry error
- Diameter fail over to alternate peer
- Diameter fail back to peer
- Diameter CEA unknown peer
- Diameter no common application
- Process initiated
- PMIPv6 unavailable
- Memory allocation failed

No LS responses

Table 131. No LS responses alarm

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

LS authentication failure

Table 132. LS authentication failure alarm

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

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

Table 133. {produce.short.name} failed to connect to LS alarm

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

Process restart

Table 134. Process restart alarm

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

Table 134. Process restart alarm

Recommended Actions	Download the process log file from the controller web interface to understand the cause of the error.

Service unavailable

Table 135. Service unavailable alarm

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

Keepalive failure

Table 136. Keepalive failure alarm

Alarm	Keepalive failure
Alarm Type	keepAliveFailure
Alarm Code	1003
Severity	Major
Aggregation Policy	From the event code 1003 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, "SCGMgmtIp"="2.2.2.2"

Table 136. Keepalive failure alarm

Displayed on the web interface	[{srcProcess}] on {produce.short.name} [{SCGMgmtIp}] restarted [{processName}] process
Description	This alarm is triggered when the *mon/nc* restarts the process due to a keep alive failure.
Recommended Actions	Download the process log file from the controller web interface to locate the cause of the error.

Resource unavailable

Table 137. Resource unavailable alarm

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

HIP failed over

NOTE: This alarm is not applicable for vSZ-H.

Table 138. HIP failed over alarm

Alarm	HIP failed over
Alarm Type	hipFailover
Alarm Code	1016

Table 138. HIP failed over alarm

Severity	Major
Aggregation Policy	Alarm is raised for every event from event code 1016. A single event triggers a single alarm.
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	[{srcProcess}] Node transitioned to Active on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is 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.

Diameter initialization error

NOTE: This alarm is not applicable for vSZ-H.

Table 139. Diameter initialization error alarm

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

Diameter peer transport failure

NOTE: This alarm is not applicable for vSZ-H.

Table 140. Diameter peer transport failure alarm

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

Diameter CER error

NOTE: This alarm is not applicable for vSZ-H.

Table 141. Diameter CER error alarm

Alarm	Diameter CER error
Alarm Type	diaCERError
Alarm Code	1404
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.

Table 141. Diameter CER error alarm

Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerIp” = “3.3.3.3” “peerName” = “OCS1” “peerRealmName” = “organization.com” “desc” = ”Failed to read from peer socket”
Displayed on the web interface	[{srcProcess}] Failed to decode CER from Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the diameter stack fails to decode the capabilities exchange request (CER) received from peer.
Recommended Actions	Check if the transport is up for the peer. Peer application may not be running.

Diameter peer add error

NOTE: This alarm is not applicable for vSZ-H.

Table 142. Diameter peer add error alarm

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

Diameter peer remove successful

NOTE: This alarm is not applicable for vSZ-H.

Table 143. Diameter peer remove successful alarm

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

Diameter realm entry error

NOTE: This alarm is not applicable for vSZ-H.

Table 144. Diameter realm entry error alarm

Alarm	Diameter realm entry error
Alarm Type	diaRealmEntryErr
Alarm Code	1410
Severity	Major
Aggregation Policy	A single event triggers a single alarm.

Table 144. Diameter realm entry error alarm

Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerRealmName” = “organization.com” “peerName” = “OCS1” “desc” = ”Failed to add route for Realm”
Displayed on the web interface	[{srcProcess}] Failed to add route for Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered due to realm route entry add error. This may arise when the realm entry exists and another realm entry is added. Creating two diameter services with same realm name causes this problem.
Recommended Actions	Ensure that peer supports the application for the given realm and is up and running.

Diameter fail over to alternate peer

NOTE: This alarm is not applicable for vSZ-H.

Table 145. Diameter fail over to alternate peer alarm

Alarm	Diameter fail over to alternate peer
Alarm Type	diaFailOverToAltPeer
Alarm Code	1411
Severity	Major
Aggregation Policy	A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerName”=ÖCS1 “peerRealmName” = “organization.com” “altPeerName” = ”OCS2” “altPeerRealmName” = “india.internal.net”“desc” = “Fwd to alt peer”
Displayed on the web interface	[{srcProcess}] Fwd from Peer [{peerName}] to AltPeer [{altPeerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered due to retransmission to an alternate peer.

Table 145. Diameter fail over to alternate peer alarm

Recommended Actions	Verify that the failover has occurred to the alternate peer and the request is processed by the same peer. Also verify if the primary peer is having a problem or is not reachable.

Diameter fail back to peer

NOTE: This alarm is not applicable for vSZ-H.

Table 146. Diameter fail back to peer alarm

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

Diameter CEA unknown peer

NOTE: This alarm is not applicable for vSZ-H.

Table 147. Diameter CEA unknown peer alarm

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

Diameter no common application

NOTE: This alarm is not applicable for vSZ-H.

Table 148. Diameter no common application alarm

Alarm	Diameter no common application
Alarm Type	diaNoCommonApp
Alarm Code	1415
Severity	Critical
Aggregation Policy	A single event triggers a single alarm.

Table 148. Diameter no common application alarm

Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerName”=ÖCS1 “peerRealmName” = “organization.com”“desc” = “No common App with peer”
Displayed on the web interface	[{srcProcess}] No common App with Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This alarm is triggered when the common application is not with the peer.
Recommended Actions	Verify that the peer is in the remote service configuration and is sending the capability negotiation message that the authentication application identifier is not compliant to the remote service.

Process initiated

NOTE: This alarm is not applicable for vSZ-H.

Table 149. Process initiated alarm

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

PMIPv6 unavailable

NOTE: This alarm is not applicable for vSZ-H.

Table 150. PMIPv6 unavailable alarm

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

Memory allocation failed

NOTE: This alarm is not applicable for vSZ-H.

Table 151. Memory allocation failed alarm

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

NOTE: Refer to System Alarms.

Threshold Alarms

The 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 152. CPU threshold exceeded alarm

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

Memory threshold exceeded

Table 153. Memory threshold exceeded alarm

Alarm	Memory threshold exceeded
Alarm Type	memoryThresholdExceeded
Alarm Code	951
Severity	Critical
Aggregation Policy	From the event code 951 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 954.
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the memory usage exceeds the threshold limit. The memory threshold value is 85% for SCG and 90% for vSZ-H.
Recommended Actions	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 154. 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 154. 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 155. License threshold exceeded alarm

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

Rate limit for TOR surpassed

Table 156. Rate limit for TOR surpassed alarm

Alarm	Rate limit for TOR surpassed
Alarm Type	rateLimitTORSurpassed
Alarm Code	1302
Severity	Critical
Aggregation Policy	From the event code 1302 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1301.
Attributef	"mvnoId"=”12”, “wlanId”=”1”, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”radiusd”, “UserName”=abc@xyz.com, “realm”=”wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1” “AAAServerType”=”Auth/Acct”, “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “MOR”=1000, “THRESHOLD”=”500”, “TOR”=”501”
Displayed on the web interface	Maximum Outstanding Requests(MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This 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 157. 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 7003 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 7001.

Table 157. The number of users exceeded its limit

Attribute	No attributes for this alarm.
Displayed on the web interface	The number of devices exceeded its 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 158. 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 7004 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 7002.
Attribute	No attributes for this alarm.
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 to Threshold Events.

Tunnel Alarms - Access Point

The 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 159. AP softGRE gateway not reachable alarm

Alarm	AP softGRE gateway not reachable
Alarm Type	apSoftGREGatewayNotReachable
Alarm Code	614
Severity	Critical
Aggregation Policy	From the event code 614 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 613.
Attribute	“apMac”=”xx:xx:xx:xx:xx:xx”, “softGREGatewayList”=”xxx.xxx.xxx.xxx”
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}]
Description	The AP fails to connect to the soft-GRE gateway.
Recommended Actions	Check the primary and secondary soft-GRE gateway.

AP is disconnected from secure gateway

Table 160. 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"

Table 160. AP is disconnected from secure gateway alarm

Displayed on the web interface	AP [{apName&&apMac}] is disconnected from secure gateway [{ipsecGWAddress}].
Description	This alarm is triggered when the AP is disconnected from secure gateway.
Recommended Actions	No action required.

AP secure gateway association failure

Table 161. 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 to Tunnel Events - Access Point (AP).

Events Types

3

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

- 3rd Party Access Point Events
- Accounting Events
- AP Authentication Events
- AP Communication Events
- AP LBS Events
- AP Mesh Events
- AP State Change Events
- AP USB Events
- Authentication Events
- Authorization Events
- Control and Data Plane Interface
- Client Events
- Cluster Events
- Configuration Events
- Data Plane Events
- DHCP Events
- GA Interface Events
- Gn/S2a Interface Events
- Gr Interface Event
- IPMI Events
- Licensing Interface Events
- Location Delivery Events
- PMIPv6 Events
- Session Events
- STA Interface Events
- System Events
- Threshold Events
- Tunnel Events - Access Point (AP)
- Tunnel Events - Data Plane

3rd Party Access Point Events

NOTE: This event is not applicable for vSZ-H.

Following events are related to 3rd party access points.

- 3rd party AP connected

3rd party AP connected

Table 162. 3rdparty AP connected event

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

Accounting Events

NOTE: This event is not applicable for vSZ-H.

Following events are related to accounting.

- Accounting session started
- Accounting session start failed
- Accounting session disabled
- Accounting session stopped successfully
- Accounting session stopped failed
- Accounting session interim failed
- Accounting server not reachable
- Accounting failed over to secondary
- Accounting fallback to primary
- AP accounting message mandatory parameter missing
- Unknown realm
- AP accounting message decode failed
- AP accounting retransmission message dropped
- AP accounting response while invalid config
- AP account message drop while no accounting start message
- Unauthorized COA/DM message dropped

Accounting session started

NOTE: This event is not applicable for vSZ-H.

Table 163. Accounting session started event

Event	Accounting session started
Event Type	accSessStarted
Event Code	1232
Severity	Debug

Table 163. Accounting session started event

Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	Accounting session started for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the accounting session starts. It is applicable for tunnel termination gateway (TTG) or packet data gateway (PDG) provided accounting process is enabled for the session.

Accounting session start failed

NOTE: This event is not applicable for vSZ-H.

Table 164. Accounting session start failed event

Event	Accounting session start failed
Event Type	accSessStartFailed
Event Code	1233
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="<reason for failure>"
Displayed on the web interface	Accounting session could not be started for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because [{cause}]
Description	This event occurs when the accounting session fails to start. This event is applicable for TTG/PDG provided accounting process is enabled for the session.

Accounting session disabled

NOTE: This event is not applicable for vSZ-H.

Table 165. Accounting session disabled event

Event	Accounting session disabled
Event Type	accSessDisabled
Event Code	1234
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	Accounting session disabled for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the accounting is disabled for the session.

Accounting session stopped successfully

NOTE: This event is not applicable for vSZ-H.

Table 166. Accounting session stopped successfully event

Event	Accounting session stopped successfully
Event Type	accSessStopSucc
Event Code	1246
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	Accounting session stopped for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}].

Table 166. Accounting session stopped successfully event

Description	This event occurs when the accounting session stops. This event is applicable for TTG/PDG provided accounting process is enabled for the session.

Accounting session stopped failed

NOTE: This event is not applicable for vSZ-H.

Table 167. Accounting session stopped failed event

Event	Accounting session stopped failed
Event Type	accSessStopFail
Event Code	1247
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="<reason for failure>"
Displayed on the web interface	No Response received or Error Stopping accounting session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because [{cause}]. Accounting session locally cleared
Description	This event occurs when the controller does not receive a response or receives an error response for accounting stop. This event is applicable for TTG/PDG provided accounting process is enabled for the session.

Accounting session interim failed

NOTE: This event is not applicable for vSZ-H.

Table 168. Accounting session interim failed event

Event	Accounting session interim failed
Event Type	accSessInterimFail
Event Code	1248
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="<reason for failure>"
Displayed on the web interface	No Response received or Error response received for accounting interim request for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because [{cause}]
Description	This event occurs when the controller receives an error response for the accounting interim request. This event is applicable for TTG/PDG provided accounting process is enabled for the session.

Accounting server not reachable

NOTE: This event is not applicable for vSZ-H.

Table 169. Accounting server not reachable event

Event	Accounting server not reachable
Event Type	accSrvrNotReachable
Event Code	1602
Severity	Major
Attribute	"mvnoId"=”12”, "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="radiusd", "realm"="wlan.3gppnetwork.org", "radProxyIp"="7.7.7.7", "accSrvrIp"="30.30.30.30", "SCGMgmtIp"="2.2.2.2"

Table 169. Accounting server not reachable event

Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the controller is unable to connect to either the primary or secondary accounting server.

Accounting failed over to secondary

NOTE: This event is not applicable for vSZ-H.

Table 170. Accounting failed over to secondary event

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

Accounting fallback to primary

NOTE: This event is not applicable for vSZ-H.

Table 171. Accounting fallback to primary event

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

AP accounting message mandatory parameter missing

NOTE: This event is not applicable for vSZ-H.

Table 172. AP accounting message mandatory parameter missing event

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

Unknown realm

NOTE: This event is not applicable for vSZ-H.

Table 173. Unknown realm event

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

AP accounting message decode failed

NOTE: This event is not applicable for vSZ-H.

Table 174. AP accounting message decode failed event

Event	AP accounting message decode failed
Event Type	apAcctMsgDecodeFailed
Event Code	1904
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, "SCGMgmtIp"="2.2.2.2", “apIpAddress”=”10.1.4.11”
Displayed on the web interface	[{srcProcess}] Malformed Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}], with username [{userName}]

Table 174. AP accounting message decode failed event

Description	This event occurs when the AP accounting message decode fails due to receipt of a malformed packet.

AP accounting retransmission message dropped

NOTE: This event is not applicable for vSZ-H.

Table 175. AP accounting retransmission message dropped event

Event	AP accounting retransmission message dropped
Event Type	apAcctRetransmittedMsgDropped
Event Code	1908
Severity	Debug
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut", "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii", “ueImsi"="12345", "ueMsisdn"="98787" “apIpAddress”=”10.1.4.11”
Displayed on the web interface	[{srcProcess}] Accounting message from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}] dropped, {produce.short.name} did not receive Accounting start message.
Description	This event occurs when the retransmitted accounting message is dropped while the call detail record is generated and the transfer to charging gateway function server is in progress.

AP accounting response while invalid config

Table 176. 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", "SCGMgmtIp"="2.2.2.2",“apIpAddress”=”10.1.4.11”
Displayed on the web interface	[{srcProcess}] sending dummy response for Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}], with username [{userName}]. Configuration is incorrect in {produce.short.name} to forward received message nor to generate CDR
Description	This event occurs when the controller sends a dummy response to the AP accounting message since the configuration in the controller is incorrect. The event could either occur when forwarding received messages or when generating call detail records.

AP account message drop while no accounting start message

Table 177. 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","SCGMgmtIp"="2.2.2.2",“apIpAddress” =”10.1.4.11”
Displayed on the web interface	[{srcProcess}] Dropped Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SCGMgmtIp}], with username [{userName}]. Accounting session timer expired, stop or interim message not received, as Account Start not received from NAS/ AP
Description	This event occurs when the accounting session timer expires. Stop or interim messages are not received since the account start is not received from the network access server (NAS) or access point (AP).

Unauthorized COA/DM message dropped

Table 178. 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”,"SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] Dropped CoA/DM Packet received from AAA [{radSrvrIp}] on {produce.short.name} [{SCGMgmtIp}], with username [{userName}]. Received message from unauthorized AAA
Description	This event occurs when the controller receives a change of authorization (CoA) or dynamic multipoint (DM) messages from an unauthorized AAA server.

NOTE: Refer to Accounting Alarms.

AP Authentication Events

Following are the events related to authentication.

- Radius server reachable
- Radius server unreachable
- LDAP server reachable
- LDAP server unreachable
- AD server reachable
- AD server unreachable

Radius server reachable

Table 179. 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"="3.1.0.0.344","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 180. Radius server unreachable event

Event	Radius server unreachable
Event Type	radiusServerUnreachable
Event Code	2102
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.1.0.0.344","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""

Table 180. Radius server unreachable event

Displayed on the web interface	AP [{apName&&apMac}] is unable to reach radius server [{ip}].
Description	This event occurs when the AP is unable to reach the radius server.

LDAP server reachable

Table 181. 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"="3.1.0.0.344","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 182. LDAP server unreachable event

Event	LDAP server unreachable
Event Type	ldapServerUnreachable
Event Code	2122
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.1.0.0.344","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach LDAP server [{ip}].
Description	This event occurs when AP is unable to reach the LDAP server.

AD server reachable

Table 183. 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"="3.1.0.0.344","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is able to reach AD server [{ip}].
Description	This event occurs when AP is able to reach the active directory successfully.

AD server unreachable

Table 184. AD server unreachable event

Event	AD server unreachable
Event Type	adServerUnreachable
Event Code	2142
Severity	Informational
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.1.0.0.344","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].
Description	This event occurs when AP is unable able to reach the active directory.

AP Communication Events

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

- AP discovery succeeded
- AP managed
- AP rejected
- AP firmware updated
- AP firmware update failed
- Updating AP firmware
- Updating AP configuration
- AP configuration updated
- AP configuration update failed
- AP pre-provision model mismatched
- AP swap model mismatched
- AP WLAN oversubscribed
- AP join zone failed
- 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 185. AP discovery succeeded event

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

AP managed

Table 186. 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 187. 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 188. 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"="3.0.0.0.340", "fromVersion"="3.0.0.0.341"
Displayed on the web interface	AP [{apName&&apMac}] updated its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP successfully updates the firmware details to the controller.

AP firmware update failed

Table 189. 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"="3.0.0.0.340", "fromVersion"="3.0.0.0.341"
Displayed on the web interface	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP fails to update the firmware details to the controller.
Auto Clearance	This event triggers the alarm 107, which is auto cleared by the event code 106.

Updating AP firmware

Table 190. 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"="3.0.0.0.340", "fromVersion"="3.0.0.0.341"
Displayed on the web interface	AP [{apName&&apMac}] firmware is being updated from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP successfully adds the new firmware details to the controller.

Updating AP configuration

Table 191. Updating AP configuration event

Event	Updating AP configuration
Event Type	apConfApplying
Event Code	109
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx", "configID"="23456781234"
Displayed on the web interface	AP [{apName&&apMac}] is being updated to new configuration ID [{configID}]
Description	This event occurs when the AP successfully updates new configuration details to the controller.

AP configuration updated

Table 192. AP configuration updated event

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

AP configuration update failed

Table 193. AP configuration update failed event

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

AP pre-provision model mismatched

Table 194. AP pre-provision model mismatched event

Event	AP pre-provision model mismatched
Event Type	apModelDiffWithPreProvConfig
Event Code	112
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx", "configModel"="ZF7962" "model"="ZF7343"
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 195. 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"="ZF7343"
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 196. AP WLAN oversubscribed event

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

AP join zone failed

Table 197. AP join zone failed event

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

AP illegal to change country code

Table 198. 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.

Rogue AP

Table 199. 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 200. SSID-spoofing rogue AP event

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

MAC-spoofing rogue AP

Table 201. 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 rogue [{rogueMac}] with [{ssid}] is detected by [{apName&&apMac}].
Description	This event occurs when the AP detects a rogue AP having the same basic service set identifier (BSSID).

Same-network rogue AP

Table 202. 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 rogue [{rogueMac}] with [{ssid}] is detected by [{apName&&apMac}].
Description	This event occurs when the AP detects a rogue AP which has the same network.

Ad-hoc network device

Table 203. Ad-hoc network rogue device event

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

Rogue AP disappeared

Table 204. 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 (LBS).

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

No LS responses

Table 205. No LS responses event

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

LS authentication failure

Table 206. LS authentication failure event

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

AP connected to LS

Table 207. 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 208. 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 209. AP started location service event

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

AP stopped location service

Table 210. AP stopped location service event

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

AP received passive calibration request

Table 211. 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}], duration=[{duration}], band=[{band}]
Description	This event occurs when the AP receives the passive calibration request.

AP received passive footfall request

Table 212. 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}], duration=[{duration}], band=[{band}]
Description	This event occurs when the AP receives the passive footfall request.

AP received unrecognized request

Table 213. AP received unrecognized request event

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

NOTE: Refer to AP LBS Alarms.

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 214. 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"

Table 214. EMAP downlink connected to MAP event

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 215. 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 216. 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 217. 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 218. 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 219. 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 219. MAP downlink connected event

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

MAP downlink connected to EMAP

Table 220. 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 EMAP.

MAP downlink disconnected from EMAP

Table 221. 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 EMAP disconnects from MAP.

RAP downlink connected to MAP

Table 222. RAP downlink connected to MAP event

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

MAP uplink connected to EMAP

Table 223. 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 224. 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 225. 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 226. 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 227. 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 228. Mesh state updated to MAP no channel event

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

Mesh state updated to RAP

Table 229. Mesh state updated to RAP event

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

Mesh state update to RAP no channel

Table 230. Mesh state update to RAP no channel event

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

MAP downlink connected to MAP

Table 231. 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 232. 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 233. 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 CLB limit reached
AP CLB 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 rebooted by user

Table 234. 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 a AP has to reboot.

AP rebooted by system

Table 235. 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 236. 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 237. 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 238. 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 239. 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"

Table 239. AP channel updated event

Displayed on the web interface	AP [{apName&&apMac}] detected interference on radio [{radio}] and has switched from channel [{fromChannel}] to channel [{toChannel}]
Description	This event occurs when the AP detects the radio interference and switches to another channel.

AP country code updated

Table 240. 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 241. AP channel updated because dynamic frequency selection (DFS) detected a radar event

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

AP change control plane

Table 242. 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 243. 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 244. AP deleted event

Event	AP deleted
Event Type	apDeleted (detected on the server)
Event Code	313
Severity	Major

Table 244. AP deleted event

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 245. AP heartbeat lost event

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

AP tagged as critical

Table 246. AP tagged as critical event

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

AP cable modem interface down

Table 247. 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 248. 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 249. 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"

Table 249. AP cable modem power-cycled by user event

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 250. 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 CLB limit reached

Table 251. AP CLB limit reached event

Event	AP CLB 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 CLB 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 CLB limit recovered

Table 252. AP CLB limit recovered event

Event	AP CLB 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 CLB 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 253. 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 254. AP capacity reached event

Event	AP capacity reached
Event Type	apCapacityReached
Event Code	323
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", “radio”:"",
Displayed on the web interface	AP [{{apName&&apMac}] radio [{radio}] stopped accepting clients because the client association threshold has been reached.
Description	This event occurs when an AP rejects a client due to the threshold limit reached by the client.

AP capacity recovered

Table 255. 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 256. 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 257. AP cable modem soft-rebooted by user event

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

AP cable modem set to factory default by user

Table 258. AP cable modem set to factory default by user event

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

NOTE: Refer to AP State Change Alarms.

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 259. AP USB software package downloaded event

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

AP USB software package download failed

Table 260. AP USB software package download failed event

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

Authentication Events

Following are the events related to authentication.

- Authentication server not reachable
- Unknown realm
- Authentication succeeded
- Authentication failed
- Pseudonym authentication succeeded
- Pseudonym authentication failed
- Fast re-authentication succeeded
- Fast re-authentication failed
- Authentication failed over to secondary
- Authentication fallback to primary

Authentication server not reachable

Table 261. 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.3gppnetwork.org" "radProxyIp"="7.7.7.7" "authSrvrIp"="20.20.20.20" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the authentication fails since the primary or secondary servers are not reachable.

Unknown realm

Table 262. Unknown realm event

Event	Unknown realm
Event Type	unknownRealm
Event Code	1603
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"="wlan.3gppnetwork.org"
Displayed on the web interface	Realm [{realm}] could not be resolved to a AAA server
Description	This event occurs when the authentication realm resolution fails.

Authentication succeeded

Table 263. Authentication succeeded event

Event	Authentication succeeded
Event Type	authSuccess
Event Code	1604
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS accept is sent back to the AP. This event applies only for TTG/PDG session. *Note:* The attribute *Permanent ID* is used for authentication.

Authentication failed

Table 264. Authentication failed event

Event	Authentication failed
Event Type	authFailed
Event Code	1605
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787", "cause"="<Cause of failure>" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Authentication failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back and the MS-ISDN is provided (if available). *Note*: The attribute *Permanent ID* is used for authentication.

Pseudonym authentication succeeded

NOTE: This event is not applicable for vSZ-H.

Table 265. Pseudonym authentication succeeded event

Event	Pseudonym authentication succeeded
Event Type	pseudonymAuthSuccess
Event Code	1606
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "authType"="EAP-SIM/AKA"

Table 265. Pseudonym authentication succeeded event

Displayed on the web interface	Pseudonym ID based authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS accept is sent back to the AP. This event is applicable when the controller acts as a host AAA server and is applicable only for TTG/PDG session. *Note*: The attribute *Pseudonym ID* is used for authentication.

Pseudonym authentication failed

NOTE: This event is not applicable for vSZ-H.

Table 266. Pseudonym authentication failed event

Event	Pseudonym authentication failed
Event Type	pseudonymAuthFailed
Event Code	1607
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1 "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="<Cause of failure>" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Pseudonym ID based authentication failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back for pseudonym authentication. This event is applicable when the controller acts as a host AAA server. The mobile subscriber integrated services digital network number (MS-ISDN) is provided (if available). *Note*: The attribute *Pseudonym ID* is used for authentication.

Fast re-authentication succeeded

NOTE: This event is not applicable for vSZ-H.

Table 267. Fast re-authentication succeeded event

Event	Fast re-authentication succeeded
Event Type	fastReauthSuccess
Event Code	1608
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Fast re-auth ID based authentication successful for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back to the AP. This event is applicable when the controller acts as a hosted AAA server for TTG/PDG session. *Note*: Attribute *FastReauth ID* is used for authentication.

Fast re-authentication failed

NOTE: This event is not applicable for vSZ-H.

Table 268. Fast re-authentication failed event

Event	Fast re-authentication failed
Event Type	fastReauthFailed
Event Code	1609
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"=" radiusd" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "cause"="<Cause of failure>" "authType"="EAP-SIM/AKA"
Displayed on the web interface	Fast re-auth ID based authentication failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]. Cause = [{cause}]. {produce.short.name} used is [{SCGMgmtIp}]
Description	This event occurs when the RADIUS reject is sent back for fast reauthentication. This event applies when the controller acts as a host AAA server. The MS-ISDN is provided (if available). *Note*: Attribute *FastReuathID* is used for reauthentication.

Authentication failed over to secondary

Table 269. 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” "SCGMgmtIp"="2.2.2.2"

Table 269. Authentication failed over to secondary event

Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the secondary authentication RADIUS server is available after the primary server becomes zombie or dead.

Authentication fallback to primary

Table 270. 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” "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the automatic fallback is enabled. The authentication failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.

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 271. DM received from AAA event

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

DM NACK sent to AAA

Table 272. DM NACK sent to AAA event

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

DM sent to NAS

Table 273. DM sent to NAS event

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

DM NACK received from NAS

Table 274. DM NACK received from NAS event

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

CoA received from AAA

Table 275. CoA received from AAA event

Event	CoA received from AAA
Event Type	coaRcvdAAA
Event Code	1645
Severity	Debug
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radius" "userName"="user name" "radSrvrIp"="7.7.7.7" "rmtRadSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA received by RAC [{radSrvrIp}] from AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control receives a change of authorization message from the AAA server.

CoA NACK sent to AAA

Table 276. 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" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control sends a change of authorization, not acknowledged to the AAA server.

CoA sent NAS

Table 277. 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” "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA requests proxied/forwarded to NAS(AP) [{nasIp}].
Description	This event occurs when the controller forwards/proxy of change of authorization to the NAS server.

CoA NAK received NAS

Table 278. 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” "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA NAK received from NAS(AP) for forwarded/proxied CoA [{radSrvrIp}]
Description	This event occurs when a change of authorization, not acknowledged is received from the NAS server.

CoA authorize only access reject

Table 279. 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" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787","rmtRadSrvrIp"="40.40.40.40 "
Displayed on the web interface	CoA Authorize Only unsuccessful for AAA Server [rmtRadSrvrIp] for UE [ueMacAddr]
Description	This event occurs when the change of authorization is rejected.

CoA RWSG MWSG notification failure

Table 280. 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" "SCGMgmtIp"="2.2.2.2" “apType” = “ “ueMacAddr”=”aa:bb:cc:gg:hh:ii”
Displayed on the web interface	Session Modify MWSG-RWSG Notification Failure/No response received
Description	This event occurs when the change of authorization in RADIUS /metro wireless service gateway notification fails.

Control and Data Plane Interface

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

- DP connected
- 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 281. DP connected event

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

DP disconnected

Table 282. DP disconnected event

Event	DP disconnected
Event Type	lostCnxnToDblade
Event Code	1202
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, “realm”=”NA”,“ctrlBladeIp”=”1.1.1.1”, "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	The connectivity between Control plane [{ctrlBladeIp}] and Data plane [{dataBladeIp}] is lost at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when either the transmission control protocol connection is lost or when the control plane is unable to complete the configuration procedure.
Auto Clearance	This event triggers the alarm 1202, which is auto cleared by the event code 1201.

Session updated at DP

Table 283. 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”, “srcProcess”=”aut”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “realm”=”realm sent by UE”, “ctrlBladeIp”=”1.1.1.1”, "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", “ueMacAddr”=”aa:bb:cc:gg:hh:ii”, “ueImsi”=”12345”, “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been updated at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session updates the request (C-D-SESS-UPD-REQ) successfully.

Session update at DP failed

Table 284. Session update at DP failed event

Event	Session update at DP failed
Event Type	sessUpdateErrAtDblade
Event Code	1206
Severity	Debug
Attribute	“mvnoId”=”12”, “wlanId”=”1”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, “zoneId”=”10”, “realm”=”realm sent by UE”, “ctrlBladeIp”=”1.1.1.1”, "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", “ueMacAddr”=”aa:bb:cc:gg:hh:ii”, “ueImsi”=”12345”, “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to update at Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session update request fails (C-D-SESS-UPD-REQ). This is either due to a request timeout or a failed response.

Session deleted at DP

Table 285. Session deleted at DP event

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

Table 285. Session deleted at DP event

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

Session delete at DP failed

Table 286. Session delete at DP failed event

Event	Session delete at DP failed
Event Type	sessDeleteErrAtDblade
Event Code	1208
Severity	Debug
Attribute	“mvnoId”=”12”, “wlanId”=”1”, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut”, “realm”=”realm sent by UE”, “ctrlBladeIp”=”1.1.1.1”, "dataBladeIp"="3.3.3.3", "SCGMgmtIp"="2.2.2.2", “ueMacAddr”=”aa:bb:cc:gg:hh:ii”, “ueImsi”=”12345”, “ueMsisdn”=”98787”
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to delete from Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the session delete request (C-D-SESS-DEL-REQ) results in a timeout or a failed response.

C2d configuration failed

Table 287. C2d configuration failed event

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

NOTE: Refer to Control and Data Plane Interface.

Client Events

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

- Client authentication failed
- Client joined
- Client failed to join
- Client disconnected
- Client connection timed out
- Client authorization successfully
- Client authorization failed
- Client session expired
- Client roaming
- Client logged out
- 3rd party client join
- 3rd party client inactivity timeout
- 3rd party client authorization
- 3rd party client authorization failure
- 3rd party client session expiration
- 3rd party client roaming
- 3rd party client session logout
- Client roaming disconnected
- Client blocked
- Client grace period
- Onboarding registration succeeded
- Onboarding registration failed
- Remediation succeeded
- Remediation failed
- Force DHCP disconnected

Client authentication failed

Table 288. Client authentication failed event

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

Client joined

Table 289. Client joined event

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

Client failed to join

Table 290. Client failed to join event

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

Client disconnected

Table 291. Client disconnected event

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

Client connection timed out

Table 292. Client connection timed out event

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

Client authorization successfully

Table 293. Client authorization successfully event

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

Client authorization failed

Table 294. Client authorization failed event

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

Client session expired

Table 295. 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 296. Client roaming event

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

Client logged out

Table 297. Client logged out event

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

3rd party client join

NOTE: This event is not applicable for vSZ-H.

Table 298. 3rd party client join event

Event	3rd party client join
Event Type	3rdPtyClientJoin
Event Code	211
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	3rd party client [{clientIP||clientMac}] joined Zone [{zoneName}] on DP [{dpName||dpMac}].
Description	This event occurs when a 3rd party client joins the AP zone session on the data plane.

3rd party client inactivity timeout

NOTE: This event is not applicable for vSZ-H.

Table 299. 3rd party client inactivity timeout event

Event	3rd party client inactivity timeout
Event Type	3rdPtyClientInactivityTimeout
Event Code	212
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	3rd party client [{clientIP||clientMac}] joined Zone [{zoneName}] on DP [{dpName||dpMac}].
Description	This event occurs when 3rd party client disconnects from an AP zone session on the data plane due to inactivity.

3rd party client authorization

NOTE: This event is not applicable for vSZ-H.

Table 300. 3rd party client authorization event

Event	3rd party client authorization
Event Type	3rdPtyClientAuthorization
Event Code	213
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	3rd Party client [{clientIP||clientMac}] of Zone [{zoneName}] on DP [{dpName||dpMac}] was authorized.
Description	This event occurs when 3rd party client on AP zone session is authorized.

3rd party client authorization failure

NOTE: This event is not applicable for vSZ-H.

Table 301. 3rd party client authorization failure event

Event	3rd party client authorization failure
Event Type	3rdPtyClientAuthorizationFailure
Event Code	214
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	3rd party client [{clientIP||clientMac}] of Zone [{zoneName}] on DP [{dpName||dpMac}] was not authorized.
Description	This event occurs when the 3rd party client on the AP zone session is not authorized.

3rd party client session expiration

NOTE: This event is not applicable for vSZ-H.

Table 302. 3rd party client session expiration event

Event	3rd party client session expiration
Event Type	3rdPtyClientSessionExpiration
Event Code	215
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	3rd party client [{clientIP||clientMac}] of Zone [{zoneName}] on DP [{dpName||dpMac}] exceeded the session time limit. Session terminated.
Description	This event occurs when the 3rd party client on the AP zone exceeds the session time limit, resulting in session termination.

3rd party client roaming

NOTE: This event is not applicable for vSZ-H.

Table 303. 3rd party client roaming event

Event	3rd party client roaming
Event Type	3rdPtyClientRoaming
Event Code	216
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	DataPlane [{dpName||dpMac}] detected 3rd party client [{clientIP||clientMac}] in Zone [{zoneName}] on DP [{dpName||fromDpMac}].
Description	This event occurs when the data plane detects a 3rd party client in the AP zone.

3rd party client session logout

NOTE: This event is not applicable for vSZ-H.

Table 304. 3rd party client session logout event

Event	3rd party client session logout
Event Type	3rdPtyClientSessionLogout
Event Code	217
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “clientIP”=”x.x.x.x”, “zoneUUID”=”xxxxxx”, “userId”=”uuid"
Displayed on the web interface	3rd party client [{clientIP||clientMac}] of Zone [{zoneName}] on DP [{dpName||dpMac}] occurred session logout.
Description	This event occurs when 3rd party client on AP zone data plane occurs. This results in a session logs out.

Client roaming disconnected

Table 305. 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.

Table 305. Client roaming disconnected event

Description	This event occurs when the client disconnects from the WLALN due to a smart roam policy.

Client blocked

Table 306. 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 307. Client grace period event

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

Onboarding registration succeeded

Table 308. 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 309. Onboarding registration failed event

Event	Onboarding registration failed
Event Type	onboardingRegistrationFailure
Event Code	222
Severity	Informational
Attribute	“apMac”=”xx:xx:xx:xx:xx:xx”, “clientMac”=”xx:xx:xx:xx:xx:xx”, “ssid”=”xxxxx”, “wlanId”=”xxxxx”, “userName”=”xxxxx”, “clientIP”=”x.x.x.x”, “userId”=”uuid",“apLocation”=”xxxx”, “groupName”=”xxxx”, “vlanId”=”xxxx”, “osType”=”xxxx”,“userAgent”=”xxxx”,“reason”=”xxxxx”
Displayed on the web interface	Client [{userName||clientIP||clientMac}] of WLAN [{ssid}] on AP [{apName&&apMac}] on boarding registration failed because of [{reason}].
Description	This event occurs when the client onboarding registration fails.

Remediation succeeded

Table 310. 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 311. 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 312. Force DHCP disconnected event

Event	Force DHCP disconnected
Event Type	forceDHCPDisconnect
Event Code	225
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”, “clientMac”=“xx:xx:xx:xx:xx:xx”, “ssid”=“xxxxx”, “bssid”=“”, “wlanId”=“xxxxx”, "tenantUUID"="xxxxx",“clientIP”=“x.x.x.x”,”apName”=“”,”vlanId”=, "radio"="", “encryption”=“”,
Displayed on the web interface	Client [{userName||IP||clientMac}] disconnected from WLAN [{ssid}] on AP [{apName&&apMac}] due to force-dhcp.
Description	This event occurs when the client disconnects by force from the dynamic host configuration protocol.

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	Resync NTP Time	Disk usage exceed threshold
Cluster out of service	Initiated moving APs in node to a new cluster	Configuration backup started
Configuration backup succeeded	Configuration backup failed	Configuration restore succeeded
Configuration restore failed	AP Certificate Expired	AP Certificate Updated
Node IPv6 address added	Node IPv6 address deleted	

Cluster created successfully

Table 313. 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”

Table 313. Cluster created successfully event

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 314. 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 315. 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 316. 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 317. 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 318. 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 319. Cluster in maintenance state event

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

Cluster back in service

Table 320. 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 321. Cluster backup completed event

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

Cluster backup failed

Table 322. Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810
Severity	Major
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason\:[{reason}].

Table 322. Cluster backup failed event

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 323. 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 324. 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 325. 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 326. 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 327. 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 328. 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 329. 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 330. 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 331. 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 332. 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 333. Node bond interface down event

Event	Node bond interface down
Event Type	nodeBondInterfaceDown
Event Code	821
Severity	Major
Attribute	“nodeMac”=” xx:xx:xx:xx:xx:xx”, “ifName”=”xxxx”
Displayed on the web interface	Network interface [{networkInterface||ifName}] on node [{nodeName}] is down.
Description	This event occurs when the network interface of a node is down.
Auto Clearance	This event triggers the alarm 809, which is auto cleared by the event code 822.

Node bond interface up

Table 334. 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 335. 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 336. 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 337. Node physical interface up event

Event	Node physical interface up
Event Type	nodePhyInterfaceUp
Event Code	825
Severity	Informational
Attribute	“nodeMac”=” xx:xx:xx:xx:xx:xx”, “ifName”=”xxxx”
Displayed on the web interface	Physical network interface [{networkInterface||ifName}] on node [{nodeName}] is up.
Description	This event occurs when the node’s physical interface is up.

Cluster node rebooted

Table 338. Cluster node rebooted event

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

NTP time synchronized

Table 339. NTP time synchronized event

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

Cluster node shutdown

Table 340. 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 341. 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 342. 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 343. 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 344. 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 345. Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834
Severity	Informational

Table 345. Cluster remove node started event

Attribute	"clusterName"=”xxx”, "nodeName" =”xxx”, "nodeMac"=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Start to remove node [{nodeName}] from cluster [{clusterName}]
Description	This event occurs when the node start is removed.

Node back in service

Table 346. 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'.

Resync NTP Time

Table 347. Resync NTP Time event

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

Disk usage exceed threshold

Table 348. Disk usage exceed threshold

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

Cluster out of service

Table 349. 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 350. 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.

Configuration backup started

Table 351. 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 352. 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 353. 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 succeeded.
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 354. Configuration restore succeeded event

Event	Configuration restore succeeded
Event Type	clusterCfgRestoreSuccess
Event Code	863
Severity	Informational
Attribute	"clusterName"="xxx"

Table 354. Configuration restore succeeded event

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 355. Configuration restore failed event

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

AP Certificate Expired

Table 356. 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 357. 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.

Node IPv6 address added

Table 358. 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 359. 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 the events related to configuration.

- Configuration updated
- Configuration update failed
- Configuration receive failed
- Incorrect flat file configuration

Configuration updated

Table 360. Configuration updated event

Event	Configuration updated
Event Type	cfgUpdSuccess
Event Code	1007
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" , "srcProcess"="cnr", "realm"="NA" "processName"="aut" "SCGMgmtIp"="x.x.x.x" "cause"="xx"
Displayed on the web interface	Configuration [{cause}] applied successfully in [{processName}] process at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the configuration notification receiver (CNR) process successfully applies the configuration to the modules.

Configuration update failed

Table 361. Configuration update failed event

Event	Configuration update failed
Event Type	cfgUpdFailed
Event Code	1008
Severity	Debug
Attribute	“ctrlBladeMac"="aa:bb:cc:dd:ee:ff" , "srcProcess"="cnr" "realm"="NA" "processName"="aut" "SCGMgmtIp"="x.x.x.x" "cause"="xx"
Displayed on the web interface	Failed to apply configuration [{cause}] in [{processName}] process at {produce.short.name} [{SCGMgmtIp}].

Table 361. Configuration update failed event

Description	This event occurs when the CNR receives an error or negative acknowledgment when applying the configuration settings to the module. Possible cause is that a particular process/module is down.

Configuration receive failed

Table 362. Configuration receive failed event

Event	Configuration receive failed
Event Type	cfgRcvFailed
Event Code	1009
Severity	Debug
Attribute	"ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”cnr” “realm”=”NA” "SCGMgmtIp"="x.x.x.x", “cause”=”xx”
Displayed on the web interface	Failed to fetch configuration [{cause}] by CNR in {produce.short.name} [{SCGMgmtIp}].
Description	This event occurs when the CNR receives an error or negative acknowledgment/improper/incomplete information from the configuration change notifier (CCN).
Auto Clearance	This event triggers the alarm 1009, which is auto cleared by the event code 1007.

Incorrect flat file configuration

Table 363. Incorrect flat file configuration event

Event	Incorrect flat file configuration
Event Type	incorrectFlatFileCfg
Event Code	1012
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut", "realm"="NA", "SCGMgmtIp"="xxxx", "cause"="xxx", "file"="xx"
Displayed on the web interface	[{srcProcess}] detected an configuration parameter is incorrectly configured in file [{file}] at {produce.short.name} [{SCGMgmtIp}].
Description	This event occurs when any flat file configuration parameter is not semantically or syntactically correct.

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 rebooted
- Data plane heartbeat lost
- Data plane IP address updated
- Data plane updated to a new control plane
- Data plane status update failed
- Data plane statistics update failed
- Data plane connected
- Data plane disconnected
- Data plane physical interface down
- Data plane physical interface up
- Data plane packet pool is under low water mark
- Data plane packet pool is under critical low water mark
- Data plane packet pool is above high water mark
- Data plane core dead
- Data plane process restarted

Data plane discovered

Table 364. Data plane discovered event

Event	Data plane discovered
Event Type	dpDiscoverySuccess (server side detect)
Event Code	501
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”

Table 364. Data plane discovered event

Displayed on the web interface	Data plane [{dpName||dpMac}] 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 365. Data plane discovery failed event

Event	Data plane discovery failed
Event Type	dpDiscoveryFail (detected on the server side)
Event Code	502
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 366. Data plane configuration updated event

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

Data plane configuration update failed

Table 367. Data plane configuration update failed event

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

Data plane rebooted

Table 368. Data plane rebooted event

Event	Data plane rebooted
Event Type	dpReboot (server side detect)
Event Code	506
Severity	Minor
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”,
Displayed on the web interface	Data plane [{dpName||dpMac}] rebooted
Description	This event occurs when the data plane is rebooted.

Data plane heartbeat lost

Table 369. Data plane heartbeat lost event

Event	Data plane heartbeat lost
Event Type	dpLostConnection (detected on the server side)
Event Code	507
Severity	Informational

Table 369. Data plane heartbeat lost event

Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”,
Displayed on the web interface	Data plane [{dpName||dpMac}] heartbeat lost.
Description	This event occurs when the data plane heartbeat lost.
Auto Clearance	This event triggers the alarm 502, which is auto cleared by the event code 512.

Data plane IP address updated

Table 370. Data plane IP address updated event

Event	Data plane IP address updated
Event Type	dpIPChanged
Event Code	508
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”,
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 371. 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	“dpMac”=”xx:xx:xx:xx:xx:xx”, “oldwsgIP”=”xxx.xxx.xxx.xxx”, “newwsgIP”=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 372. Data plane status update failed event

Event	Data plane status update failed
Event Type	dpUpdateStatusFailed
Event Code	510
Severity	Minor
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 373. Data plane statistics update failed event

Event	Data plane statistics update failed
Event Type	dpUpdateStatisticFailed
Event Code	511
Severity	Minor
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 374. Data plane connected event

Event	Data plane connected
Event Type	dpConnected
Event Code	512
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] connected to {produce.short.name} [{cpName||wsgIP}].
Description	This event occurs when the data plane connects to the controller.

Data plane disconnected

Table 375. Data plane disconnected event

Event	Data plane disconnected
Event Type	dpDisconnected
Event Code	513
Severity	Critical
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] disconnected from {produce.short.name} {cpName||wsgIP}].
Description	This event occurs when the data plane disconnects from the controller.
Auto Clearance	This event triggers the alarm 503, which is auto cleared by the event code 512.

Data plane physical interface down

Table 376. Data plane physical interface down event

Event	Data plane physical interface down
Event Type	dpPhyInterfaceDown
Event Code	514
Severity	Critical
Attribute	“portID”=”xx”, “dpMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName||dpMac}] 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 377. Data plane physical interface up event

Event	Data plane physical interface up
Event Type	dpPhyInterfaceUp
Event Code	515
Severity	Informational
Attribute	“portID”=”xx”, “dpMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName||dpMac}] 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 378. 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	Major
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName||dpMac}] 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 379. 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	Critical
Attribute	dpMac="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName||dpMac}] is under critical low-water mark.
Description	This event occurs when the data core packet pool reaches the critical water mark level.

Data plane packet pool is above high water mark

Table 380. 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	dpMac="xx:xx:xx:xx:xx:xx", "id"="x"
Displayed on the web interface	Pool [{id}] on data plane [{dpName||dpMac}] is above high-water mark
Description	This event occurs when the data core packet pool is higher than the water mark level.

Data plane core dead

Table 381. Data plane core dead event

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

Data plane process restarted

Table 382. Data plane process restarted event

Event	Data plane process restarted
Event Type	dpProcessRestart
Event Code	520
Severity	Major
Attribute	dpMac="xx:xx:xx:xx:xx:xx", processName="xxxx"
Displayed on the web interface	[{processName}] on data plane [{dpMac}] is restarted.
Description	This event occurs when a process in the data plane restarts since it fails to pass the health check.

NOTE: Refer to Data Plane Alarms.

DHCP Events

NOTE: This event is not applicable for vSZ-H.

Following are the events related to DHCP (Dynamic Host Configuration Protocol).

- DHCP inform received
- DHCP dcln received

DHCP inform received

Table 383. DHCP inform received event

Event	DHCP inform received
Event Type	dhcpInfmRcvd
Event Code	1238
Severity	Informational
Attribute	"mvnoId"=NA "wlanId"=NA,"zoneId"="NA" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="dhcp","realm"="NA" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	DHCP Inform was received by {produce.short.name} [{SCGMgmtIp}] from UE [{ueMacAddr}]
Description	This event occurs when the controller receives the DHCP information.

DHCP dcln received

Table 384. DHCP dcln received event

Event	DHCP dcln received
Event Type	dhcpDclnRcvd
Event Code	1239
Severity	Major
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut","realm"="NA" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	DHCP Decline was received by {produce.short.name} [{SCGMgmtIp}] from UE [{ueMacAddr}]
Description	This event occurs when the controller receives the DHCP declined message. The GTP (GPRS Tunneling Protocol) tunnel is deleted and recreated.

GA Interface Events

NOTE: This section is not applicable for vSZ-H.

Following are the events related to the GA interface (CDRs and GTP').

- Connection to CGF failed
- CGF keep alive not responded
- CDR transfer succeeded
- CDR transfer failed
- CDR generation failed

Connection to CGF failed

Table 385. Connection to CGF failed event

Event	Connection to CGF failed
Event Type	cnxnToCgfFailed
Event Code	1610
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA", "radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Connection with CGF [{cgfSrvrIp}] from RADServerIP [{radSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when channel interface processor (CIP) or GPRS tunneling protocol prime (GTPP) stack detects a connection loss to the charging gateway function (CGF server.
Auto Clearance	This event triggers the alarm 1610, which is auto cleared by the event code 1613.

CGF keep alive not responded

Table 386. CGF keep alive not responded event

Event	CGF keep alive not responded
Event Type	cgfKeepAliveNotResponded
Event Code	1612
Severity	Informational
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="NA","radSrvrIp"="7.7.7.7" "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Heartbeat missed between RAD Server [{radSrvrIp}] and CGF Server [{cgfSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when channel interface processor does not receive an acknowledgment for a keep alive request.

CDR transfer succeeded

Table 387. CDR transfer succeeded event

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

CDR transfer failed

Table 388. CDR transfer failed event

Event	CDR transfer failed
Event Type	cdrTxfrFailed
Event Code	1614
Severity	Major
Attribute	“mvnoId”=”2” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”cip” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radSrvrIp”=”7.7.7.7” "cgfSrvrIp"="40.40.40.40" "SCGMgmtIp"="2.2.2.2" “cause”=”<reason for failure>”
Displayed on the web interface	CDR Transfer failed from RAD Server [{radSrvrIp}] to CGF [{cgfSrvrIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the call detail record transfers fails.

CDR generation failed

Table 389. CDR generation failed event

Event	CDR generation failed
Event Type	cdrGenerationFailed
Event Code	1615
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="cip" "realm"="wlan.3gppnetwork.org" "radSrvrIp"="7.7.7.7" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Failed to generate CDR by RAD Server [{radSrvrIp}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the controller cannot format/generate the call detail records.

NOTE: Refer to GA Interface Alarms.

Gn/S2a Interface Events

NOTE: This event is not applicable for vSZ-H.

Following are the events related to Gn/S2a interface.

GGSN restarted	GGSN not reachable	Echo response not received
GGSN not resolved	PDP context established	PDP create failed
PDP update by HLR succeeded	PDP update by HLR failed	PDP update by roaming succeeded
PDP update by roaming failed	PDP update by GGSN succeeded	PDP update by GGSN failed
PDP delete by TTG succeeded	PDP delete by TTG failed	PDP delete by GGSN succeeded
PDP delete by GGSN failed	IP assigned	IP not assigned
Unknown UE	PDP update success COA	PDP update fail COA
PDNGW could not be resolved	PDNGW version not supported	Associated PDNGW down
Create session response failed	Decode failed	Modify bearer response failed
Delete session response failed	Delete bearer request failed	Update bearer request failed
CGF server not configured		

GGSN restarted

Table 390. GGSN restarted event

Event	GGSN restarted
Event Type	ggsnRestarted
Event Code	1210
Severity	Major
Attribute	"mvnoId"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm" "realm"="NA" "gtpcIp"="5.5.5.5", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{ggsnIp}] connected to {produce.short.name} [{SCGMgmtIp}] (GTPC-IP [{gtpcIp}]) is restarted

Table 390. GGSN restarted event

Description	This event occurs when GPRS protocol control plane receives a new recovery value.

GGSN not reachable

Table 391. GGSN not reachable event

Event	GGSN not reachable
Event Type	ggsnNotReachable
Event Code	1211
Severity	Major
Attribute	"mvnoId"="12","ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm","realm"="NA", "gtpcIp"="5.5.5.5", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{ggsnIp}] connected to {produce.short.name} (GTPC-IP [{gtpcIp}]) is not reachable
Description	This event occurs when echo request is timed out.

Echo response not received

Table 392. Echo response not received event

Event	Echo response not received
Event Type	echoRspNotRcvd
Event Code	1212
Severity	Informational
Attribute	"mvnoId"="12", "ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="sm" "realm"="NA" "gtpcIp"="5.5.5.5", "ggsnIp"="10.10.10.10", "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	GGSN [{ggsnIp}] did not respond to Echo Request from {produce.short.name} (GTPC-IP [{gtpcIp}]) is not reachable
Description	This event occurs when GPRS protocol control plane does not receive an acknowledgment for the single echo request.

GGSN not resolved

Table 393. GGSN not resolved event

Event	GGSN not resolved
Event Type	ggsnNotResolved
Event Code	1215
Severity	Major
Attribute	"mvnoId"="12", "wlanId"="1","zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787"
Displayed on the web interface	Failed to resolve GGSN from APN [{apn}] for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}]
Description	This even occurs when access point name is unable to resolve to gateway GPRS support node.

PDP context established

Table 394. PDP context established event

Event	PDP context established
Event Type	pdpCtxtEstablished
Event Code	1216
Severity	Debug
Attribute	"mvnoId"=12,"wlanId"=1 "zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	PDP context created for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol is established.

PDP create failed

Table 395. PDP create failed event

Event	PDP create failed
Event Type	crtPdpFailed
Event Code	1217
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	PDP context create failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Cause [{cause}]
Description	This event occurs when create packet data protocol fails.

PDP update by HLR succeeded

Table 396. PDP update by HLR succeeded event

Event	PDP update by HLR succeeded
Event Type	initPdpUpdSuccHlr
Event Code	1218
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "hlrEvent"="<event received from HLR>"
Displayed on the web interface	PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because of [hlrEvent] from HLR

Table 396. PDP update by HLR succeeded event

Description	This event occurs when packet data protocol context is updated successfully. Update is initiated by tunneling termination gateway (TTG) control plane as a result of the home location register (HLR) initiation.

PDP update by HLR failed

Table 397. PDP update by HLR failed event

Event	PDP update by HLR failed
Event Type	initPdpUpdFailureHlr
Event Code	1219
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error" "hlrEvent"="<event received from HLR>"
Displayed on the web interface	PDP context update initiated because of HLR Event [{hlrEvent}] failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Failure Cause [{cause}]
Description	This event occurs when update packet data protocol fails. Update is initiated by TTG control plane as a result of HLR initiation.

PDP update by roaming succeeded

Table 398. PDP update by roaming succeeded event

Event	PDP update by roaming succeeded
Event Type	initPdpUpdSuccRoam
Event Code	1220
Severity	Debug

Table 398. PDP update by roaming succeeded event

Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787"
Displayed on the web interface	PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because of UE Roaming
Description	This event occurs when packet data protocol context is updated successfully. Update is initiated by TTG control plane as a result of user equipment.

PDP update by roaming failed

Table 399. PDP update by roaming failed event

Event	PDP update by roaming failed
Event Type	initPdpUpdFailureRoam
Event Code	1221
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	PDP context update initiated because of UE Roaming failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] Failure Cause [{cause}]
Description	This event occurs when the packet data protocol update fails. This is initiated by TTG control plane as a result of user equipment.

PDP update by GGSN succeeded

Table 400. PDP update by GGSN succeeded event

Event	PDP update by GGSN succeeded
Event Type	recvPdpUpdSuccGgsn
Event Code	1222
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	GGSN initiated; PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol is updated successfully, which is initiated by the GGSN.

PDP update by GGSN failed

Table 401. PDP update by GGSN failed event

Event	PDP update by GGSN failed
Event Type	recvPdpUpdFailureGgsn
Event Code	1223
Severity	Debug
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”sm_process” “realm”=”NA" “gtpcIp”=”5.5.5.5” "ggsnIp"="10.10.10.10" “ueMacAddr”=”NA” “ueImsi”=”NA” "apn"="NA" "SCGMgmtIp"="2.2.2.2" “cause”=”cause of error”
Displayed on the web interface	GGSN initiated; PDP context update received from IP [{ggsnIp}] at {produce.short.name} [{SCGMgmtIp}] is failed. Cause [{cause}]
Description	This event occurs when the packet data protocol update fails.

PDP delete by TTG succeeded

Table 402. PDP delete by TTG succeeded event

Event	PDP delete by TTG succeeded
Event Type	initPdpDelSucc
Event Code	1224
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787"
Displayed on the web interface	{produce.short.name} initiated; PDP context deleted for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol delete is successful.

PDP delete by TTG failed

Table 403. PDP delete by TTG failed event

Event	PDP delete by TTG failed
Event Type	initPdpDelFailure
Event Code	1225
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="cause of error"
Displayed on the web interface	{produce.short.name} initiated; PDP context delete failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Cause [{cause}]
Description	This event occurs when packet data protocol delete fails.

PDP delete by GGSN succeeded

Table 404. PDP delete by GGSN succeeded event

Event	PDP delete by GGSN succeeded
Event Type	recvPdpDelSucc
Event Code	1226
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	GGSN initiated; PDP context deleted for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when packet data protocol delete is successful, as initiated by the GGSN.

PDP delete by GGSN failed

Table 405. PDP delete by GGSN failed event

Event	PDP delete by GGSN failed
Event Type	recvPdpDelFailure
Event Code	1227
Severity	Debug
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”sm_process” “realm”=”NA" “gtpcIp”=”5.5.5.5” "ggsnIp"="10.10.10.10" “ueMacAddr”=”NA” “ueImsi”=”NA” "apn"="NA" "SCGMgmtIp"="2.2.2.2" “cause”=”cause of error”
Displayed on the web interface	GGSN initiated; PDP context delete received from IP [{ggsnIp}] at {produce.short.name} [{SCGMgmtIp}] is failed. Cause [{cause}].
Description	This event occurs when delete packet data protocol fails. Delete is initiated by GGSN.

IP assigned

Table 406. IP assigned event

Event	IP assigned
Event Type	ipAssigned
Event Code	1229
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] was assigned IP [{ueIpAddr}] at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when IP address is assigned to the user equipment. This event is applicable for TTG/PDG sessions only.

IP not assigned

Table 407. IP not assigned event

Event	IP not assigned
Event Type	ipNotAssigned
Event Code	1230
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "cause"="<why IP could not be assigned>"
Displayed on the web interface	IP could not be assigned to UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because [{cause}]
Description	This event occurs when the IP address is not assigned to user euipment. This event is applicable for TTG/PDG sessions only.

Unknown UE

Table 408. Unknown UE event

Event	Unknown UE
Event Type	unknownUE
Event Code	1231
Severity	Minor
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "cause"="Subscriber Info Not Found" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Received request from un-known UE [{ueMacAddr}] in {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when TTG control plane receives either a DHCP message or a trigger from data plane. It is unable to find the user equipment in the session context.

PDP update success COA

Table 409. PDP update success COA event

Event	PDP update success COA
Event Type	pdpUpdSuccCOA
Event Code	1244
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "aaaSrvrIp"="5.5.5.5"
Displayed on the web interface	PDP context updated for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}] because of COA from AAA server [{aaaSrvrIp}]
Description	This event occurs when the packet data protocol update is successful when initiating the update process based on the change of authorization received from the external AAA server.

PDP update fail COA

Table 410. PDP update fail COA event

Event	PDP update fail COA
Event Type	pdpUpdFailCOA
Event Code	1245
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "gtpcIp"="5.5.5.5" "apn"="ruckuswireless.com" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345","ueMsisdn"="98787" "aaaSrvrIp"="5.5.5.5" "cause"="cause of error"
Displayed on the web interface	PDP context update initiated because of COA from AAA server [{gtpcIp}] failed for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] at {produce.short.name} [{SCGMgmtIp}]. Failure Cause [{cause}].
Description	This event occurs when the packet data protocol update fails when initiating the update process based on the change of authorization received from the external AAA server.

PDNGW could not be resolved

Table 411. PDNGW could not be resolved event

Event	PDNGW could not be resolved
Event Type	pdnGwNotResolved
Event Code	1950
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "apn"="ruckus.com"
Displayed on the web interface	[{srcProcess}] APN [{apn}] could not be resolved on {produce.short.name} [{SCGMgmtIp}], with username [{ueImsi}@{realm}]

Table 411. PDNGW could not be resolved event

Description	This event occurs when the access point name is unable to resolve to PDN GW.

PDNGW version not supported

Table 412. PDNGW version not supported event

Event	PDNGW version not supported
Event Type	pdnGwVersionNotSupportedMsgReceived
Event Code	1952
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii""ueImsi"="12345","ueMsisdn"="98787" "APN"="ruckus.com", “pgwIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Version not supported message received from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the version is not supported for messages received from PDN GW.

Associated PDNGW down

Table 413. Associated PDNGW down event

Event	Associated PDNGW down
Event Type	pdnGwAssociationDown
Event Code	1953
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "APN"="ruckus.com",“pgwIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Association with PDN GW with IP [{pgwIp}] from {produce.short.name} [{SCGMgmtIp}] down
Description	This event occurs when the association with PDN GW is down due to echo request time out or it fails to send messages to PDN GW.

Create session response failed

Table 414. Create session response failed event

Event	Create session response failed
Event Type	createSessionResponseFailed
Event Code	1954
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "APN"="ruckus.com" "cause"="xx",“pgwIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Create Session response from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	This event occurs when create session response from PDN GW fails with a cause.

Decode failed

Table 415. Decode failed event

Event	Decode failed
Event Type	decodeFailed
Event Code	1955
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="sm_proces" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345", "ueMsisdn"="98787" "APN"="ruckus.com",“pgwIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Decode of message received from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed
Description	This event occurs when decoding of messages received from PDN GW fails.

Modify bearer response failed

Table 416. Modify bearer response failed event

Event	Modify bearer response failed
Event Type	modifyBearerResponseFailed
Event Code	1956
Severity	Major
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787", "APN"="ruckus.com" "cause"="xx",“pgwIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Modify Bearer Response from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	This event occurs when modify bearer response from PDN GW fails with a cause.

Delete session response failed

Table 417. Delete session response failed event

Event	Delete session response failed
Event Type	deleteSessionResponseFailed
Event Code	1957
Severity	Major
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com" "cause"="xx","pgwIp"="1.1.1.1"
Displayed on the web interface	[{srcProcess}] Delete Session response from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	This event occurs when the delete session response from PDN GW fails.

Delete bearer request failed

Table 418. Delete bearer request failed event

Event	Delete bearer request failed
Event Type	deleteBearerRequestFailed
Event Code	1958
Severity	Major
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com","cause"="<reason for failure>","pgwIp"="1.1.1.1"
Displayed on the web interface	[{srcProcess}] Delete Bearer Request from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]

Table 418. Delete bearer request failed event

Description	This event occurs when the delete bearer request from PDN GW fails with decode error.

Update bearer request failed

Table 419. Update bearer request failed event

Event	Update bearer request failed
Event Type	updateBearerRequestFailed
Event Code	1959
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"="ruckus.com",“cause”=”<reason for failure>”,“pgwIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Update bearer request from PDN GW with IP [{pgwIp}] on {produce.short.name} [{SCGMgmtIp}] failed, for UE with username [{ueImsi}@{realm}] because [{cause}]
Description	This event occurs when the update bearer request fails with a decode error.

CGF server not configured

Table 420. CGF server not configured event

Event	CGF server not configured
Event Type	cgfServerNotConfigured
Event Code	1960
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="CIP" "realm"="wlan.3gppnetwork.org" "SCGMgmtIp"="2.2.2.2" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueImsi"="12345" "ueMsisdn"="98787" "APN"=ruckus.com "cgfSrvrIp" = "1.1.1.1", “ggsnIp”=”10.10.10.10”
Displayed on the web interface	CGF server IP [{cgfSrvrIp}] received from PDN GW/GGSN with IP [{ggsnIp}] on {produce.short.name} [{SCGMgmtIp}] is not configured
Description	This event occurs when the IP address of the charging gateway function server received from GGSN/PDNGW is not configured in the controller web interface.

NOTE: Refer to Gn/S2a Interface Alarms.

Gr Interface Event

NOTE: This section is not applicable for vSZ-H.

Following are the events related to GR interface.

- Destination not reachable
- Destination available
- App server down
- App server inactive
- App server active
- Association establishment failed
- Association down
- Association up
- Send auth info success
- Auth info sending failed
- GPRS location update succeeded
- GPRS location update failed
- Insert sub data success
- Insert sub data failed
- Outbound routing failure
- Did allocation failure
- Restore data success
- Restore data failed

Destination not reachable

Table 421. Destination not reachable event

Event	Destination not reachable
Event Type	destNotRecheable
Event Code	1618
Severity	Critical
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "pointCode"="1.1.1"
Displayed on the web interface	Remote Point Code [{pointCode}] is unavailable
Description	This event occurs when the point code is unreachable due to a pause indicator
Auto Clearance	This event triggers the alarm 1618, which is auto cleared by the event code 1620.

Destination available

Table 422. Destination available event

Event	Destination available
Event Type	destAvailable
Event Code	1620
Severity	Critical
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "pointCode"="1.1.1"
Displayed on the web interface	Remote Point Code [{pointCode}] is available
Description	This event occurs when the point code is available due to the resume indicator.

App server down

Table 423. App server down event

Event	App server down
Event Type	appServerDown
Event Code	1623
Severity	Critical
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "routingContext" ="1" "pointCode"="1.1.1" "SSN" = "7"
Displayed on the web interface	Application Server Down, Routing Context [{routingContext}], local Point Code [{pointCode}], local SSN [{SSN}]
Description	This event occurs when the local application server is down from the remote IP security protocol (IPSP) or controller.
Auto Clearance	This event triggers the alarm 1623, which is auto cleared by the event code 1625.

App server inactive

Table 424. App server inactive event

Event	App server inactive
Event Type	appServerInactive
Event Code	1624
Severity	Critical
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "routingContext" ="1" "pointCode"="1.1.1" "SSN" = "7"
Displayed on the web interface	Application Server Inactive, Routing Context [{routingContext}], lpcal Point Code [{pointCode}], local SSN [{SSN}]
Description	This event occurs when the local application server is inactive from the remote IPSP/controller.
Auto Clearance	This event triggers the alarm 1624, which is auto cleared by the event code 1625.

App server active

Table 425. App server active event

Event	App server active
Event Type	appServerActive
Event Code	1625
Severity	Critical
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "routingContext" ="1" "pointCode"="1.1.1" "SSN" = "7"
Displayed on the web interface	Application Server Active, Routing Context [{routingContext}], Ipcal Point Code [{pointCode}], local SSN [{SSN}]
Description	This event occurs when the local application server is active from the remote IPSP or signalling gateway (SG).

Association establishment failed

Table 426. Association establishment failed event

Event	Association establishment failed
Event Type	assocEstbFailed
Event Code	1626
Severity	Critical
Attribute	"mvnoId"="3" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "srcIP"="10.1.4.10" "srcPort"="2960" "destIP"="10.1.4.20" "destPort"="2960"
Displayed on the web interface	Unable to establish SCTP association srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This event occurs when it is unable to establish an association to the controller/IPSP.
Auto Clearance	This event triggers the alarm 1626, which is auto cleared by the event code 1628.

Association down

Table 427. Association down event

Event	Association down
Event Type	assocDown
Event Code	1627
Severity	Critical
Attribute	"mvnoId"="3" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "srcIP"="10.1.4.10" "srcPort"="2960" "destIP"="10.1.4.20" "destPort"="2960"
Displayed on the web interface	SCTP association DOWN srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This event occurs when the stream control transmission protocol (SCTP) association is down.
Auto Clearance	This event triggers the alarm 1627, which is auto cleared by the event code 1628.

Association up

Table 428. Association up event

Event	Association up
Event Type	assocUp
Event Code	1628
Severity	Critical
Attribute	"mvnoId"="3" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "srcIP"="10.1.4.10" "srcPort"="2960" "destIP"="10.1.4.20" "destPort"="2960"
Displayed on the web interface	SCTP association UP. srcIP [{srcIP}], srcPort [{srcPort}], destIP[{destIP}], destPort [{destPort}]
Description	This event occurs when the SCTP association is UP.

Send auth info success

Table 429. Send auth info success event

Event	Send auth info success
Event Type	sendAuthInfoSuccess
Event Code	1630
Severity	Debug
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918"
Displayed on the web interface	MAP-SendAuthInfo Operation successful from IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when authentication parameters are successfully retrieved.

Auth info sending failed

Table 430. Auth info sending failed event

Event	Auth info sending failed
Event Type	sendAuthInfoFailed
Event Code	1631
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-SendAuthInfo Operation Failed for IMSI [{ueImsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to retrieve the authentication parameters.

GPRS location update succeeded

Table 431. GPRS location update succeeded event

Event	GPRS location update succeeded
Event Type	updateGprsLocSuccess
Event Code	1632
Severity	Debug
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918"
Displayed on the web interface	MAP-UpdateGprsLocation Operation Successful for IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when it successfully updates the GPRS location operation.

GPRS location update failed

Table 432. GPRS location update failed event

Event	GPRS location update failed
Event Type	updateGprsLocFailed
Event Code	1633
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-UpdateGprsLocation Operation Failed for IMSI [{ueImsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when the GPRS location update process fails.

Insert sub data success

Table 433. Insert sub data success event

Event	Insert sub data success
Event Type	insertSubDataSuccess
Event Code	1634
Severity	Debug
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918"
Displayed on the web interface	MAP-InsertSubscriberData Operation Successful for IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when it successfully inserts the subscriber data operation.

Insert sub data failed

Table 434. Insert sub data failed event

Event	Insert sub data failed
Event Type	insertSubDataFailed
Event Code	1635
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918" "cause"="ASN decode error"
Displayed on the web interface	MAP-InsertSubscriberData Operation Failed for IMSI [{ueImsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to insert the subscriber data operation

Outbound routing failure

Table 435. Outbound routing failure event

Event	Outbound routing failure
Event Type	outboundRoutingFailure
Event Code	1636
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "operation"="updateGprsLocationReq" "hlrInstance"=" Vodafone_HLR" "ueImsi "=" 04844624203918"
Displayed on the web interface	Unable to route [{operation}] for IMSI [{ueImsi}] to HLR [{hlrInstance}]
Description	This event occurs when it is unable to route transaction capabilities application (TCAP) message to the destination.

Did allocation failure

Table 436. Did allocation failure event

Event	Did allocation failure
Event Type	didAllocationFailure
Event Code	1637
Severity	Critical
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip"
Displayed on the web interface	HIP unable to allocate new dialogue
Description	This event occurs when it is unable to allocate the dialogue identifier for a new transaction. This indicates an overload condition.

Restore data success

Table 437. Restore data success event

Event	Restore data success
Event Type	restoreDataSuccess
Event Code	1639
Severity	Debug
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi "="04844624203918"
Displayed on the web interface	MAP-RestoreData Operation Successful for IMSI [{ueImsi}] with [{hlrInstance}]
Description	This event occurs when it successfully restores the data operation.

Restore data failed

Table 438. Restore data failed event

Event	Restore data failed
Event Type	restoreDataFailed
Event Code	1640
Severity	Major
Attribute	"mvnoId"="2" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="hip" "hlrInstance"="Vodafone_HLR" "ueImsi"="04844624203918" "cause"="Timeout"
Displayed on the web interface	MAP-RestoreData Operation Failed for IMSI [{ueImsi}] with [{hlrInstance}], cause [{cause}]
Description	This event occurs when it fails to restore the data operation.

NOTE: Refer to GR Interface Alarms.

IPMI Events

NOTE: This section is not applicable for vSZ-H.

Following are the events related to IPMIs.

ipmiVoltage	ipmiThempBB	ipmiThempFP
ipmiThempIOH	ipmiThempMemP	ipmiThempPS
ipmiThempP	ipmiThempHSBP	ipmiFan
ipmiPower	ipmiCurrent	ipmiFanStatus
ipmiPsStatus	ipmiDrvStatus	ipmiREVotage
ipmiREThempBB	ipmiREThempFP	ipmiREThempIOH
ipmiREThempMemP	ipmiREThempPS	ipmiREThempP
ipmiREThempHSBP	ipmiREFan	ipmiREPower
ipmiRECurrent	ipmiREFanStatus	ipmiREPsStatus
ipmiREDrvStatus		

ipmiVoltage

Table 439. ipmiVoltage event

Event	ipmiVoltage
Event Type	ipmiVotage
Event Code	901
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard voltage [{status}] on control plane [{nodeMac}]
Description	This event occurs due to under /over voltage on the control plane. Baseboard threshold temperatures are: • Critical high - 66^0 C • Non critical high - 61^0 C • Non critical low - 10^0 C • Critical low - 5^0 C

Table 439. ipmiVoltage event

Auto Clearance	This event triggers the alarm 901, which is auto cleared by the event code 926.

ipmiThempBB

Table 440. 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.

ipmiThempFP

Table 441. ipmiThempFP event

Event	ipmiThempFP
Event Type	ipmiThempFP
Event Code	903
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the front panel temperature status is sent. Front panel threshold temperatures are in the range of 5^0 Celsius to 44^0 Celsius. The default threshold is 44^0C.

Table 441. ipmiThempFP event

Auto Clearance	This event triggers the alarm 903, which is auto cleared by the event code 928.

ipmiThempIOH

Table 442. ipmiThempIOH event

Event	ipmiThempIOH
Event Type	ipmiThempIOH
Event Code	904
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Chipset temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the chip set temperature status is sent. IOH thermal margin threshold temperatures are in the range of -20^0 Celsius to 5^0 Celsius. The default threshold is 5^0C.
Auto Clearance	This event triggers the alarm 904, which is auto cleared by the event code 929.

ipmiThempMemP

Table 443. ipmiThempMemP event

Event	ipmiThempMemP
Event Type	ipmiThempMemP
Event Code	905
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] memory temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the processor memory temperature status is sent. Process 1 memory thermal margin threshold temperatures are in the range of -20^0 Celsius to 5^0 Celsius. The default threshold is 5^0C.

Table 443. ipmiThempMemP event

Auto Clearance	This event triggers the alarm 905, which is auto cleared by the event code 930.

ipmiThempPS

Table 444. ipmiThempPS event

Event	ipmiThempPS
Event Type	ipmiThempPS
Event Code	906
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the power supply temperature status is sent. Power supply 1 and power supply 2 threshold temperatures are in the range of -20^0 Celsius to 5^0 Celsius. The default threshold is 5^0C.
Auto Clearance	This event triggers the alarm 906, which is auto cleared by the event code 931.

ipmiThempP

Table 445. ipmiThempP event

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

ipmiThempHSBP

Table 446. ipmiThempHSBP event

Event	ipmiThempHSBP
Event Type	ipmiThempHSBP
Event Code	908
Severity	Majorf
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Hot swap backplane temperature [{status}] on control plane [{nodeMac}]
Description	This event occurs when the hot swap back plane temperature status in the range of 9^0 Celsius to 55^0 Celsius. The default threshold is 55^0C.
Auto Clearance	This event triggers the alarm 908, which is auto cleared by the event code 933.

ipmiFan

Table 447. ipmiFan event

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

ipmiPower

Table 448. ipmiPower event

Event	ipmiPower
Event Type	ipmiPower
Event Code	910
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}]
Description	This event occurs when the AC power input status is sent.
Auto Clearance	This event triggers the alarm 910, which is auto cleared by the event code 935.

ipmiCurrent

Table 449. ipmiCurrent event

Event	ipmiCurrent
Event Type	ipmiCurrent
Event Code	911
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] +12V% of maximum current output [{status}] on control plane [{nodeMac}]
Description	This event occurs when the power supply and the maximum voltage output status is sent.
Auto Clearance	This event triggers the alarm 911, which is auto cleared by the event code 936.

ipmiFanStatus

Table 450. ipmiFanStatus event

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

ipmiPsStatus

Table 451. ipmiPsStatus event

Event	ipmiPsStatus
Event Type	ipmiPsStatus
Event Code	913
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the power supply status is sent.
Auto Clearance	This event triggers the alarm 913, which is auto cleared by the event code 938.

ipmiDrvStatus

Table 452. ipmiDrvStatus event

Event	ipmiDrvStatus
Event Type	ipmiDrvStatus
Event Code	914
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Disk drive [{id}] [{status}] on control plane [{nodeMac}]
Description	This event occurs when the disk drive status is sent.
Auto Clearance	This event triggers the alarm 914, which is auto cleared by the event code 939.

ipmiREVotage

Table 453. ipmiREVotage event

Event	ipmiREVotage
Event Type	ipmiREVotage
Event Code	926
Severity	Informational
Attribute	“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Baseboard voltage [{status}] on control plane [{nodeMac}].
Description	This event occurs when the baseboard voltage comes back to the the normal status.

ipmiREThempBB

Table 454. ipmiREThempBB event

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

ipmiREThempFP

Table 455. ipmiREThempFP event

Event	ipmiREThempFP
Event Type	ipmiREThempFP
Event Code	928
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Front panel temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the front panel temperature comes back to the normal status.

ipmiREThempIOH

Table 456. ipmiREThempIOH event

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

Table 456. ipmiREThempIOH event

Displayed on the web interface	Chipset temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the chipset temperature comes back to the normal status.

ipmiREThempMemP

Table 457. ipmiREThempMemP event

Event	ipmiREThempMemP
Event Type	ipmiREThempMemP
Event Code	930
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Processor [{id}] memory temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the processor memory temperature comes back to the normal status.

ipmiREThempPS

Table 458. ipmiREThempPS event

Event	ipmiREThempPS
Event Type	ipmiREThempPS
Event Code	931
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the power supply temperature comes back to the normal status.

ipmiREThempP

Table 459. ipmiREThempP event

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

ipmiREThempHSBP

Table 460. ipmiREThempHSBP event

Event	ipmiREThempHSBP
Event Type	ipmiREThempHSBP
Event Code	933
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Hot swap backplane temperature [{status}] on control plane [{nodeMac}].
Description	This event occurs when the hot swap backplane temperature comes back to the normal status.

ipmiREFan

Table 461. ipmiREFan event

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

Table 461. ipmiREFan event

Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}].
Description	This event occurs when the system fan module comes back to the normal status.

ipmiREPower

Table 462. ipmiREPower event

Event	ipmiREPower
Event Type	ipmiREPower
Event Code	935
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}].
Description	This event occurs when the AC power supply comes back to the normal status.

ipmiRECurrent

Table 463. ipmiRECurrent event

Event	ipmiRECurrent
Event Type	ipmiRECurrent
Event Code	936
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] AC power input [{status}] on control plane [{nodeMac}].
Description	This event occurs when the AC power supply comes back to the normal status.

ipmiREFanStatus

Table 464. ipmiREFanStatus event

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

ipmiREPsStatus

Table 465. ipmiREPsStatus event

Event	ipmiREPsStatus
Event Type	ipmiREPsStatus
Event Code	938
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Power supply [{id}] [{status}] on control plane [{nodeMac}].
Description	This event occurs when the power supply comes back to the normal status.

ipmiREDrvStatus

Table 466. ipmiREDrvStatus event

Event	ipmiREDrvStatus
Event Type	ipmiREDrvStatus
Event Code	939
Severity	Informational
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Disk drive [{id}] [{status}] on control plane [{nodeMac}].
Description	This event occurs when the disk drive status comes back to the normal status.

NOTE: Refer to IPMI Alarms.

Licensing Interface Events

Following are the events related to licensing.

- TTG session warning threshold
- TTG session major threshold
- TTG session critical threshold
- TTG session license exhausted
- License sync succeeded
- License sync failed
- License import succeeded
- License import failed
- License data changed

TTG session warning threshold

NOTE: This event is not applicable for vSZ-H.

Table 467. TTG session warning threshold event

Event	TTG session warning threshold
Event Type	ttgSessionWarningThreshold
Event Code	1240
Severity	Warning
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut/lic”
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached warning level.
Description	This event occurs when the number of user equipment attached to the system has reached the warning/major/critical threshold limit.

TTG session major threshold

NOTE: This event is not applicable for vSZ-H.

Table 468. TTG session major threshold event

Event	TTG session major threshold
Event Type	ttgSessionMajorThreshold
Event Code	1241
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut/lic”
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached major level.
Description	This event occurs when the number of user equipment attached to the system has reached the warning/major/critical threshold limit.

TTG session critical threshold

NOTE: This event is not applicable for vSZ-H.

Table 469. TTG session critical threshold event

Event	TTG session critical threshold
Event Type	ttgSessionCriticalThreshold
Event Code	1242
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut/lic”
Displayed on the web interface	The licensed sessions of {produce.short.name} [{SCGMgmtIp}] have reached critical level.
Description	This event occurs when the number of user equipment attached to the system has reached the warning/major/critical threshold limit.

TTG session license exhausted

NOTE: This event is not applicable for vSZ-H.

Table 470. TTG session license exhausted event

Event	TTG session license exhausted
Event Type	ttgSessionLicenseExausted
Event Code	1243
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”aut/lic”
Displayed on the web interface	The licensed of {produce.short.name} [{SCGMgmtIp}] have been exhausted for all sessions.
Description	This event occurs when the number of user equipment attached to the system has exceeded the license limit.

License sync succeeded

Table 471. 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 472. 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 473. 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 474. 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 475. 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.

NOTE: Refer to Licensing Alarms.

Location Delivery Events

NOTE: This section is not applicable for vSZ-H.

Following are the events related to location delivery.

- Unavailable location info requested
- Incapable location info requested
- Unsupported location delivery request

Unavailable location info requested

Table 476. Unavailable location info requested event

Event	Unavailable location info requested
Event Type	unavailableLocInfoRequested
Event Code	1655
Severity	Debug
Attribute	“mvnoId”=12, “wlanId”=1, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”radiusd”, “realm”=”operator realm”, “radSrvrIp”=”1.1.1.1”, “requestedInfo”=”target location|geo location, etc”, “SCGMgmtIp”=”2.2.2.2”
Displayed on the web interface	AAA [{radSrvrIp}] requests [{requestedInfo}] that is not available with {produce.short.name}[{SCGMgmtIp}]
Description	This event occurs when the AAA server requests for the location information, which is not available at the controller. For example, the AAA server requests for the target location even after the controller communicating that it can only support NAS locations.

Incapable location info requested

Table 477. Incapable location info requested event

Event	Incapable location info requested
Event Type	incapableLocInfoRequested
Event Code	1656
Severity	Debug
Attribute	“mvnoId”=12, “wlanId”=1, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”“srcProcess”=”radius” “realm”=”operator realm”, “radSrvrIp”=”1.1.1.1”, “requestedInfo”=”target location|geo location, etc”, “SCGMgmtIp”=”2.2.2.2”
Displayed on the web interface	AAA [{radSrvrIp}] requests [{requestedInfo}] that is not advertised by {produce.short.name}[{SCGMgmtIp}]
Description	This event occurs when the AAA server requests for location information though the controller does not advertise that it is capable of delivering the location information.

Unsupported location delivery request

Table 478. Unsupported location delivery request event

Event	Unsupported location delivery request
Event Type	unSupportedLocDeliveryRequest
Event Code	1657
Severity	Debug
Attribute	“mvnoId”=12, “wlanId”=1, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”radius” “realm”=”operator realm”, “radSrvrIp”=”1.1.1.1” “requestedMethod”=”out of band|intial request, etc” “SCGMgmtIp”=”2.2.2.2”
Displayed on the web interface	AAA [{radSrvrIp}] requests [{requestedInfo}] that is not supported by {produce.short.name}[{SCGMgmtIp}].
Description	This event occurs when the AAA server requests for a delivery method that is not supported by the controller.

PMIPv6 Events

NOTE: This section is not applicable for vSZ-H.

Following are the events related to PMIPv6.

- Config update failed
- LMA ICMP reachable
- LMA ICMP unreachable
- LMA server unreachable
- LMA failed over
- Connect To DHCP
- DHCP connection lost

Config update failed

Table 479. Config update failed event

Event	Config update failed
Event Type	updateCfgFailed
Event Code	5004
Severity	Major
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”,”cause”=“reason”
Displayed on the web interface	Failed to apply configuration [{cause}] in PMIPv6 process at {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 receives an error or negative acknowledgment or improper/incomplete information from D-bus client.

LMA ICMP reachable

Table 480. LMA ICMP reachable event

Event	LMA ICMP reachable
Event Type	lmaIcmpReachable
Event Code	5005
Severity	Debug

Table 480. LMA ICMP reachable event

Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”,”lmaIp”=“1.1.1.1”
Displayed on the web interface	[{lmaIp}] ICMP reachable on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 daemon connects to the local mobility anchor (LMA) server through the internet control message protocol (ICMP) packet.

LMA ICMP unreachable

Table 481. LMA ICMP unreachable event

Event	LMA ICMP unreachable
Event Type	lmaIcmpUnreachable
Event Code	5006
Severity	Debug
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”,”lmaIp”=“1.1.1.1”
Displayed on the web interface	[{lmaIp}] ICMP unreachable on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 daemon is unable to connect to the LMA server through the ICMP packet.
Auto Clearance	This event triggers the alarm 5006, which is auto cleared by the event code 5005.

LMA server unreachable

Table 482. LMA server unreachable event

Event	LMA server unreachable
Event Type	lmaHbUnreachable
Event Code	5007
Severity	Debug
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”,”lmaIp”=“1.1.1.1”

Table 482. LMA server unreachable event

Displayed on the web interface	[{lmaIp}] fail have been detected on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 daemon detects either restart or failure of the LMA server.

LMA failed over

Table 483. LMA failed over event

Event	LMA failed over
Event Type	lmaFailOver
Event Code	5008
Severity	Major
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”,”lmaIp”= “1.1.1.1”
Displayed on the web interface	[{lmaIp}] Failover on {produce.short.name} [{SCGMgmtIp}]
Description	This event s logged when the standby LMA transits to an active mode. This includes the control plane identifier of the newly active LMA.

Connect To DHCP

Table 484. Connect To DHCP event

Event	Connect To DHCP
Event Type	connectedToDHCP
Event Code	5101
Severity	Debug
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”
Displayed on the web interface	PMIPv6 process connect to DHCP server successfully on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the PMIPv6 completes the configuration procedure successfully.

DHCP connection lost

Table 485. DHCP connection lost event

Event	DHCP connection lost
Event Type	lostCnxnToDHCP
Event Code	5102
Severity	Debug
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”SCGMgmtIp”=“2.2.2.2”
Displayed on the web interface	PMIPv6 process cannot connect to DHCP server on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the connection between PMIPv6 process and DHCP server is lost.
Auto Clearance	This event triggers the alarm 5102, which is auto cleared by the event code 5101.

NOTE: Refer to PMIPv6 Alarms.

Session Events

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

- Session timeout
- Delete all
- Binding succeeded
- Binding failed
- Binding time expired
- Binding revoked
- Binding released

Session timeout

NOTE: This event is not applicable for vSZ-H.

Table 486. Session timeout event

Event	Session timeout
Event Type	sessTimeout
Event Code	1235
Severity	Debug
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" "ueMacAddr"="bb:aa:dd:dd:ee:ff" "cause"="Session Timeout" "SCGMgmtIp"="2.2.2.2" "ueImsi"="12345","ueMsisdn"="98787"
Displayed on the web interface	Session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] got deleted due to Session Timeout on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when a session is deleted due to a timeout specified by the AAA server.

Delete all

Table 487. Delete all sessions event

Event	Delete all sessions
Event Type	delAllSess
Event Code	1237
Severity	Minor
Attribute	"mvnoId"="NA" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="NA" "cause"="Admin Delete" "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	All sessions got terminated on {produce.short.name} [{SCGMgmtIp}] due to [{cause}]
Description	This event occurs when all sessions are deleted based on the indicators received from the controller web interface or CLI.

Binding succeeded

NOTE: This event is not applicable for vSZ-H.

Table 488. Binding succeeded event

Event	Binding succeeded
Event Type	bindingSuccess
Event Code	5009
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmaIp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "ueIpAddr"="5.5.5.5" "dataBladeIp"="3.3.3.3"
Displayed on the web interface	[{ueMacAddr}] UE binding update successful on {produce.short.name}-D [{dataBladeIp}], and get IP address: [{ueIpAddr}] from LMA: [{lmaIp}]
Description	This event occurs when the binding update is successful.

Binding failed

NOTE: This event is not applicable for vSZ-H.

Table 489. Binding failed event

Event	Binding failed
Event Type	bindingFailure
Event Code	5010
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "ImaIp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5" "cause"="failure cause"
Displayed on the web interface	Binding for [{ueMacAddr}] UE binding update failure on {produce.short.name}-D [{dataBladeIp}]. Failure Cause [{cause}].
Description	This event occurs when the binding update fails.
Auto Clearance	This event triggers the alarm 5010, which is auto cleared by the event code 5009.

Binding time expired

NOTE: This event is not applicable for vSZ-H.

Table 490. Binding time expired event

Event	Binding time expired
Event Type	bindingExpired
Event Code	5011
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "SCGMgmtIp"="2.2.2.2" "ImaIp"="1.1.1.1", "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	[{ueMacAddr}] UE Binding expired on {produce.short.name}-D [{dataBladeIp}]
Description	This event occurs when the binding expires.

Binding revoked

NOTE: This event is not applicable for vSZ-H.

Table 491. Binding revoked event

Event	Binding revoked
Event Type	bindingRevoked
Event Code	5012
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmaIp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	[{ueMacAddr}] UE Binding have been revoked on {produce.short.name}-D [{dataBladeIp}]
Description	This event occurs when the binding is revoked on the controller.

Binding released

NOTE: This event is not applicable for vSZ-H.

Table 492. Binding released event

Event	Binding released
Event Type	bindingReleased
Event Code	5013
Severity	Debug
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "SCGMgmtIp"="2.2.2.2" "lmaIp"="1.1.1.1" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "dataBladeIp"="3.3.3.3" "ueIpAddr"="5.5.5.5"
Displayed on the web interface	[{ueMacAddr}] UE Binding have been released on {produce.short.name}-D [{dataBladeIp}]
Description	This event occurs when the controller send a binding update message to the LMA on a PMIP session termination from AP.

NOTE: Refer to Session Alarms.

STA Interface Events

NOTE: This section is not applicable for vSZ-H.

Following are the events related to STA interface.

- STA successful authentication
- STA authentication failed transport down
- STA authentication failed failure response
- STA authentication failed decode failure
- STA session termination {produce.short.name} initiated success
- STA session termination AAA initiated success
- STA session termination AAA initiated failed
- STA re-authorization successful
- STA re-authorization failed
- STA response timer expired
- Retransmission exhausted

STA successful authentication

Table 493. STA successful authentication event

Event	STA successful authentication
Event Type	staSucessfulAuthentication
Event Code	1550
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaServIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with AAA server [{aaaSrvrIp}] Successful

Table 493. STA successful authentication event

Description	This event occurs when the authentication procedure with external 3GPP AAA server is successful. The diameter EAP request (DER is received from the 3GPP AAA server with result code as successful.

STA authentication failed transport down

Table 494. STA authentication failed transport down event

Event	STA authentication failed transport down
Event Type	staAuthFailedTransDown
Event Code	1551
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with AAA [{aaaSrvrIp}] failed as Transport is down
Description	This event occurs when the authentication procedure with external AAA server fails and the STA transport is down.

STA authentication failed failure response

Table 495. STA authentication failed failure response event

Event	STA authentication failed failure response
Event Type	staAuthFailedFailureResp
Event Code	1552
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”, “resultCode” =”Decode Failed”
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with 3GPP AAA [{aaaSrvrIp}] failed, DEA with failure code [{resultCode}]

Table 495. STA authentication failed failure response event

Description	This event occurs when the authentication procedure with external AAA server fails. The diameter EAP answer received from 3GPP AAA server fails with result code.

STA authentication failed decode failure

Table 496. STA authentication failed decode failure event

Event	STA authentication failed decode failure
Event Type	staAuthFailedDecodeFailure
Event Code	1553
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”, “resultCode”=”xyz”
Displayed on the web interface	[{srcProcess}] Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with 3GPP AAA [{aaaSrvrIp}] failed, DEA decode failed
Description	This event occurs when the authentication procedure with external 3GPP AAA server fails. The DEA received from 3GPP AAA server fails with result code.

STA session termination {produce.short.name} initiated success

Table 497. STA session termination {produce.short.name} initiated success event

Event	STA session termination {produce.short.name} initiated success
Event Type	staSessionTermSCGInitSuccess
Event Code	1554
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12,“srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”

Table 497. STA session termination {produce.short.name} initiated success event

Displayed on the web interface	[{srcProcess}] session termination of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] with 3GPP AAA [{aaaSrvrIp}] successful
Description	This event occurs when the controller initiated session termination-r (STR) is received and successfully terminated by the STA interface.

STA session termination AAA initiated success

Table 498. STA session termination AAA initiated success event

Event	STA session termination AAA initiated success
Event Type	staSessionTermAAAInitSucess
Event Code	1555
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Session Termination of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] sucessful. AS-R request from AAA
Description	This event occurs when the controller receives and successfully terminates the abort session request (ASR) initiated by the 3GPP AAA server.

STA session termination AAA initiated failed

Table 499. STA session termination AAA initiated failed event

Event	STA session termination AAA initiated failed
Event Type	staSessionTermAAAInitFailed
Event Code	1556
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp ”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Session Termination of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] failed. AS-R request from AAA
Description	This event occurs when the controller does not receive the abort session request initiated by the 3GPP AAA server.

STA re-authorization successful

Table 500. STA re-authorization successful event

Event	STA re-authorization successful
Event Type	staReAuthSuccess
Event Code	1557
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”=”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Re-Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] successful
Description	This event occurs when the 3GPP AAA initiated reauthorization re-auth request (RAR) is successful.

STA re-authorization failed

Table 501. STA re-authorization failed event

Event	STA re-authorization failed
Event Type	staReAuthFailed
Event Code	1558
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Re-Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] failed
Description	This event occurs when the 3GPP AAA initiated reauthorization re-auth request fails.

STA response timer expired

Table 502. STA response timer expired event

Event	STA response timer expired
Event Type	staResponseTimerExpired
Event Code	1559
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12, “srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Re-Auth of [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] from 3GPP AAA [{aaaSrvrIp}] failed]
Description	This event occurs when the Tx timer expires and the controller does not receive a response from 3GPP AAA server.

Retransmission exhausted

Table 503. Retransmission exhausted event

Event	Retransmission exhausted
Event Type	retransmitExausted
Event Code	1560
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, mvnoId”=12,“srcProcess”=”STA”, “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org", “ueImsi”=”12345”, “ueUsername”=”98787”, "SCGMgmtIp"="2.2.2.2",“aaaSrvrIp”=”1.1.1.1”
Displayed on the web interface	[{srcProcess}] Retransmission for [{ueImsi}]/[{ueUsername}] on {produce.short.name} [{SCGMgmtIp}] to 3GPP AAA [{aaaSrvrIp}] failed. Retransmission of messages to 3GPP AAA [{resultCode}] failed
Description	This event occurs when the retransmission from the 3GPP AAA server fails.

NOTE: Refer to STA Interface Alarms.

System Events

Following are the events with the system log severity.

NOTE: {produce.short.name} refers to SCG or vSZ-H

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 calibration request to AP
{produce.short.name} forwarded footfall request to AP	{produce.short.name} received unrecognized request	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	HIP started	HIP stopped
HIP failed over	Standby HIP restarted	HIP cache cleaned
Diameter initialization error	Diameter initialization	Diameter peer transport failure
Diameter CER error	Diameter CER success	Diameter invalid version
Diameter peer add error	Diameter peer add successful	Diameter peer remove successful
Diameter realm entry error	Diameter failover to alternate peer	Diameter fail back to peer
Diameter CEA unknown peer	Diameter no common application	ZD AP migrating
ZD AP migrated	ZD AP rejected	ZD AP migration failed
Database error	Process initiated	PMIPv6 unavailable
Memory allocation failed	Process stopped	

No LS responses

Table 504. No LS responses event

Event	No LS responses
Event Type	scgLBSNoResponse
Event Code	721
Severity	Major
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “url”=““, “port”=““, “SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] no response from LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller does not get a response while connecting to the location based service.

LS authentication failure

Table 505. LS authentication failure event

Event	LS authentication failure
Event Type	scgLBSAuthFailed
Event Code	722
Severity	Major
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “url”=““, “port”=““, “SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] authentication failed: url=[{url}], port=[{port}]
Description	This event occurs due to the authentication failure on connecting to the location based service.

{produce.short.name} connected to LS

Table 506. {produce.short.name} connected to LS event

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

Table 506. {produce.short.name} connected to LS event

Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] connected to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller successfully connects to the location based service.

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

Table 507. {produce.short.name} failed to connect to LS event

Event	{produce.short.name} failed to connect to LS
Event Type	scgLBSConnectFailed
Event Code	724
Severity	Major
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “url”=““, “port”=““, “SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] connection failed to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller failed to connect to the location based service.
Auto Clearance	This event triggers the alarm 724, which is auto cleared by the event code 723.

{produce.short.name} received passive request

Table 508. {produce.short.name} received passive request event

Event	{produce.short.name} received passive request
Event Type	scgLBSStartLocationService
Event Code	725
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx:”, “type”=““, “venue”=““, “SCGMgmtIp”=““, "band"=""
Displayed on the web interface	SmartZone [{SCGMgmtIp}] received Passive Request, band=[{band}], type=[{type}]
Description	This event occurs when the controller receives a passive request.

{produce.short.name} sent controller information report

Table 509. {produce.short.name} sent controller information report event

Event	{produce.short.name} sent controller information report
Event Type	scgLBSSentControllerInfo
Event Code	727
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “api”=““, “sw”=““, “clusterName”=““,”SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent Controller Info Report: mac =[{mac}], api=[{api}], sw=[{sw}], clusterName =[{clusterName}]
Description	This event occurs when the controller sends the controller information report.

{produce.short.name} received management request

Table 510. {produce.short.name} received management request event

Event	{produce.short.name} received management request
Event Type	scgLBSRcvdMgmtRequest
Event Code	728
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “venue”=““,”type”=““, “SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] received Management Request: venue=[{venue}], type=[{type}]
Description	This event occurs when the controller receives the management request.

{produce.short.name} sent AP info by venue report

Table 511. {produce.short.name} sent AP info by venue report event

Event	{produce.short.name} sent AP info by venue report
Event Type	scgLBSSendAPInfobyVenueReport
Event Code	729
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “venue”=““,”count”=““, “SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent AP Info by Venue Report: venue=[{venue}], count =[{count}]
Description	This event occurs when the controller sends the venue report regarding AP information.

{produce.short.name} sent query venues report

Table 512. {produce.short.name} sent query venues report event

Event	{produce.short.name} sent query venues report
Event Type	scgLBSSendVenuesReport
Event Code	730
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “count”=““, “SCGMgmtIp”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent Query Venues Report: count=[{count}]
Description	This event occurs when the controller sends the query venue report.

{produce.short.name} sent associated client report

Table 513. {produce.short.name} sent associated client report event

Event	{produce.short.name} sent associated client report
Event Type	scgLBSSendClientInfo
Event Code	731
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “count”=““, “SCGMgmtIp”=““, “type”=““
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] sent Associated Client Report: count= [{count}], type= [{type}]
Description	This event occurs when the controller sends the associated client report.

{produce.short.name} forwarded calibration request to AP

Table 514. {produce.short.name} forwarded calibration request to AP event

Event	{produce.short.name} forwarded calibration request to AP
Event Type	scgLBSFwdPassiveCalReq
Event Code	732
Severity	Informational
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "SCGMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue "="", "interval"="", "duration "="", "band"="", "count"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] forward Passive Calibration Request to [{apName&&apMac}]: venue= [{venue}], interval= [{interval}], duration= [{duration}], band= [{band}], count= [{count}]
Description	This event occurs when the controller sends a forward calibration request to the AP on its reconnection to the controller.

{produce.short.name} forwarded footfall request to AP

Table 515. {produce.short.name} forwarded footfall request to AP event

Event	{produce.short.name} forwarded footfall request to AP
Event Type	scgLBSFwdPassiveFFReq
Event Code	733
Severity	Informational
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "SCGMgmtIp"="", "apMac"="xx:xx:xx:xx:xx:xx", "venue "="", "interval"="", "duration "="", "band"="
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] forward Passive Footfall Request to [{apName&&apMac}]: venue= [{venue}], interval= [{interval}], duration= [{duration}], band= [{band}]
Description	This event occurs when the controller sends a forward footfall request to the AP on its reconnection to the controller.

{produce.short.name} received unrecognized request

Table 516. {produce.short.name} received unrecognized request event

Event	{produce.short.name} received unrecognized request
Event Type	scgLBSRcvdUnrecognizedRequest
Event Code	734
Severity	Warning
Attribute	"ctrlBladeMac"="xx:xx:xx:xx:xx:xx", "type"="", "length"="", "SCGMgmtIp"=""
Displayed on the web interface	{produce.short.name} [{SCGMgmtIp}] received Unrecognized: length =[{length}]
Description	This event occurs when the controller receives an unrecognized request.

FTP transfer

Table 517. 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 518. 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"

Table 518. FTP transfer error event

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 519. File upload event

Event	File upload
Event Type	fileUpload
Event Code	980
Severity	Informational
Attribute	“ip”=”xxx.xxx.xxx.xxx”,“cause”=”xxxxx”
Displayed on the web interface	Backup file [{cause}] uploading from [{ip}] failed
Description	This event occurs when the backup file upload fails.

Email sent successfully

Table 520. Email sent successfully event

Event	Email sent successfully
Event Type	mailSendSuccess
Event Code	981
Severity	Informational
Attribute	"srcProcess"="xxxxx", "receiver"= "xxxxx", "nodeMac"="xxxxx","nodeName"="xxxxx","tenantUUID"="xxxxx"
Displayed on the web interface	[{srcProcess}] sent email to [{receiver}] successfully.
Description	This event occurs when system sends mail successfully.

Email sent failed

Table 521. 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 522. SMS sent successfully event

Event	SMS sent successfully
Event Type	smsSendSuccess
Event Code	983
Severity	Informational
Attribute	"srcProcess"="xxxxx","receiver"= "xxxxx", "nodeMac"="xxxxx","nodeName"="xxxxx","tenantUUID"="xxxxx"
Displayed on the web interface	[{srcProcess}] sent short message to [{receiver}] successfully.
Description	This event occurs when system sends the short message successfully.

SMS sent failed

Table 523. SMS sent failed event

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

Process restart

Table 524. Process restart event

Event	Process restart
Event Type	processRestart
Event Code	1001
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[{processName}] process got re-started on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when any process crashes and restarts.

Service unavailable

Table 525. Service unavailable event

Event	Service unavailable
Event Type	serviceUnavailable
Event Code	1002
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[{processName}] process is not stable on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the process repeatedly restarts and is unstable.

Keepalive failure

Table 526. Keepalive failure event

Event	Keepalive failure
Event Type	keepAliveFailure
Event Code	1003
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] on {produce.short.name} [{SCGMgmtIp}] restarted [{processName}] process.
Description	This event occurs when the *mon/nc* restarts the process due to a keep alive failure.

Resource unavailable

Table 527. Resource unavailable event

Event	Resource unavailable
Event Type	resourceUnavailable
Event Code	1006
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=“radiusd”, “realm”=”NA”, ”SCGMgmtIp”=“3.3.3.3’, “cause”=“xx”
Displayed on the web interface	System resource [{cause}] not available in [{srcProcess}] process at {produce.short.name} [{SCGMgmtIp}]
Description	This event is generated due to unavailability of any other system resource, such as memcached.

HIP started

NOTE: This event is not applicable for vSZ-H.

Table 528. HIP started event

Event	HIP started
Event Type	hipStarted
Event Code	1014
Severity	Informational
Attribute	“ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP”, "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	[{srcProcess}] process gets Started on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged by starting the host identify protocol (HIP) instance. This event is included in the control plane identifier and the status of the node is active/ standby.

HIP stopped

NOTE: This event is not applicable for vSZ-H.

Table 529. HIP stopped event

Event	HIP stopped
Event Type	hipStopped
Event Code	1015
Severity	Informational
Attribute	“ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102”
Displayed on the web interface	[{srcProcess}] process stopped HIP on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when HIP is stopped by the monitor.

HIP failed over

NOTE: This event is not applicable for vSZ-H.

Table 530. HIP failed over event

Event	HIP failed over
Event Type	hipFailover
Event Code	1016
Severity	Major
Attribute	"ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102"
Displayed on the web interface	[{srcProcess}] Node transitioned to Active on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the standby HIP transits to an active mode and includes the control plane identifier of the newly active HIP.

Standby HIP restarted

NOTE: This event is not applicable for vSZ-H.

Table 531. Standby HIP restarted event

Event	Standby HIP restarted
Event Type	hipStandbyRestart
Event Code	1017
Severity	Informational
Attribute	“ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102”
Displayed on the web interface	[{srcProcess}] Standby HIP node failed detected from Active {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the active node detects failure of the standby node.

HIP cache cleaned

NOTE: This event is not applicable for vSZ-H.

Table 532. HIP cache cleaned event

Event	HIP cache cleaned
Event Type	hipCacheCleanup
Event Code	1018
Severity	Informational
Attribute	“ctrlBladeMac"="50:A7:33:24:E7:90", "srcProcess"="HIP", "realm"="NA", "processName"="HIP", "SCGMgmtIp"="100.13.0.102", mvnoId="12", hlrProfileName="HLR1",
Displayed on the web interface	[{srcProcess}] Cache cleanup started on {produce.short.name} [{SCGMgmtIp}]
Description	This event is generated when the cache cleanup process is completed.

Diameter initialization error

NOTE: This event is not applicable for vSZ-H.

Table 533. Diameter initialization error event

Event	Diameter initialization error
Event Type	dialnitilizeErr
Event Code	1401
Severity	Critical
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”srcProcess”=“<Application Name>“ “realm”=“ruckus.com”,”originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”desc” = “Diameter Stack Initialization Failure on {produce.short.name}”
Displayed on the web interface	[{srcProcess}] Diameter Stack Initialization Failure on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs due to stack initialization failure.

Diameter initialization

NOTE: This event is not applicable for vSZ-H.

Table 534. Diameter initialization event

Event	Diameter initialization
Event Type	dialnitialization
Event Code	1402
Severity	Debug
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,”originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”desc” = “Diameter Stack Initialization is Successful”
Displayed on the web interface	[{srcProcess}] Diameter Stack up and running on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs due to diameter stack is up and running.

Diameter peer transport failure

NOTE: This event is not applicable for vSZ-H.

Table 535. Diameter peer transport failure event

Event	Diameter peer transport failure
Event Type	diaPeerTransportFailure
Event Code	1403
Severity	Major
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,”originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerIp” = “3.3.3.3”,”peerName” = “OCS1”,”peerRealmName” = “operator.com”,”desc” = “Failed to read from peer socket”
Displayed on the web interface	[{srcProcess}] Failed to read from peer [{peerName}] Transport Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the transport with the peer is down and the stack fails to read the data.

Diameter CER error

NOTE: This event is not applicable for vSZ-H.

Table 536. Diameter CER error event

Event	Diameter CER error
Event Type	diaCERError
Event Code	1404
Severity	Critical

Table 536. Diameter CER error event

Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff “,”mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,“originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerIp” = “3.3.3.3”,”peerName” = “OCS1”,”peerRealmName” = “operator.com”,”desc” = “Failed to decode CER from Peer”
Displayed on the web interface	[{srcProcess}] Failed to decode CER from Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the diameter stack fails to decode the capabilities exchange request (CER) received from peer.

Diameter CER success

NOTE: This event is not applicable for vSZ-H.

Table 537. Diameter CER success event

Event	Diameter CER success
Event Type	diaCERSuccess
Event Code	1405
Severity	Debug
Attribute	”ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”, “mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,”originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerIp” = “3.3.3.3”,”peerName” = “OCS1”,”peerRealmName” = “organization.com”,”desc” = “Successfully decoded CER received from Peer”
Displayed on the web interface	[{srcProcess}] CER Success From Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the CER received from peer is successfully decoded.

Diameter invalid version

NOTE: This event is not applicable for vSZ-H.

Table 538. Diameter invalid version event

Event	Diameter invalid version
Event Type	diaInvalidVer
Event Code	1406
Severity	Warning
Attribute	”ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”, “mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “src Process”=“<Application Name>“,”realm”=“ruckus.com”,”originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerIp” = “3.3.3.3”,”peerName” = “OCS1”,”peerRealmName” = “organization.com”,”desc” = “Invalid version in Diameter header of received CER from peer”
Displayed on the web interface	[{srcProcess}] Invalid version in Diameter header in CER from Peer [{peerName}], Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the version in the diameter header of received CER is invalid.

Diameter peer add error

NOTE: This event is not applicable for vSZ-H.

Table 539. Diameter peer add error event

Event	Diameter peer add error
Event Type	diaPeerAddError
Event Code	1407
Severity	Critical

Table 539. Diameter peer add error event

Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerIp” = “3.3.3.3” “peerName” = “OCS1” “peerRealmName” = “organization.com” “desc” = ”Failed to add Peer” “appropriate cause”
Displayed on the web interface	[{srcProcess}] Failed to add Peer [{peerName}], Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the diameter stack fails to add a peer to the peer table.

Diameter peer add successful

NOTE: This event is not applicable for vSZ-H.

Table 540. Diameter peer add successful event

Event	Diameter peer add successful
Event Type	diaPeerAddSuccess
Event Code	1408
Severity	Debug
Attribute	”ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,“originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerIp” = “3.3.3.3”,”peerName” = “OCS1”,”peerRealmName” = “organization.com”,”desc” = “Peer addition successful”
Displayed on the web interface	[{srcProcess}] Peer [{peerName}] Realm [{peerRealmName}] addition is successful on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the peer addition is successful.

Diameter peer remove successful

NOTE: This event is not applicable for vSZ-H.

Table 541. Diameter peer remove successful event

Event	Diameter peer remove successful
Event Type	diaPeerRemoveSuccess
Event Code	1409
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerIp” = “3.3.3.3” “peerName” = “OCS1” “peerRealmName” = “organization.com”“desc” = ”Peer removal success”
Displayed on the web interface	[{srcProcess}] Peer [{peerName}] Realm [{peerRealmName}] removal is successful on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the peer is removed successfully from the table. The remote peer sends a diameter disconnect peer request (DPR) with the cause of not wanting to talk. In such instances, the peer is removed from the table.

Diameter realm entry error

NOTE: This event is not applicable for vSZ-H.

Table 542. Diameter realm entry error event

Event	Diameter realm entry error
Event Type	diaRealmEntryErr
Event Code	1410
Severity	Major

Table 542. Diameter realm entry error event

Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerRealmName” = “organization.com” “peerName” = “OCS1” “desc” = ”Failed to add route for Realm”
Displayed on the web interface	[{srcProcess}] Failed to add route for Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs due to realm route entry add error. This may arise when the realm entry exists and another realm entry is added. Creating two diameter services with same realm name causes this problem.

Diameter failover to alternate peer

NOTE: This event is not applicable for vSZ-H.

Table 543. Diameter failover to alternate peer event

Event	Diameter fail over to alternate peer
Event Type	diaFailOverToAltPeer
Event Code	1411
Severity	Major
Attribute	“ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,“originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerName”=“OCS1”,”peerRealmName” = “Vodafone.com”,”altPeerName” = “OCS2”,”altPeerRealmName” = “india.internal.net”“desc” = “Fwd to alt peer”
Displayed on the web interface	[{srcProcess}] Fwd from Peer [{peerName}] to AltPeer [{altPeerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs due to retransmission to an alternate peer.

Diameter fail back to peer

NOTE: This event is not applicable for vSZ-H.

Table 544. Diameter fail back to peer event

Event	Diameter fail back to peer
Event Type	diaFailbackToPeer
Event Code	1412
Severity	Major
Attribute	”ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, “srcProcess”=“<Application Name>“,”realm”=“ruckus.com”,“originHost” = “Node1”,”SCGMgmtIp”=“2.2.2.2”,”peerName”=“OCS1”, “peerRealmName” = “Vodafone.com”,”altPeerName” = “OCS2”,”altPeerRealmName” = “india.internal.net”,”desc” = “Failback to main peer”
Displayed on the web interface	[{srcProcess}] Failback to Main Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs due to retransmission to the main peer in case of a fail back.

Diameter CEA unknown peer

NOTE: This event is not applicable for vSZ-H.

Table 545. Diameter CEA unknown peer event

Event	Diameter CEA unknown peer
Event Type	diaCEAUnknownPeer
Event Code	1414
Severity	Critical

Table 545. Diameter CEA unknown peer event

Attribute	”ctrlBladeMac”=“aa:bb:cc:dd:ee:ff”,”mvnoId”=“839f87c6-d116-497e-afce-aa8157abd30c”, srcProcess”=“SessMgr”, ”realm”=“ruckus.com”,“originHost” = “Node1”,” SCGMgmtIp”=“2.2.2.2”,”peerName”=“OCS8”,”peerRealmName” = “Vodafone.com”,”desc” = “CEA received from Unknown peer
Displayed on the web interface	[{srcProcess}] CEA received from Unknown Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs due when the capabilities exchange answer (CEA) is received from an unknown peer.

Diameter no common application

NOTE: This event is not applicable for vSZ-H.

Table 546. Diameter no common application event

Event	Diameter no common application
Event Type	diaNoCommonApp
Event Code	1415
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “mvnoId”=12 “srcProcess”=”<Application Name>” “realm”=”ruckus.com" “originHost” = “Node1” "SCGMgmtIp"="2.2.2.2" “peerName”=ÖCS1 “peerRealmName” = “organization.com”“desc” = “No common App with peer”
Displayed on the web interface	[{srcProcess}] No common App with Peer [{peerName}] Realm [{peerRealmName}] on {produce.short.name} [{SCGMgmtIp}]
Description	This event occurs when the common application is not with the peer.

ZD AP migrating

Table 547. ZD AP migrating event

Event	ZD AP migrating
Event Type	zdAPMigrating
Event Code	2001
Severity	Informational
Attribute	“apMac”=“ C0:C5:20:12:2B:2C “, “serialNumber”=“501003003033”, “model”=“ZF7962”, “firmware”=“3.0.0.0.0”
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is upgrading with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP is upgrading with the controller AP firmware image.

ZD AP migrated

Table 548. 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"="ZF7962", “firmware”=”3.0.0.0.0”
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] has been upgraded with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP has upgraded its firmware with the controller AP firmware image.

ZD AP rejected

Table 549. ZD AP rejected event

Event	ZD AP rejected
Event Type	zdAPRejected
Event Code	2003
Severity	Warning
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="ZF7962"
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is not being upgraded with {produce.short.name} AP firmware because of ACL setting.
Description	This event occurs when the ZoneDirector AP is not upgraded with the controller AP firmware because of ACL setting.

ZD AP migration failed

Table 550. ZD AP migration failed event

Event	ZD AP migration failed
Event Type	zdAPMigrationFailed
Event Code	2004
Severity	Major
Attribute	“apMac”=“ C0:C5:20:12:2B:2C “, “serialNumber”=“501003003033”, “model”=“ZF7962”, “firmware”=“3.0.0.0.0”
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is failed to upgrade with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when the Zone Director AP fails to upgrade with the controller AP firmware image.

Database error

Table 551. Database error event

Event	Database error
Event Type	cassandraError
Event Code	3001
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, "SCGMgmtIp"="2.2.2.2", reason="reason",
Displayed on the web interface	Database internal error on node [{nodeName}], reason: [{reason}].
Description	This event occurs due to internal errors on the database.

Process initiated

NOTE: This event is not applicable for vSZ-H.

Table 552. Process initiated event

Event	Process initiated
Event Type	processInit
Event Code	5001
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process got re-started on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when PMIPv6 process crashes and restarts.

PMIPv6 unavailable

NOTE: This event is not applicable for vSZ-H.

Table 553. PMIPv6 unavailable event

Event	PMIPv6 unavailable
Event Type	pmipUnavailable
Event Code	5002
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	PMIPv6 process is not stable on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the PMIPv6 process repeatedly restarts and is not stable.

Memory allocation failed

NOTE: This event is not applicable for vSZ-H.

Table 554. Memory allocation failed event

Event	Memory allocation failed
Event Type	unallocatedMemory
Event Code	5003
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, "SCGMgmtIp"="2.2.2.2"
Displayed on the web interface	Insufficient Heap Memory in PMIPv6 process at {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the memory allocation fails in the PMIPv6 process.

Process stopped

NOTE: This event is not applicable for vSZ-H.

Table 555. Process stopped event

Event	Process stopped
Event Type	processTerminated
Event Code	5100
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “SCGMgmtIp”=”2.2.2.2”,
Displayed on the web interface	PMIPv6 process stop on {produce.short.name} [{SCGMgmtIp}]
Description	This event is logged when the PMIPv6 process stops

NOTE: Refer to System Alarms.

Threshold Events

Following are the events related to threshold system set.

- CPU threshold exceeded
- Memory threshold exceeded
- Disk usage threshold exceeded
- CPU threshold back to normal
- Memory threshold back to normal
- Disk threshold back to normal
- License threshold exceeded
- 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 556. CPU threshold exceeded event

Event	CPU threshold exceeded
Event Type	cpuThresholdExceeded
Event Code	950
Severity	Critical
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	CPU threshold [{perc}%] exceeded on control plane [{nodeName}-C]
Description	This event occurs when the CPU usage exceeds the threshold limit of 80%.
Auto Clearance	This event triggers the alarm 950, which is auto cleared by the event code 954.

Memory threshold exceeded

Table 557. Memory threshold exceeded event

Event	Memory threshold exceeded
Event Type	memoryThresholdExceeded
Event Code	951
Severity	Critical
Attribute	“nodeName”=”xxx”,“nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This event occurs when the memory usage exceeds the threshold limit of 85%.
Auto Clearance	This event triggers the alarm 951, which is auto cleared by the event code 955.

Disk usage threshold exceeded

Table 558. 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%.

CPU threshold back to normal

Table 559. 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 560. 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 561. 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 561. Disk threshold back to normal event

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

License threshold exceeded

Table 562. 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 equipments attached to the system haves exceeded the license limit.

Rate limit threshold surpassed

Table 563. Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "UserName"=abc@xyz.com "realm"="wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]

Table 563. Rate limit threshold surpassed event

Description	This event occurs when the rate limit threshold is surpassed. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds the limit of 701.

Rate limit threshold restored

Table 564. Rate limit threshold restored event

Event	Rate limit threshold restored
Event Type	rateLimitThresholdRestored
Event Code	1301
Severity	Informational
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "UserName"=abc@xyz.com "realm"="wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold restored for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is restored. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server is lesser or equal to 700.

Rate limit for TOR surpassed

Table 565. Rate limit for TOR surpassed event

Event	Rate limit for TOR surpassed
Event Type	rateLimitMORSurpassed
Event Code	1302
Severity	Critical
Attribute	"mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "UserName"=abc@xyz.com "realm"="wlan.3gppnetwor" "SCGMgmtIp"="2.2.2.2" "aaaSrvrIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "ueMacAddr"="aa:bb:cc:gg:hh:ii" "MOR"=1000,"THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This event occurs when the rate limit for maximum outstanding requests (MOR) is surpassed. The threshold limit for this event is dependent on the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds 1000.
Auto Clearance	This event triggers the alarm1302, which is auto cleared by the event code 1301.

The number of users exceed its limit

Table 566. The number of users exceed its limit event

Event	The number of users exceed its limit
Event Type	tooManyUsers
Event Code	7001
Severity	Major
Attribute	No attributes for this event.

Table 566. The number of users exceed its limit event

Displayed on the web interface	The number of users exceeded its limit.
Description	This event occurs when the number of users exceeds the specified limit. The threshold limit for SCG-200 and vSZ-H is 950000.
Auto Clearance	Alarm code 7003, which is auto cleared by this event code.

The number of devices exceeded its limit

Table 567. The number of devices exceeded its limit event

Event	The number of devices exceeded its limit
Event Type	tooManyDevices
Event Code	7002
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	The number of devices exceeded its limit
Description	This event occurs when the number of devices exceeds the specified limit. The threshold limit for SCG-200 and vSZ-H is 2850000.
Auto Clearance	Alarm code 7004, which is auto cleared by this event.

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 568. Data plane accepted a tunnel request event

Event	Data plane accepted a tunnel request
Event Type	dpAcceptTunnelRequest
Event Code	601
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “apMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 569. Data plane rejected a tunnel request event

Event	Data plane rejected a tunnel request
Event Type	dpRejectTunnelRequest
Event Code	602
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “apMac”=”xx:xx:xx:xx:xx:xx”, “reason”=”xxxxxxxxxxxx”
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 570. Data plane terminated a tunnel event

Event	Data plane terminated a tunnel
Event Type	dpTearDownTunnel
Event Code	603
Severity	Informational
Attribute	“dpMac”=”xx:xx:xx:xx:xx:xx”, “apMac”=”xx:xx:xx:xx:xx:xx”, “reason”=”xx”
Displayed on the web interface	Data plane [{dpName||dpMac}] terminated a tunnel from AP [{apName&&apMac}]. Reason: [{reason}]
Description	This event occurs when the data plane terminates a tunnel from the AP.
Auto Clearance	This event triggers the alarm 603, which is auto cleared by the event code 627.

AP created a tunnel

Table 571. 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 572. 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.
Auto Clearance	This event triggers the alarm 610, which is auto cleared by the event code 608.

AP softGRE tunnel fails over primary to secondary

Table 573. AP softGRE tunnel fails over primary to secondary event

Event	AP softGRE tunnel fails over primary to secondary
Event Type	apSoftGRETunnelFailoverPtoS
Event Code	611
Severity	Warning
Attribute	“apMac"="xx:xx:xx:xx:xx:xx", "primaryGRE"="xxx.xxx.xxx.xxx", "secondaryGRE"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] fails over from primaryGRE [{primaryGRE}] to secondaryGRE[{secondaryGRE}].
Description	This event occurs when AP moves from a primary to a secondary GRE.

AP softGRE tunnel fails over secondary to primary

Table 574. 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 AP moves from a secondary to a primary GRE.

AP softGRE gateway reachable

Table 575. AP softGRE gateway reachable event

Event	AP softGRE gateway reachable
Event Type	apSoftGREGatewayReachable
Event Code	613
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softgreGW"="xxx.xxx.xxx.xxx", "softgreGWAddress"="xxxx"
Displayed on the web interface	AP [{apname&&apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully
Description	This event occurs when AP builds a soft GRE tunnel successfully.

AP softGRE gateway not reachable

Table 576. AP softGRE gateway not reachable event

Event	AP softGRE gateway not reachable
Event Type	apSoftGREGatewayNotReachable
Event Code	614
Severity	Critical
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "softGREGatewayList"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach the following gateways: [{softGREGatewayList}].
Description	This event occurs when AP fails to build a soft GRE tunnel either on the primary or the secondary GRE.
Auto Clearance	This event triggers the alarm 614, which is auto cleared by the event code 613.

Data plane set up a tunnel

NOTE: This event is not applicable for vSZ-H.

Table 577. Data plane set up a tunnel event

Event	Data plane set up a tunnel
Event Type	dpSetUpTunnel
Event Code	627
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Data plane [{dpName||dfpMac}] set up a tunnel from AP [{apName&&apMac}].
Description	This event occurs when the data plane sets up a tunnel from the AP.

AP secure gateway association success

Table 578. 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 579. AP is disconnected from secure gateway event

Event	AP is disconnected from secure gateway
Event Type	ipsecTunnelDisassociated
Event Code	661
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","ipsecGWAddress"="x.x.x.x"
Displayed on the web interface	AP [{apName&&apMac}] is disconnected from secure gateway [{ipsecGWAddress}].
Description	This event occurs when the AP is disconnected from secure gateway.

AP secure gateway association failure

Table 580. 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

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

- DP softGRE GW unreachable
- DP softGRE keepalive timeout
- DP softGRE GW inactive
- DP DHCPRelay no resp
- DP DHCPRelay failOver
- DP softGRE new tunnel
- DP softGRE del tunnel
- DP softGRE keepalive recovery
- DP DHCPRelay response recovery
- DP softGRE GW reachable
- DP softGRE GW active
- DP softGRE GW failover

DP softGRE GW unreachable

Table 581. DP softGRE GW unreachable event

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

DP softGRE keepalive timeout

Table 582. DP softGRE keepalive timeout event

Event	DP softGRE keepalive timeout
Event Type	dpSgreKeepAliveTimeout
Event Code	616
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 softGRE GW inactive

Table 583. DP softGRE GW inactive event

Event	DP softGRE GW inactive
Event Type	dpSgreGWInact
Event Code	617
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "GatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 resp

Table 584. DP DHCPRelay no resp event

Event	DP DHCPRelay no resp
Event Type	dpDhcpRelayNoResp
Event Code	618
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 585. DP DHCPRelay failOver event

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

DP softGRE new tunnel

Table 586. DP softGRE new tunnel event

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

DP softGRE del tunnel

Table 587. DP softGRE del tunnel event

Event	DP softGRE del tunnel
Event Type	dpSgreDelTunnel
Event Code	621
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", “greType”=”L2oGRE, L3oGRE", "apIpAddress"="x.x.x.x"
Displayed on the web interface	Dataplane [{dpName||dpMac}] lost a [{greType}] tunnel connection to AP[{apIP}].
Description	This event occurs when access tunnel is disconnected due to a timeout.

DP softGRE keepalive recovery

Table 588. DP softGRE keepalive recovery event

Event	DP softGRE keepalive recovery
Event Type	dpSgreKeepAliveRecovery
Event Code	622
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName||dpMac}] 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 589. DP DHCPRelay response recovery event

Event	DP DHCPRelay response recovery
Event Type	dpDhcpRelayRespRecovery
Event Code	623
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName||dpMac}] detected DHCP server [{dhcpIP}] is now responsive
Description	This event occurs when the DHCP server resumes answering the relay request from data plane.

DP softGRE GW reachable

Table 590. DP softGRE GW reachable event

Event	DP softGRE GW reachable
Event Type	dpSgreGWReachable
Event Code	624
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName||dpMac}] detected Core Gateway [{gatewayIP}] is now reachable
Description	This event occurs when the core gateway is reachable.

DP softGRE GW active

Table 591. DP softGRE GW active event

Event	DP softGRE GW active
Event Type	dpSgreGWAct
Event Code	625
Severity	Informational
Attribute	"dpMac"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName||dpMac}] detected [{gatewayIP}] is now active
Description	This event occurs when the core gateway changes to an active mode.

DP softGRE GW failover

Table 592. DP softGRE GW failover event

Event	DP softGRE GW failover
Event Type	dpSgreGWFailOver
Event Code	626
Severity	Informational
Attribute	“dpMac”=“xx:xx:xx:xx:xx:xx“, “preGatewayIp”=“x.x.x.x”, “curGatewayIP”=“x.x.x.x”
Displayed on the web interface	Data plane [{dpName/dpMac}] switched over from CoreGateway[{preGatewayIP}] to CoreGateway[{curGatewayIP}].
Description	This event occurs when the data plane switches to the other gateway due to failover threshold limit.

NOTE: Refer to Tunnel Alarms - Access Point.

Index

Numerics

3rd party access point 161
3rd Party Access Point Events 161
3rd party AP connected 161
3rd party client authorization 242
3rd party client authorization failure 242
3rd party client inactivity timeout 241
3rd party client join 241
3rd party client roaming 243
3rd party client session expiration 243
3rd party client session logout 244
3rdPartyAPConnected 161
3rdPtyClientAuthorization 242
3rdPtyClientAuthorizationFailure 242
3rdPtyClientInactivityTimeou 241
3rdPtyClientJoin 241
3rdPtyClientRoaming 243
3rdPtyClientSessionExpiration 243
3rdPtyClientSessionLogout 244

A

accFailedOverToSecondary 63, 167
accFallbackToPrimary 63, 168
accounting alarms 62
accounting failed over to secondary 167
accounting failover to secondary 63
accounting fallback to primary 63, 168
accounting server not reachable 62, 166
accounting session disabled 164
accounting session interim failed 166
accounting session start failed 163
accounting session started 162
accounting session stopped failed 165
accounting session stopped successfully 164
accSessDisabled 164
accSessInterimFail 166
accSessStarted 162
accSessStartFailed 163
accSessStopFail 165
accSessStopSucc 164
accSrvrNotReachable 62, 166
ad-hoc network device 188
ad-hoc-networkRogueAPDetecte 188
alarm 56, 57
alarm and event management 56
ap account message drop while no accounting start message 66, 173
ap accounting message decode failed 65, 170
ap accounting message mandatory parameter missing 64, 169
ap accounting response while invalid config 172
ap accounting retransmission message dropped 171
AP brownout 210
ap cable modem interface down 77, 210
ap cable modem power-cycled by user 210
ap cable modem set to factory default by user 215
ap cable modem soft-rebooted by user 214
ap capacity reached 213
ap capacity recovered 213
ap certificate expired 93, 269
ap certificate updated 270
ap change control plane 208
ap channel updated 206
ap channel updated dfs detected a radar 207
ap clb limit reached 211
ap clb limit recovered 212
ap communication alarms 68
ap communication events 178, 216
ap configuration update failed 69, 183
ap configuration updated 182
ap connected 208
ap connected to ls 190
ap country code updated 207
ap created a tunnel 392
ap deleted 76, 208
ap disconnected 76, 205
ap discovery succeeded 179
AP failed to connect to LS 74
ap failed to connect to ls 191
ap firmware update failed 70, 181

ap firmware updated 180
ap heartbeat lost 209
ap illegal to change country code 185
ap ip address updated 206
ap is disconnected from secure gateway 158, 396
ap join zone failed 72, 185
ap managed 179
ap mesh events 194
ap pre-provision model mismatched 70, 183
ap rebooted by system 75, 205
ap rebooted by user 204
ap received passive calibration request 192
ap received passive footfall request 193
AP received unrecognized request 193
ap rejected 68, 180
ap reset to factory default 206
ap secure gateway association failure 396
ap secure gateway association success 395
ap smart monitor turn off wlan 211
ap softgre gateway not reachable 158, 394
ap softgre gateway reachable 394
ap softgre tunnel fails over primary to secondary 393
ap softgre tunnel fails over secondary to primary 393
ap started location service 191
ap state change alarms 75
ap state change events 204
ap stopped location service 192
ap swap model mismatched 69, 184
ap tagged as critical 209
ap tunnel disconnected 392
ap USB software package download failed 216
ap USB software package downloaded 216
ap WLAN oversubscribed 71
ap wlan oversubscribed 184
ap wlan state changed 212
apAcctMsgDecodeFailed 170
apAcctMsgDropNoAcctStartMsg 66, 173
apAcctMsgMandatoryPrmMissing 64, 169
apAcctRespWhileInvalidConfig 172
apAcctRetransmittedMsgDropped 171
apBrownout 210
apBuildTunnelSuccess 392
apCapacityReached 213
apCapacityRecovered 213
apCertificateExpire 93, 269
apCertificateExpireClear 270
apChangeControlBlade 208
apChannelChanged 206
apCLBlimitReached 211
apCLBlimitRecovered 212
apConfApplying 182
apConfUpdated 182
apConfUpdateFailed 69, 183
apConnected 208
apCountryCodeChanged 207
apDeleted 208
apDfsRadarEvent 207
apDiscoverySuccess 179
apFirmwareApplying 181
apFirmwareUpdated 180
apFirmwareUpdateFailed 70, 181
apHeartbeatLost 209
apIllgalToChangeCountryCode 185
apIPChanged 206
apJoinZoneFailed 72, 185
apLBSAuthFailed 73, 190
apLBSConnectFailed 74, 191
apLBSConnectSuccess 190
apLBSNoResponses 73, 189
apLBSRcvdPassiveCalReq 192
apLBSRcvdPassiveFFReq 193
apLBSRcvdUnrecognizedRequest 193, 339
apLBSStartLocationService 191
apLBSStopLocationService 192
apModelDiffWithPreProvConfig 70, 84, 183, 252
apModelDiffWithSwapOutAP 69, 184
apP cable modem interface up 214
app server active 311
app server down 112, 310
app server inactive 112, 310
appServerActive 311
appServerDown 112, 310
appServerInactive 112, 310
apRebootBySystem 75, 205
apSoftGREGatewayNotReachable 158, 394
apSoftGREGatewayReachable 394

apSoftGRETunnelFailoverPtoS 393
apSoftGRETunnelFailoverStoP 393
apStatusManaged 179
apStatusRejected 68, 180
apTaggedAsCritical 209
apTunnelDisconnected 392
apUsbSoftwarePackageDownloaded 216
apUsbSoftwarePackageDownloadFailed 216
apWlanOversubscribed 71, 184
apWLANStateChanged 212
assocDown 114, 312
assocEstbFailed 113, 311
associated PDNGW down 302
associated pdngw down 105
association down 114, 312
association establishment failed 113, 311
association up 312
assocUp 312
auth info sending failed 313
authentication alarms 78
authentication events 217
authentication failed 219
authentication failed over to secondary 79, 222
authentication fallback to primary 80, 223
authentication server not reachable 78, 217
authentication succeeded 218
authFailed 219
authFailedOverToSecondary 79, 222
authFallbackToPrimary 80, 223
authorization events 224
authSrvrNotReachable 78, 217
authSuccess 218
auto cleared 68, 69, 70, 74, 76, 77, 81, 82, 83, 84, 85, 86, 87, 88, 90, 91, 92, 93, 94, 95, 96, 99, 111, 112, 113, 114, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 130, 131, 132, 137, 140, 153, 154, 156, 157, 158, 159, 180, 181, 183, 191, 205, 210, 231, 250, 251, 252, 254, 256, 259, 260, 262, 266, 268, 269, 273, 277, 278, 280, 281, 282, 287, 309, 310, 311, 312, 319, 320, 321, 322, 323, 324, 325, 340, 342, 345, 356, 383, 384, 388, 389, 391, 392, 394, 396
aystem alarms 138

B

backupClusterFailed 85, 253
backupClusterSuccess 253
binding failed 132, 345
binding released 346
binding revoked 346
binding succeeded 344
binding time expired 345
bindingExpired 345
bindingFailure 345
bindingReleased 346
bindingRevoked 346
bindingSuccess 344

C

c2d configuration failed 234
c2dCfgFailed 234
cableModemDown 210
cableModemUp 214
cassandraError 380
cdr generation failed 101, 289
cdr transfer failed 100, 289
cdr transfer succeeded 288
cdrGenerationFailed 101
cdrTxfrFailed 100
ceate session response failed 106, 303
cfgRcvFailed 273
cfgUpdFailed 272
cfgUpdSuccess 272
cgf keep alive not responded 288
cgf server not configured 110, 307
cgfServerNotConfigured 110, 307
client authentication failed 236
client authorization failed 239
client authorization successfully 238
client blocked 245
client connection timed out 238
client disconnected 237
client events 235
client failed to join 237
client grace period 245
client joined 236
client logged out 240
client roaming 240
client roaming disconnected 244
client session expired 239
clientAuthFailure 236
clientAuthorization 238
clientAuthorizationFailure 239

clientBlockByDeviceType 245
clientDisconnect 237
clientGracePeriod 245
clientInactivityTimeout 238
clientJoin 236
clientJoinFailure 237
clientRoaming 240
clientSessionExpiration 239
clientSessionLogout 240
cluster application started 257
cluster application stopped 87, 256
cluster back in service 253
cluster backup completed 253
cluster backup failed 85, 253
cluster backup started 257
cluster created successfully 249
cluster events 249
cluster in maintenance state 84, 252
cluster leader changed 258
cluster node rebooted 89, 261
cluster node shut down 90
cluster node shutdown 262
cluster node upgrade completed 255
cluster out of service 91, 266
cluster remove node started 264
cluster restore completed 254
cluster restore failed 86, 254
Cluster upgrade failed 86
cluster upgrade failed 256
cluster upgrade started 258
cluster upload completed 263
cluster upload failed 264
cluster upload started 263
clusterAppStart 257
clusterAppStop 87, 256
clusterBackToInService 253
clusterBackupStart 257
clusterCfgBackupFailed 91, 268
clusterCfgBackupStart 267
clusterCfgBackupSuccess 268
clusterCfgRestoreFailed 92, 269
clusterCfgRestoreSuccess 268
clusterCreatedSuccess 249
clusterLeaderChanged 258
clusterOutOfService 91, 266
clusterUpgradeStart 258
cmRebootByUser 210
cmResetByUser 214
cmResetFactoryByUser 215
coA authorize only access reject 228
coA nack sent to AAA 227
coA NAK received NAS 228
coA received from AAA 226
coA RWSG MWSG notification failure 229
coA sent NAS 227
coaAuthorizeOnlyAccessReject 228
coaNackSntAAA 227
coaNakRcvdNas 228
coaRcvdAAA 226
coaRWSGMWSGNotifFailure 229
coaSentNas 227
config update failed 129, 339
Configuration backup failed 91
configuration backup failed 268
configuration backup started 267
configuration backup succeeded 268
configuration events 272
configuration receive failed 273
configuration restore failed 92, 269
configuration restore succeeded 268
configuration update failed 272
configuration updated 272
configuration-change events 56
connect To DHCP 341
connected to LS 355
connectedToDblade 230
connectedToDHCP 341
connection to cgf failed 99, 287
control and data plane 81, 230
cpu threshold back to normal 385
cpu threshold exceeded 153, 383
cpuThresholdBackToNormal 385
cpuThresholdExceeded 153, 383

D

data plane 94, 275
data plane accepted a tunnel request 390
data plane configuration update failed 94, 277
data plane configuration updated 276
data plane connected 280
data plane core dead 97, 283
data plane disconnected 95, 280
data plane discovered 275
data plane discovery failed 276
data plane heartbeat lost 277
data plane ip address updated 278
data plane packet pool is above high water mark 283

data plane packet pool is under critical low water mark 97, 282
data plane packet pool is under low water mark 96, 282
data plane physical interface down 95, 281
data plane physical interface up 281
data plane process restarted 98, 284
data plane rebooted 96, 277
data plane rejected a tunnel request 391
data plane set up a tunnel 395
data plane softgre gw unreachable 397
data plane statistics update failed 279
data plane status update failed 279
data plane terminated a tunnel 391
data plane updated to a new control plane 278
database error 380
datablade alarms 94
debug 57
decode failed 107, 304
delAllSess 344
delete all sessions 344
delete bearer request failed 109, 305
delete session response failed 108, 305
deleteBearerRequestFailed 109
deleteSessionResponseFailed 108
destAvailable 309
destination available 309
destination not reachable 111, 309
destNotReacheable 111
destNotRecheable 309
dhcp connection lost 131, 342
dhcp dcln received 286
dhcp events 285
dhcp inform received 285
diaCEAUnknownPeer 149, 376
diaCERError 144, 370
diaCERSuccess 371
diaFailbackToPeer 148, 376
diaFailOverToAltPeer 147, 375
diaInitialization 369
diaInitilizeErr 143, 369
diaInvalidVer 372
diameter CEA unknown peer 149, 376
diameter CER error 144, 370
diameter CER success 371
diameter fail back to peer 148, 376
diameter fail over to alternate peer 147, 375
diameter initialization 369
diameter initialization error 143, 369
diameter invalid version 372
diameter no common application 149, 377
diameter peer add error 145, 372
diameter peer add successful 373
diameter peer remove successful 146, 374
diameter peer transport failure 144, 370
diameter realm entry error 146, 374
diaNoCommonApp 149, 377
diaPeerAddError 145, 372
diaPeerAddSuccess 373
diaPeerRemoveSuccess 146, 374
diaPeerTransportFailure 144, 370
diaRealmEntryErr 146, 374
did allocation failure 115, 316
didAllocationFailure 115, 316
disk threshold back to normal 385
disk usage exceed threshold 90, 266
disk usage threshold exceeded 154, 384
diskUsageExceed 90, 266
diskUsageThresholdExceeded 154, 384
dm nack received from NAS 226
dm nack sent to AAA 225
dm received from AAA 224
dm sent to NAS 225
dmNackRcvdNAS 226
dmNackSntAAA 225
dmRcvdAAA 224
dmSntNAS 225
DP connected 230
dp DHCP relay no resp 399
dp dhcprelay failover 399
dp dhcprelay response recovery 401
dp disconnected 81, 231
dp softgre del tunnel 400
DP softGRE gw active 402
dp SoftGRE GW failover 403
dp SoftGRE GW inactive 398
dp softgre gw reachable 402
dp SoftGRE keepalive recovery 401
dp SoftGRE keepalive timeout 398
dp softGRE new tunnel 400
dpAcceptTunnelRequest 390
dpCoreDead 97, 283
dpDhcpRelayFailOver 399
dpDhcpRelayNoResp 399
dpDhcpRelayRespRecovery 401

dpDisconnected 95
dpPhyInterfaceDown 95
dpPktPoolCriticalLow 97, 282
dpPktPoolLow 96, 282
dpPktPoolRecover 283
dpProcessRestart 98, 284
dpReboot 96
dpRejectTunnelRequest 391
dpSetUpTunnel 395
dpSgreDelTunnel 400
dpSgreGWAct 402
dpSgreGWFailOver 403
dpSgreGWInact 398
dpSgreGWReachable 402
dpSgreGWUnreachable 397
dpSgreKeepAliveRecovery 401
dpSgreKeepAliveTimeout 398
dpSgreNewTunnel 400
dpTearDownTunnel 391
dpUpdateStatisticFailed 279

E

echo response not received 291
email sent failed 363
email sent successfully 362
emap downlink connected to map 194
emap downlink disconnected from map 195
emap uplink connected to map 195
emap uplink disconnected from map 196
emapDlinkConnectWithMap 194
emapDlinkDisconnectWithMap 195
emapUlinkConnectWithMap 195
emapUlinkDisconnectWithMap 196
entire cluster upgraded successfully 255
event 57
event attributes 57
event categories 56
event detail information 57
event severity 57
event source 57
event type 57

F

failed to connect to LS 140, 356
fast re-authentication failed 222
fast re-authentication succeeded 221
fastReauthFailed 222
fastReauthSuccess 221
file upload 362
fileUpload 362
force DHCP disconnected 248
forceDHCPDisconnect 248
forwarded calibration request to AP 360
forwarded footfall request to AP 360
ftp transfer 361
ftp transfer error 361
ftpTransfer 361
ftpTransferError 361

G

ga interface alarms 99
ga interface events 287
generation of event and alarm 57
genericRogueAPDetected 186
ggsn not reachable 103, 291
ggsn not resolved 103, 292
ggsn restarted 102, 290
ggsnNotReachable 103
ggsnNotResolved 103
ggsnRestarted 102
gn S2a interface alarms 102
gn S2a interface events 290
gprs location update failed 314
gprs location update succeeded 314
gr interface alarms 111
gr interface event 308

H

hIP cache cleaned 368
hIP failed over 142, 367
hip started 366
hip stopped 367
hipCacheCleanup 368
hipFailover 142, 150, 367, 380
hipStandbyRestart 368
hipStarted 366
hipStopped 367

I

incapable location info requested 338
incapableLocInfoRequested 338
incorrect flat file configuration 274
informational 57
insert sub data failed 315

insert sub data success 315
insertSubDataFailed 315
insertSubDataSuccess 315
ip assigned 299
ip not assigned 299
ipmi alarms 116
ipmi events 318
ipmiCurrent 124, 323
ipmiDrvStatus 126, 325
ipmiFan 123, 322
ipmiFanStatus 124, 324
ipmiPower 123, 323
ipmiPsStatus 125, 324
ipmiRECurrent 329
ipmiREDrvStatus 331
ipmiREFan 328
ipmiREFanStatus 330
ipmiREPower 329
ipmiREPsStatus 330
ipmiREThempBB 326
ipmiREThempFP 326
ipmiREThempHSBP 328
ipmiREThempIOH 326
ipmiREThempMemP 327
ipmiREThempP 328
ipmiREThempPS 327
ipmiREVotage 325
ipmiThempBB 118, 319
ipmiThempFP 119, 319
ipmiThempHSBP 122, 322
ipmiThempIOH 119, 320
ipmiThempMemP 120, 320
ipmiThempP 122, 321
ipmiThempPS 121, 321
ipmiVoltage 117, 318
ipmiVotage 117, 318
ipsecTunnelAssociated 395
ipsecTunnelAssociateFailed 396
ipsecTunnelDisassociated 158, 396

K

keepalive failure 141, 365
keepAliveFailure 141, 365

L

license data changed 336
license import failed 336
license import succeeded 335
license sync failed 335
license sync succeeded 334
license threshold exceeded 155, 386
licenseChanged 336
licenseImportFail 336
licenseImportSuccess 335
licenseSyncFail 335
licenseSyncSuccess 334
licenseThresholdExceeded 155, 386
licensing alarms 127
licensing interface events 332
lma failed over 130, 341
lMA ICMP is unreachable 340
lma icmp is unreachable 130
lma ICMP reachable 339
lMA server unreachable 340
lmaFailOver 130, 341
lmaHbUnreachable 340
lmaIcmpReachable 339
lmaIcmpUnreachable 130, 340
logging events 56
lostCnxnToDblade 81, 231
lostCnxnToDHCP 131, 342
LS authentication failure 73, 139
ls authentication failure 190, 355

M

MAC-spoofing rogue AP 187
mac-spoofingRogueAPDetected 187
mailSendFailed 363
mailSendSuccess 362
maliciousRogueAPTimeout 188
map disconnected 196
map downlink connected 196
map downlink connected to emap 197
map downlink connected to map 202
map downlink disconnected from emap 197
map downlink disconnected from map 203
map uplink connected to emap 198
map uplink connected to map 200
map uplink connected to rap 199
map uplink disconnected from emap 199
mapDisconnected 196
mapDlinkConnected 196
mapDlinkConnectWitheMap 197
mapDlinkConnectWithMap 202
mapDlinkDisconnectWitheMap 197

mapDlinkDisconnectWithMap 203
mapUlinkConnectToeMap 198
mapUlinkConnectToMap 200
mapUlinkConnectToRap 199
mapUlinkDisconnectToeMap 199
Memory allocation failed 152
memory allocation failed 381
memory threshold back to normal 385
memory threshold exceeded 154, 384
memoryThresholdBackToNormal 385
memoryThresholdExceeded 154, 384
Mesh state update to rap no channel 202
mesh state updated to map 200
mesh state updated to map no channel 201
mesh state updated to RAP 201
meshStateUpdateToMap 200
meshStateUpdateToMapNoChannel 201
meshStateUpdateToRap 201
meshStateUpdateToRapNoChannel 202
modify bearer response failed 107, 304
modifyBearerResponseFailed 107

N

new node failed to join 82, 250
new node joined successfully 250
newNodeJoinFailed 82, 250
newNodeJoinSuccess 250
No LS responses 73, 189
no LS responses 139
no ls responses 355
node back in service 265
node bond interface down 88, 259
node bond interface up 259
Node ip address changed 260
node out of service 84, 252
node physical interface down 88, 260
node physical interface up 261
node removal completed 251
node removal failed 83, 251
nodeBondInterfaceDown 88, 259
nodeBondInterfaceUp 259
nodeIPChanged 260
nodeOutOfService 84, 252
nodePhyInterfaceUp 261
nodeShutdown 90, 262
ntp time synchronized 262
ntpTimeSynched 262
number of devices exceeded it's limit 157
number of users exceeded it's limit 156

O

onboarding registration failed 246
onboarding registration succeeded 246
onboardingRegistrationFailure 246
onboardingRegistrationSuccess 246
outbound routing failure 114, 316
outboundRoutingFailure 114, 316
overview 56

P

pdf update success coa 300
pdngw could not be resolved 104, 301
pdngw version not supported 105, 302
pdnGwAssociationDown 105, 302
pdnGwNotResolved 104, 301
pdnGwVersionNotSupportedMsgReceived 105, 302
pdp context established 292
pdp delete by GGSN failed 298
pdp delete by GGSN succeeded 298
pdp delete by TTG failed 297
pdp delete by TTG succeeded 297
pdp update by GGSN failed 296
pdp update by GGSN succeeded 296
pdp update by HLR failed 294
pdp update by HLR succeeded 293
pdp update by roaming failed 295
pdp update by roaming succeeded 294
pdp update fail COA 301
pdpUpdFailCOA 301
pdpUpdSuccCOA 300
pmipUnavailable 151, 381
pMIPv6 unavailable 151, 381
process initiated 150, 380
process restart 140, 364
process stopped 382
processRestart 140, 364
pseudonym authentication failed 220
pseudonym authentication succeeded 219
pseudonymAuthFailed 220
pseudonymAuthSuccess 219

R

radius server reachable 175

radius server unreachable 175
rap downlink connected to map 198
rap downlink disconnected from map 203
rapDlinkConnectWithMap 198
rapDlinkDisconnectWithMap 203
rate limit for TOR surpassed 156, 388
rate limit threshold restored 387
rate limit threshold surpassed 386
rateLimitMORSurpassed 156, 388
rateLimitThresholdRestored 387
rateLimitThresholdSurpassed 386
received management request 358
received passive request 357
received unrecognized request 361
remediation failed 247
remediation succeeded 247
remediationFailure 247
remediationSuccess 247
removeNodeFailed 83, 251
removeNodeSuccess 251
resource unavailable 142, 366
resourceUnavailable 142, 366
restore data failed 317
restore data success 317
restoreClusterFailed 86, 254
restoreClusterSuccess 254
restoreDataFailed 317
restoreDataSuccess 317
resync NTP Time 265
retransmission exhausted 137, 353
retransmitExausted 137, 353
Rogue AP 186
rogue AP disappeared 188

S

same network rogue ap 187
same-networkRogueAPDetected 187
scg forwarded footfall request to AP 360
scgLBSAuthFailed 139, 355
scgLBSConnectFailed 140, 356
scgLBSConnectSuccess 355
scgLBSFwdPassiveCalReq 360
scgLBSFwdPassiveFFReq 360
scgLBSNoResponse 139, 355
scgLBSRcvdMgmtRequest 358
scgLBSRcvdUnrecognizedRequest 361
scgLBSSendAPInfobyVenueReport 358
scgLBSSendClientInfo 359
scgLBSSendVenuesReport 359
scgLBSSentControllerInfo 357
scgLBSStartLocationService 357
send auth info success 313
sendAuthInfoFailed 313
sendAuthInfoSuccess 313
sent AP info by venue report 358
sent associated client report 359
sent controller information report 357
sent query venues report 359
service unavailable 141, 365
serviceUnavailable 141, 365
sessDeletedAtDblade 232
sessDeleteErrAtDblade 233
session delete at DP failed 233
session deleted at DP 232
session interface events 343
session license exhausted 334
session timeout 343
session update at DP failed 232
session updated at DP 231
sessTimeout 343
sessUpdatedAtDblade 231
sessUpdateErrAtDblade 232
smartMonitorTurnOffWLAN 211
smartRoamDisconnect 244
sms sent failed 364
sms sent successfully 363
smsSendFailed 364
smsSendSuccess 363
ssh tunnel switched 264
ssid-spoofing rogue AP 186
ssid-spoofingRogueAPDetected 186
STA 352
sta authentication failed decode failure 135, 349
sta authentication failed failure response 134, 348
sta authentication failed transport down 133, 348
sta reauthorization failed 135, 352
sta reauthorization successful 351
sta response timer expired 136, 352
sta session termination AAA initiated failed 351
sta session termination AAA initiated success 350
sta session termination SCG initiated success 349
sta successful authentication 347
staAuthFailedDecodeFailure 135, 349

staAuthFailedFailureResp 134, 348
staAuthFailedTransDown 133, 348
standby HIP restarted 368
staReAuthFailed 135, 352
staReAuthSuccess 351
staResponseTimerExpired 136, 352
staSessionTermAAAInitFailed 351
staSessionTermAAAInitSucess 350
staSessionTermSCGInitSuccess 349
system interface events 354

T

threshold alarms 153
threshold events 383
threshold-crossing alerts 56
timestamp 57
tooManyUsers 156
ttg session critical threshold 127, 333
ttg session license exhausted 128
ttg session major threshold 333
ttg session warning threshold 332
ttgSessionCriticalThreshold 127, 333
ttgSessionLicenseExausted 128, 334
ttgSessionMajorThreshold 333
ttgSessionWarningThreshold 332
tunnel alarms 158
tunnel events - datablade 397

U

unallocatedMemory 152, 381
unauthorized COA/DM message dropped 174
unauthorized CoA/DM message dropped 67
unauthorizedCoaDmMessageDropped 67, 174
Unavailable location info requested 337
unavailableLocInfoRequested 337
unknown realm 170, 218
unknown ue 300
unknownRealm 218
unsupported location delivery request 338
unSupportedLocDeliveryRequest 338
update bearer request failed 109, 306
updateBearerRequestFailed 109
updateCfgFailed 129
updateGprsLocFailed 314
updateGprsLocSuccess 314
updating ap configuration 182
updating ap firmware 181
upgradeClusterFailed 86, 256
upgradeClusterNodeSuccess 255
upgradeEntireClusterSuccess 255

Z

zD AP Migrated 378
zd AP Migrating 378
ZD AP Migration Failed 379
zD AP Rejected 379
zdAPMigrated 378
zdAPMigrating 378
zdAPMigrationFailed 379
zdAPRejected 379

Copyright © 2006-2015. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com