MESSAGE REFERENCE GUIDE

Ruckus SmartZone 100 and Virtual SmartZone Essentials Alarm and Event Reference Guide, 5.1.2

Supporting SmartZone 5.1.2

Part Number: 800-72349-001 Rev A
Publication Date: August 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Document Conventions

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

TABLE 1 Text Conventions

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

Notes, Cautions, and Warnings

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

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

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

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

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

Command Syntax Conventions

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

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

Document Feedback

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

You can email your comments to Ruckus at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

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

For example:

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

Ruckus Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting Ruckus Customer Services and Support

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

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

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

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

About This Guide

Introduction

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

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

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

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

What's New in This Document

The following are the new events in 5.1.2 release.

- Event code 753 - system service failure
- Event code 99250 - remote administration
- Event code 99251 - remote administration

Terminology

Table 2 lists the terms used in this guide.

TABLE 2 Terms used

Term	Description
AAA	Authentication, Authorization, and Accounting
AP	Access Point
APN	Access Point Name
CDR	A formatted collection of information on chargeable events used for accounting and billing. For example, call set-up, call duration and amount of data transferred.
CLB	Client Load Balance
CNN	Configuration Change Notifier

TABLE 2 Terms used (continued)

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

Alarm and Event Management

Overview

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

NOTE
Refer to About This Guide on page 23 for the conventions used in this guide.

Alarm and Event Management

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

- Event Categories on page 25
- Event Attributes on page 26
- Generation of Alarm and Event on page 26

Event Categories

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

- Alarms: These are unexpected events indicating a condition that typically requires management attention
- Configuration Change Events: Configuration change events are events that inform of a configuration change effect on the device.
- Threshold Crossing Alerts: These are events that inform of a performance-related state variable that has exceeded a certain value. These events point to conditions that might require management attention to prevent network and service degradation.
- Logging Events: These are events that occur regularly and are expected to occur during the operation of a network, that indicate what is currently going on in the network. Some examples of these events include:
  - Activity on the network and service
  - Operator activity
  - System activity
  - Informational events – Any other kind of event.
  - Debug and Informational events - All the debug and informational events pertaining to TTG modules like RADIUS proxy, HIP, CIP and AUT are not displayed on the controller web interface. This is because it reduces the performance of the system since its large in numbers. Enabling display of these events on the controller web interface is possible through CLI but it is not recommended.

Event Attributes

An event always includes the following attributes:

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

Generation of Alarm and Event

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

1. Alarm
   a. An alarm is a persistent indication of a fault that clears only when the triggering condition had been resolved.
   b. An alarm can be filtered in the controller web interface based on:
      - Acknowledge Time: The time when the alarm is acknowledged
      - Date and Time - Date and time when the alarm is acknowledged
      - Severity: Severity is classified as critical, major or minor
      - Status - Could either be cleared or outstanding
      - Type - Alarm type
   c. To view the below alarm information in the controller web interface navigate to **Monitor** > **Alarms**
      - Date and Time
      - Code
      - Alarm Type
      - Severity
      - Status
      - Activity
      - Acknowledged on
      - Cleared By
      - Cleared On
      - Comments
   d. On an alarm generation, the controller web interface **Monitor** > **Alarms** provides the following information as seen in Figure 1.

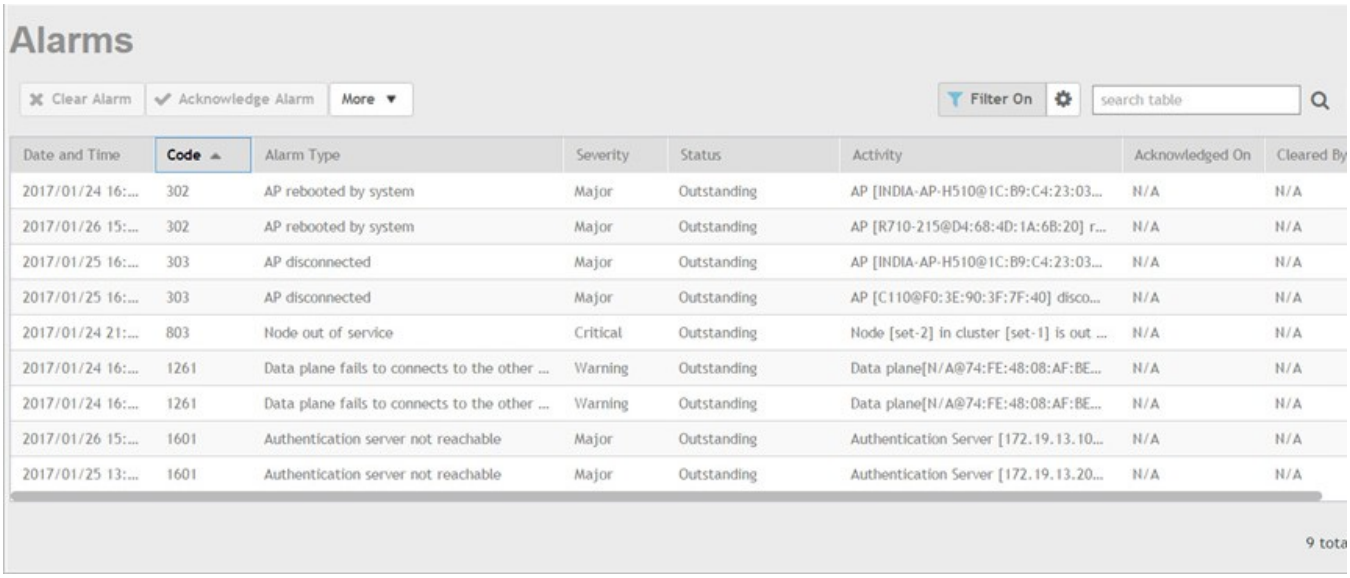
      Threshold Events are triggered at the source whenever possible.

      Users are able to perform various operations on the events, such as filtration, aggregation and counting. The Filter button is deactivated by default. Click this button if you want to turn off the filter. Click on the gear icon to set the filters. A text box appears where you can enter the severity, status and start and end date and time. Click OK when done.

      - Alarm console, which displays the cleared and outstanding alarms visible to the user who is currently logged on.
      - Alarm summary, which lists various information such as outstanding alarm counts and unacknowledged alarm counts, etc.

- You may clear an alarm or a set of alarms to let other administrators know that you have already resolved the issue. When you select a group of alarms, the **Clear Alarms** button is activated. Click this button. A text box appears where you can enter comments or notes about the resolved issue. Click **Apply** when done. To view the cleared alarms, select the cleared option.
- You may acknowledge an alarm or a set of alarms to let other administrators know that you have acknowledged it. When you select an alarm or group of alarms, the **Acknowledge Alarm** button is activated. Click this button. A text box appears where you need to confirm the acknowledgment. Click **Yes** when done. The **Acknowledged on** column in the Alarms table gets updated.
- Filtering features based on the alarm attributes. The **Filter** button is deactivated by default. Click this button if you want to turn on the filter. Click the gear icon to set the filters. A text box appears where you can enter the severity, status and start and end date and time. Click **OK** when done.
- You may also export the data as a CSV file.

FIGURE 1 Alarms



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

- Activity

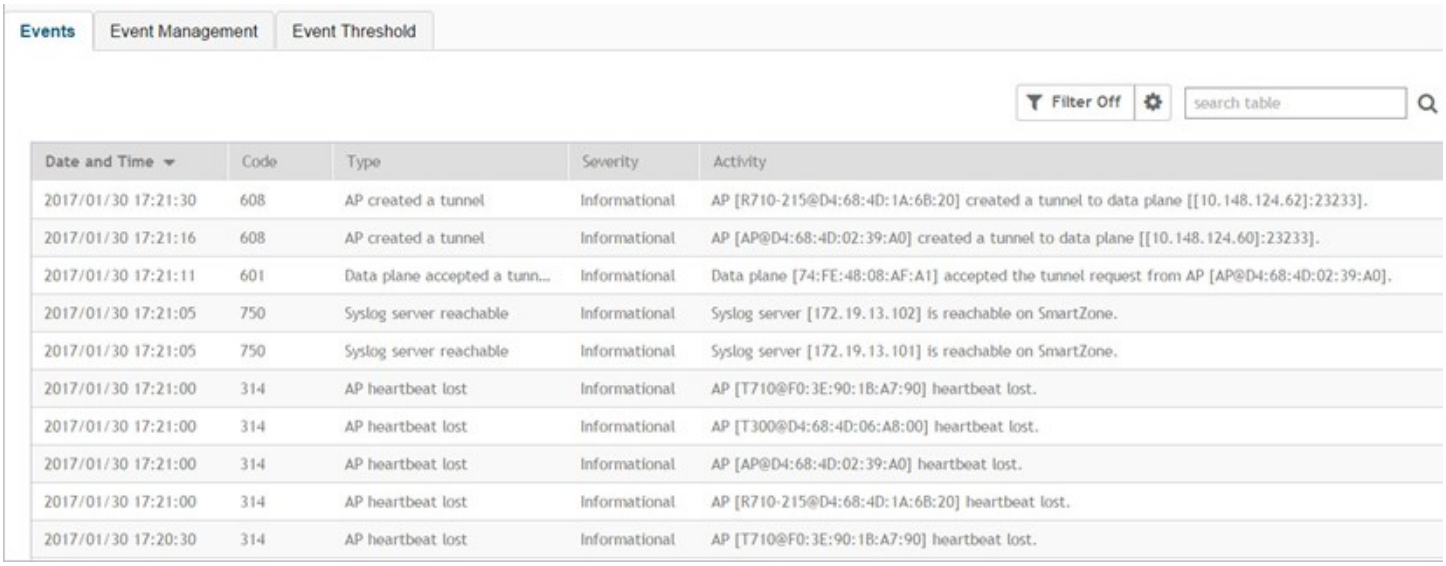
Event Management lists the disabled events that are filtered at the source whenever possible to minimize resources for processing events. The SMTP server is disabled by default. You must enable and configure the SMTP server so notification emails can be delivered successfully.

Threshold Events are triggered at the source whenever possible.

Users are able to perform various operations on the events, such as filtration, aggregation and counting. The **Filter** button is deactivated by default. Click this button if you want to turn off the filter. Click on the gear icon to set the filters. A text box appears where you can enter the severity, status and start and end date and time. Click **OK** when done.

The controller gives you the option of exporting the data as a CSV file.

FIGURE 2 Events



NOTE
Refer to Alarm Types on page 29 and Events Types on page 89 for the list of alarms and events that the controller generates.

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

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

Alarm Types

Introduction

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

Accounting Alarms

Following are the alarms related to accounting.

Accounting server not reachable

TABLE 3 Accounting server not reachable alarm

Alarm	Accounting server not reachable
Alarm Type	accSrvrNotReachable
Alarm Code	1602
Severity	Major
Aggregation Policy	An alarm is raised for every event from the event code 1602. A single event triggers a single alarm.
Attribute	“mvnoId”=12, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd”, “realm”=”wlan.3gppnetwork.org" “radProxyIp”=”7.7.7.7”, “accSrvrIp"=”30.30.30.30” " {produce.short.name}"="2.2.2.2"

TABLE 3 Accounting server not reachable alarm (continued)

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

NOTE
Refer to Accounting Events on page 89.

AP Authentication Alarms

Following are the alarms related to AP authentication.

RADIUS server unreachable

TABLE 4 RADIUS server unreachable alarm

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

LDAP server unreachable

TABLE 5 LDAP server unreachable alarm

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

AD server unreachable

TABLE 6 AD server unreachable alarm

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

WeChat ESP authentication server unreachable

TABLE 7 WeChat ESP authentication server unreachable alarm

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

TABLE 7 WeChat ESP authentication server unreachable alarm (continued)

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

WeChat ESP authentication server unresolvable

TABLE 8 WeChat ESP authentication server unresolvable alarm

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

WeChat ESP DNAT server unreachable

TABLE 9 WeChat ESP DNAT server unreachable alarm

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

TABLE 9 WeChat ESP DNAT server unreachable alarm (continued)

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

WeChat ESP DNAT server unresolvable

TABLE 10 WeChat ESP DNAT server unresolvable alarm

Alarm	WeChat ESP DNAT server unresolvable
Alarm Type	espDNATServerUnresolvable
Alarm Code	2164
Severity	Major
Aggregation Policy	From the event code 2164 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx","dn"="www.test.com","profileId"="1","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Auto Clearance	The alarm is auto cleared with the event code 2163.
Displayed on the web interface	AP [{apName&&apMac}] is unable to resolve WeChat ESP DNAT server domain name [{dn}] to IP
Description	This alarm is triggered when the AP is unable to resolve WeChat ESP DNAT server domain name.
Recommended Actions	Check the DNS server configuration settings in the controller web interface.

NOTE
Refer to AP Authentication Events on page 134.

AP Communication Alarms

Following are the alarms related to access point communications.

AP rejected

TABLE 11 AP rejected alarm

Alarm	AP rejected
Alarm Type	apStatusRejected

TABLE 11 AP rejected alarm (continued)

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

AP configuration update failed

TABLE 12 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 13 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}]

TABLE 13 AP swap model mismatched alarm (continued)

Alarm	AP swap model mismatched
Description	This alarm is triggered when the AP model differs from the swapped configuration model.
Recommended Actions	If the model is incorrect delete and rejoin the AP.

AP pre-provision model mismatched

TABLE 14 AP pre-provision model mismatched alarm

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

AP firmware update failed

TABLE 15 AP firmware update failed alarm

Alarm	AP firmware update failed
Alarm Type	apFirmwareUpdateFailed
Alarm Code	107
Severity	Major
Aggregation Policy	From the event code 107 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 106.
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx"
Displayed on the web interface	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}] [{reason}]
Description	This alarm is triggered when the AP fails to update the firmware details on the controller.
Recommended Actions	Retrieve the AP support text. Reboot the AP and trigger another configuration change for upgrading the AP. If it fails revert to the previous zone firmware.

AP WLAN oversubscribed

TABLE 16 AP WLAN oversubscribed alarm

Alarm	AP WLAN oversubscribed
Alarm Type	apWlanOversubscribed
Alarm Code	108
Severity	Major
Aggregation Policy	From the event code 114 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"apMac"=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	AP [{apName&&apMac}] does not have enough capacity to deploy all wlans. Only maximum wlan number of the AP can be deployed
Description	This alarm is triggered when the AP exceeds the maximum capacity for deploying all WLANs. Only a maximum number of WLAN APs can be deployed.
Recommended Actions	Any of the following are the recommended actions. • Create a new WLAN group with WLANs. Ensure that it is not more than the AP's WLAN capacity. Apply the new WLAN group to either the AP or the AP's AP Group. • Find the WLAN group used by the AP and reduce the number of WLAN.

AP LBS Alarms

Following are the alarms related to AP Location Based Service.

- No LS responses on page 36
- LS authentication failure on page 37
- AP failed to connect to LS on page 37

No LS responses

TABLE 17 No LS responses alarm

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

LS authentication failure

TABLE 18 LS authentication failure alarm

Alarm	LS authentication failure
Alarm Type	apLBSAuthFailed
Alarm Code	702
Severity	Major
Aggregation Policy	From the event code 702 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx“, “url”=““,”port”=““
Displayed on the web interface	AP [{apName&&apMac}] LBS authentication failed: url=[{url}], port=[{port}]
Description	This alarm is triggered 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 19 AP failed to connect to LS alarm

Alarm	AP failed to connect to LS
Alarm Type	apLBSConnectFailed
Alarm Code	704
Severity	Major
Aggregation Policy	From the event code 704 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 703.
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx“, “url”=““,”port”=““
Displayed on the web interface	AP [{apName&&apMac}] connection failed to LS: url=[{url}], port=[{port}]
Description	This alarm is triggered when the AP fails to connect to the location based service.
Recommended Actions	This alarm is triggered either when the location server is unreachable or the network connection is unstable or the domain name system (DNS) configuration is incorrect. It is recommended to check all the three possible error codes 701, 702 and 704.

NOTE
Refer to AP LBS Events on page 104.

AP State Change Alarms

Following are the alarms related to access point state changes.

- AP rebooted by system on page 38
- AP disconnected on page 38
- AP deleted on page 39

AP rebooted by system

TABLE 20 AP rebooted by system alarm

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

AP disconnected

TABLE 21 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 22 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 23 AP cable modem interface down alarm

Alarm	AP cable modem interface down
Alarm Type	cableModemDown
Alarm Code	308
Severity	Major
Aggregation Policy	From the event code 316 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 325.
Attribute	“apMac”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	AP [{apName&&apMac}] cable modem interface is down
Description	This alarm is triggered when the AP cable modem interface is down.
Recommended Actions	Check cable modem. Try rebooting the cable modem.

NOTE
Refer to AP State Change Events on page 114.

AP DHCP service failure

TABLE 24 AP DHCP service failure alarm

Alarm	Both primary and secondary DHCP server APs are down
Alarm Type	apDHCPServiceFailure
Alarm Code	341
Severity	Major
Aggregation Policy	From the event code 341 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	”primaryServerMac”=“xx:xx:xx:xx:xx:xx”, “secondaryServerMac”=“xx:xx:xx:xx:xx:xx”

TABLE 24 AP DHCP service failure alarm (continued)

Alarm	Both primary and secondary DHCP server APs are down
Displayed on the web interface	AP DHCP service failure. Both primary DHCP AP [{primaryServerMac}] and secondary DHCP server AP [{secondaryServerMac}] are down.
Description	This alarm is triggered when the primary and secondary DHCP server APs fail.
Recommended Actions	Deploy DHCP service on another AP.

AP NAT failure

TABLE 25 AP NAT failure alarm

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

AP DHCP/NAT DWPD Ethernet port configuration override

TABLE 26 AP DHCP/NAT DWPD Ethernet port configuration override alarm

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

SZ DHCP/NAT DWPD Ethernet port configuration override

TABLE 27 SZ DHCP/NAT DWPD Ethernet port configuration override alarm

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

NOTE
Refer to AP State Change Alarms on page 37.

SIM removal

TABLE 28 SIM removal alarm

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

Authentication Alarms

The following are the alarms related to authentication.

Authentication server not reachable

TABLE 29 Authentication server not reachable alarm

Alarm	Authentication server not reachable
Alarm Type	authSrvrNotReachable
Alarm Code	1601
Severity	Major
Aggregation Policy	From the event code 1601 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “authSrvrIp"=”20.20.20.20” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Authentication Server [{authSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered when 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 30 Authentication failed over to secondary alarm

Alarm	Authentication failed over to secondary
Alarm Type	authFailedOverToSecondary
Alarm Code	1651
Severity	Major
Aggregation Policy	From the event code 1651 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered when the secondary RADIUS server is available after the primary server becomes zombie or dead.
Recommended Actions	No operator action is required.

Authentication fallback to primary

TABLE 31 Authentication fallback to primary alarm

Alarm	Authentication fallback to primary
Alarm Type	authFallbackToPrimary
Alarm Code	1652
Severity	Major
Aggregation Policy	From the event code 1652 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered when automatic fallback is enable. Consequently, the authentication failover to secondary server occurs and the revival timer for the primary server expires, and the requests falls back to the primary server.
Recommended Actions	No action is required.

AD/LDAP connectivity failure

TABLE 32 AD/LDAP connectivity failure alarm

Alarm	AD/LDAP connectivity failure
Alarm Type	racADLDAPFail
Alarm Code	1752
Severity	Major
Aggregation Policy	From the event code 1752 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, "SZMgmtIp"="2.2.2.2" “desc”= "Connection to AD/LDAP fails"
Displayed on the web interface	[{srcProcess}] Connect to AD/LDAP[{authSrvrIp}] fails from {produce.short.name}[{SZMgmtIp}]
Description	This alarm is triggered when RADIUS server fails to connect with AD/LDAP server.
Recommended Actions	• Check whether AD/LDAP server instance is running on the target machine • Check whether the AD/LDAP server can be reached from the controller • Verify if AD/LDAP server instances are listening on ports 3268 and 389 • Verify if the requests are reaching AD/LDAP servers by any packet capture tool (tcpdump, wireshark)

Bind fails with AD/LDAP

TABLE 33 Bind fails with AD/LDAP alarm

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

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

TABLE 34 Bind success with LDAP, but unable to find clear text password for the user alarm

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

RADIUS fails to connect to AD NPS server

TABLE 35 RADIUS fails to connect to AD NPS server alarm

Alarm	RADIUS fails to connect to AD NPS server
Alarm Type	racADNPSFail
Alarm Code	1755
Severity	Major
Aggregation Policy	From the event code 1755 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12 “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”= ”Fails to connect to AD NPS server”
Displayed on the web interface	[{srcProcess}] Fails to connect to AD NPS[{authSrvrIp}] from {produce.short.name} [{SZMgmtIp}
Description	This alarm is triggered RADIUS server fails to connect to AD NPS server.
Recommended Actions	• Verify if the configured NPS server instance is up and running (Network Policy Server) • Verify if the NPS server instance is communicating on the standard RADIUS port 1812 • Ensure that Windows server where AD/NPS server is provisioned can be reached from the controller web interface

RADIUS fails to authenticate with AD NPS server

TABLE 36 RADIUS fails to authenticate with AD NPS server alarm

Alarm	RADIUS fails to authenticate with AD NPS server
Alarm Type	racADNPSFailToAuthenticate
Alarm Code	1756
Severity	Major
Aggregation Policy	From the event code 1756 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”=”Fails to authenticate with AD NPS”
Displayed on the web interface	[{srcProcess}] Fails to authenticate AD NPS[{authSrvrIp}] on {produce.short.name}[{SZMgmtIp}] for User[{userName}
Description	This alarm is triggered when RADIUS server fails to authenticate with AD NPS server.
Recommended Actions	• The shared secret for NPS server should be same as that of administrator password provisioned in the controller web interface for AD server • NPS should be configured to accept request (CHAP and MSCHAPv2) from the controller • For CHAP authentication to work the AD server should store the password in reversible encryption format • Ensure that NPS is registered with AD server

NOTE
Refer to Authentication Events on page 142.

Fails to establish TLS tunnel with AD/LDAP

TABLE 37 Fails to establish TLS tunnel with AD/LDAP alarm

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

NOTE
Refer to Authentication Events on page 142.

Control and Data Plane Interface Alarms

NOTE
This section is not applicable for vSZ-E.

Following alarm relates to control and data plane.

- GtpManager (DP) disconnected on page 46

GtpManager (DP) disconnected

TABLE 38 GtpManager (DP) disconnected alarm

Alarm	GtpManager (DP) disconnected
Alarm Type	lostCnxnToDblade
Alarm Code	1202
Severity	Major
Aggregation Policy	From the event code 1202 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1201.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”NA” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2"

TABLE 38 GtpManager (DP) disconnected alarm (continued)

Alarm	GtpManager (DP) disconnected
Displayed on the web interface	The connectivity between Control plane [{ctrlBladeIp}] and Data plane [{dataBladeIp}] is lost at {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered due to transmission control protocol (TCP) connection loss or when control plane is unable to complete the configuration procedure successfully.
Recommended Actions	A manual intervention is required. Refer to Control and Data Plane Interface Events on page 150 event 1201.

NOTE
Refer to Control and Data Plane Interface Events on page 150.

Cluster Alarms

Following are alarms related to cluster:

- New node failed to join on page 48
- Node removal failed on page 48
- Node out of service on page 49
- Cluster in maintenance state on page 49
- Cluster backup failed on page 49
- Cluster restore failed on page 50
- Cluster upgrade failed on page 50
- Cluster application stopped on page 51
- Node bond interface down on page 51
- Node physical interface down on page 52
- Cluster node rebooted on page 52
- Cluster node shut down on page 53
- Disk usage exceed threshold on page 53
- Cluster out of service on page 54
- Cluster upload AP firmware failed on page 54
- Cluster add AP firmware failed on page 54
- Unsync NTP time on page 55
- Cluster upload KSP file failed on page 55
- Configuration backup failed on page 55
- Configuration restore failed on page 56
- AP certificate updated on page 56
- Upgrade SS table failed on page 57
- Over switch max capacity on page 57

New node failed to join

TABLE 39 New node failed to join alarm

Alarm	New node failed to join
Alarm Type	newNodeJoinFailed
Alarm Code	801
Severity	Critical
Aggregation Policy	From the event code 803 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 802.
Attribute	“clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”
Displayed on the web interface	New node [([{nodeName}]) failed to join cluster [{clusterName}]
Description	This alarm is triggered when a node fails to join a cluster session. The controller web Interface displays the error message.
Recommended Actions	When the operation fails, the user can run the **join process**. If it continues to fail, please send the complete log files to Ruckus support. Download the system log file by logging to the controller system. Navigate to Administration >> Diagnostics >> Application Logs & Status. 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 40 Node removal failed alarm

Alarm	Node removal failed
Alarm Type	removeNodeFailed
Alarm Code	802
Severity	Major
Aggregation Policy	From the event code 805 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 804.
Attribute	“clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Node [{nodeName}] failed to remove from cluster [{clusterName}].
Description	This alarm is triggered when it is unable to remove a node from the cluster.
Recommended Actions	In general, this alarm should rarely occur. If it occurs, restore to the previous backup file. Please send the complete log files to Ruckus support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status.

Node out of service

TABLE 41 Node out of service alarm

Alarm	Node out of service
Alarm Type	nodeOutOfService
Alarm Code	803
Severity	Critical
Aggregation Policy	From the event code 806 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 835.
Attribute	“clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Node [{nodeName}] in cluster [{clusterName}] is out of service. Reason: [{reason}].
Description	This alarm is triggered when a node is out of service.
Recommended Actions	The operator/user needs to check the application/interface state.

Cluster in maintenance state

TABLE 42 Cluster in maintenance state alarm

Alarm	Cluster in maintenance state
Alarm Type	clusterInMaintenanceState
Alarm Code	804
Severity	Critical
Aggregation Policy	From the event code 807 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 808.
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] is in maintenance state
Description	This alarm is triggered when a cluster is in a maintenance state.
Recommended Actions	Possible causes: • The entire system backup is in process. • In a two-node cluster, the remove-node process is working. For any other cause, please send the complete log files to Ruckus support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status.

Cluster backup failed

TABLE 43 Cluster backup failed alarm

Alarm	Cluster backup failed
Alarm Type	backupClusterFailed
Alarm Code	805
Severity	Major

TABLE 43 Cluster backup failed alarm (continued)

Alarm	Cluster backup failed
Aggregation Policy	From the event code 810 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 809.
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason:[{reason}].
Description	This alarm is triggered when a cluster backup fails.
Recommended Actions	Check the disk usage. Try restoring the communication between nodes for a few more times. If the backup continues to fail or if you encounter Python script errors, please send the complete log files to Ruckus support. Download the system log file by logging to the controller system. Navigate to Administration > Diagnostics > Application Logs & Status. Possible causes: • Insufficient disk space. • Communication between nodes may be broken. • Errors due to the underlying Python script.

Cluster restore failed

TABLE 44 Cluster restore failed alarm

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

Cluster upgrade failed

TABLE 45 Cluster upgrade failed alarm

Alarm	Cluster upgrade failed
Alarm Type	upgradeClusterFailed
Alarm Code	807

TABLE 45 Cluster upgrade failed alarm (continued)

Alarm	Cluster upgrade failed
Severity	Major
Aggregation Policy	From the event code 815 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 814.
Attribute	"clusterName”=”xxx”, “nodeName”=”xxx”, “nodeMac”=” xx:xx:xx:xx:xx:xx”, “fromVersion”="x.x", “toVersion”="x.x"
Displayed on the web interface	Cluster [{clusterName}] could not be upgraded from [{fromVersion}] to [{toVersion}]. Reason:[{reason}].
Description	This alarm is triggered when a version upgrade of a cluster fails.
Recommended Actions	Check the disk usage. Try restoring the communication between nodes for a few times. If the backup continues to fail or if you encounter Python script errors, please send the complete log files to Ruckus support. Download the system log file by logging to the controller system. Navigate to **Administration** > **Diagnostics** > **Application Logs & Status**. Possible causes: • Insufficient disk space. • Communication between nodes might be broken. • Errors due to the underlying Python script.

Cluster application stopped

TABLE 46 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 47 Node bond interface down alarm

Alarm	Node bond interface down
Alarm Type	nodeBondInterfaceDown

TABLE 47 Node bond interface down alarm (continued)

Alarm	Node bond interface down
Alarm Code	809
Severity	Major
Aggregation Policy	From the event code 821 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 822.
Attribute	"nodeName"="xxx", "nodeMac"="xxx", "ifName"="xxxx"
Displayed on the web interface	Network interface [{networkInterface||ifName}] on node [{nodeName}] is down.
Description	This alarm is triggered when the network interface of a node is down.
Recommended Actions	Check if the network cables of both the physical interfaces are broken. Alternatively, check if the physical interfaces for this bond interface 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 48 Node physical interface down alarm

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

Cluster node rebooted

TABLE 49 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.

TABLE 49 Cluster node rebooted alarm (continued)

Alarm	Cluster node rebooted
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 50 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 51 Disk usage exceed threshold alarm

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

Cluster out of service

TABLE 52 Cluster out of service alarm

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

Cluster upload AP firmware failed

TABLE 53 Cluster upload AP firmware failed alarm

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

Cluster add AP firmware failed

TABLE 54 Cluster add AP firmware failed alarm

Alarm	Cluster add AP firmware failed
Alarm Type	clusterAddAPFirmwareFailed
Alarm Code	853
Severity	Major
Aggregation Policy	From the event code 853 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 852
Attribute	"clusterName"="xx"

TABLE 54 Cluster add AP firmware failed alarm (continued)

Alarm	Cluster add AP firmware failed
Displayed on the web interface	Cluster [{clusterName}] add AP firmware failed.
Description	This alarm is triggered when the cluster upload to AP firmware fails.
Recommended Actions	It is recommended that the operator applies the AP patch.

Unsync NTP time

TABLE 55 Unsync NTP time alarm

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

Cluster upload KSP file failed

TABLE 56 Cluster upload KSP file failed alarm

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

Configuration backup failed

TABLE 57 Configuration backup failed alarm

Alarm	Configuration backup failed
Alarm Type	clusterCfgBackupFailed
Alarm Code	862
Severity	Major

TABLE 57 Configuration backup failed alarm (continued)

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

Configuration restore failed

TABLE 58 Configuration restore failed alarm

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

AP certificate updated

TABLE 59 AP certificate updated alarm

Alarm	AP certificate updated
Alarm Type	apCertificateExpire
Alarm Code	865
Severity	Critical
Aggregation Policy	From the event code 865 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 866.
Attribute	"count"="XXX"
Displayed on the web interface	[{count}] APs need to update their certificates.
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 on page 169.

Upgrade SS table failed

TABLE 60 Upgrade SS table failed alarm

Alarm	Upgrade SS table failed
Alarm Type	upgradeSSTableFailed
Alarm Code	868
Severity	Major
Aggregation Policy	From the event code 866 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"nodeName"="xxx"
Displayed on the web interface	Node [{nodeName}] upgrade SSTable failed.
Description	This alarm is triggered when the SS table upgrade fails.

Over switch max capacity

TABLE 61 Over switch max capacity alarm

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

Configuration Alarms

Following are the alarms related to configuration.

- Zone configuration preparation failed on page 58
- AP configuration generation failed on page 58
- End-of-life AP model detected on page 58
- VLAN configuration mismatch on non DHCP/NAT WLAN on page 59
- VLAN configuration mismatch on DHCP/NAT WLAN on page 59

Zone configuration preparation failed

TABLE 62 Zone configuration preparation failed alarm

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

AP configuration generation failed

TABLE 63 AP configuration generation failed alarm

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

End-of-life AP model detected

TABLE 64 End-of-life AP model detected alarm

Alarm	End-of-life AP model detected
Alarm Type	cfgGenSkippedDueToEolAp
Alarm Code	1023
Severity	Major
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“nodeMac”="50:A7:33:24:E7:90","zoneName"="openZone","model"="R300,T300"

TABLE 64 End-of-life AP model detected alarm (continued)

Alarm	End-of-life AP model detected
Displayed on the web interface	Detected usage of end-of-life ap model(s)[{model}] while generating configuration for AP(s) under zone[{zoneName}]
Description	This alarm is triggered when the controller detects the AP model's end-of-life under a certain zone.
Recommended Actions	These obsoleted APs occupies licensed AP space. Disconnect these unsupported AP models from the given zone by: • Reset the APs to a factory setting using the AP command line Delete these APs through the **controller Web Interface** > **Configuration AP List**

NOTE
Refer to Configuration Events on page 191.

VLAN configuration mismatch on non DHCP/NAT WLAN

TABLE 65 VLAN configuration mismatch on non DHCP/NAT WLAN alarm

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

VLAN configuration mismatch on DHCP/NAT WLAN

TABLE 66 VLAN configuration mismatch on DHCP/NAT WLAN alarm

Alarm	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on DHCP/NAT WLAN
Alarm Type	apCfgDhcpNatWlanVlanConfigMismatch
Alarm Code	1025
Severity	Critical
Aggregation Policy	From the event code 1023 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"ssid"="xxxx", "wlanID"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac""xx:xx:xx:xx:xx:xx"
Displayed on the web interface	DHCP/NAT gateway AP [{apMac}] detected VLAN configuration mismatch on DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and

TABLE 66 VLAN configuration mismatch on DHCP/NAT WLAN alarm (continued)

Alarm	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on DHCP/NAT WLAN
	resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This alarm is triggered when the AP detects a DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

NOTE
Refer to Configuration Events on page 191.

Data Plane Alarms

Following are the alarms related to data plane.

Data plane configuration update failed

TABLE 67 Data plane configuration update failed alarm

Alarm	Data plane configuration update failed
Alarm Type	dpConfUpdateFailed
Alarm Code	501
Severity	Major
Aggregation Policy	From the event code 505 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 504
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “configID”=” 123456781234567”
Displayed on the web interface	Data plane [{dpName||dpKey}] failed to update to configuration [{configID}].
Description	This alarm is triggered when the data plane configuration update fails since it was unable to transfer the configuration update from the control plane to the data plane.
Recommended Actions	Check the data plane configuration and the CPU utilization of the control plane. The possible cause could be of the server being busy at that particular moment. Check to see if the event is persistent.

Data plane disconnected

TABLE 68 Data plane disconnected alarm

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

Data plane physical interface down

TABLE 69 Data plane physical interface down alarm

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

Data plane process restarted

TABLE 70 Data plane process restarted alarm

Alarm	Data plane process restarted
Alarm Type	dpProcessRestart
Alarm Code	520
Severity	Major
Aggregation Policy	From the event code 520 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	dpKey="xx:xx:xx:xx:xx:xx", processName="xxxx"

TABLE 70 Data plane process restarted alarm (continued)

Alarm	Data plane process restarted
Displayed on the web interface	[{processName}] process got re-started on data plane [{dpName&&dpKey}]
Description	This alarm is triggered when a process in data plane restarts since it fails to pass the health check.
Recommended Actions	No action required.

Data plane license is not enough

NOTE
Alarm 538 is applicable only for vSZ-E.

TABLE 71 Data plane license is not enough alarm

Alarm	Data plane license is not enough
Alarm Type	dpLicenseInsufficient
Alarm Code	538
Severity	Major
Aggregation Policy	From the event code 538 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"count"=<delete-vdp-count>
Displayed on the web interface	DP license is not enough, [{count}] instance of DP will be deleted.
Description	This alarm is triggered when the number of data plane licenses are insufficient.
Recommended Actions	Check if the number of data plane licenses has exceeded the limit. You would need to purchase additional licenses, in case of insufficient licenses and synchronize the licenses.

Data plane upgrade failed

NOTE
Alarm 553 is applicable only for vSZ-E

TABLE 72 Data plane upgrade failed alarm

Alarm	Data plane upgrade failed
Alarm Type	dpLicenseInsufficient
Alarm Code	553
Severity	Major
Aggregation Policy	From the event code 553 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to upgrade.
Description	This alarm is triggered when the data plane upgrade fails.
Recommended Actions	There are several possible reasons to trigger alarm 553. The operator has to ensure the accuracy of network connectivity and version availability. For advanced process, check the debug log for reason of upgrade failure. **Note**:

TABLE 72 Data plane upgrade failed alarm (continued)

Alarm	Data plane upgrade failed
	Debug file includes the upgrade log file. The operator can get the debug log from vSZ web interface or through vSZ-D CLI. The operator can use the following vSZ-D CLI commands to: • View the previous upgrade status and reason in case of a failure - `ruckus# show upgrade-state / ruckus# show upgrade-history` • Save the debug file for viewing - `ruckus(debug)# save-log` • Check the connection status between vSZ and vSZ-D - `ruckus# show status` • Check the current vSZ-D software version - `ruckus# show version` **Note**: Refer to the vSZ-D CLI Reference Guide for details on the CLI commands mentioned above.

NOTE
Refer to Data Plane Events on page 201.

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

TABLE 73 Data plane of data center side fails to connect to the CALEA server alarm

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

Data plane fails to connects to the other data plane

TABLE 74 Data plane fails to connects to the other data plane alarm

Alarm	Data plane fails to connects to the other data plane
Alarm Type	dpP2PTunnelConnectFail
Alarm Code	1261
Severity	Major
Aggregation Policy	From the event code 1261 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, "dpIP"="xx.xx.xx.xx", “targetDpKey”=“xx:xx:xx:xx:xx:xx”, “targetDpIp”=“xxx.xxx.xxx.xxx”

TABLE 74 Data plane fails to connects to the other data plane alarm (continued)

Alarm	Data plane fails to connects to the other data plane
Displayed on the web interface	Data Plane[{dpName&&dpKey}] fails connects to the other Data Plane[{targetDpKey&&targetDpIp}]
Description	This alarm is triggered when the data plane fails to connect to another data plane.
Recommended Actions	Check the connectivity between data planes.

Data Plane DHCP IP Pool usage rate is 100 percent

TABLE 75 Data plane DHCP IP pool usage rate is 100 percent alarm

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

NOTE
Refer toData Plane Events on page 201

IPMI Alarms

NOTE
This section is not applicable for vSZ-E.

Following are the alarms related to IPMIs.

ipmiThempBB

TABLE 76 ipmiThempBB alarm

Alarm	ipmiThempBB
Alarm Type	ipmiThempBB
Alarm Code	902

TABLE 76 ipmiThempBB alarm (continued)

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

ipmiThempP

TABLE 77 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.

ipmiFan

TABLE 78 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"

TABLE 78 ipmiFan alarm (continued)

Alarm	ipmiFan
Displayed on the web interface	System fan [{id}] module [{status}] on control plane [{nodeMac}]
Description	This alarm is triggered when the control plane's fan module status is shown.
Recommended Actions	Replace the fan module.

ipmiFanStatus

TABLE 79 ipmiFanStatus alarm

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

NOTE
Refer to IPMI Events on page 219.

Licensing Interface Alarms

The following are the alarms related to licensing:

- License going to expire on page 66
- Insufficient license capacity on page 67
- Data plane DHCP IP license insufficient on page 67
- Data plane NAT session license insufficient on page 68
- Insufficient license capacity on page 68

License going to expire

TABLE 80 License going to expire alarm

Alarm	License going to expire
Alarm Type	licenseGoingToExpire
Alarm Code	1255
Severity	Major

TABLE 80 License going to expire alarm (continued)

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

Insufficient license capacity

TABLE 81 Insufficient license capacity alarm

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

NOTE
Refer to Licensing Interface Events on page 222.

Data plane DHCP IP license insufficient

TABLE 82 Data plane DHCP IP license insufficient alarm

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

TABLE 82 Data plane DHCP IP license insufficient alarm (continued)

Alarm	Data plane DHCP IP license insufficient
Description	This alarm is triggered when the data plane DHCP IP license is insufficient.

Data plane NAT session license insufficient

TABLE 83 Data plane NAT session license insufficient alarm

Alarm	Data plane NAT session license insufficient
Alarm Type	dpNatSessionLicenseNotEnough
Alarm Code	1278
Severity	Major
Aggregation Policy	From the event code 1277 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This alarm occurs when Data Plane NAT session license insufficient. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This alarm is triggered when the data plane NAT server license is insufficient.

NOTE
Refer to Licensing Interface Events on page 222.

Insufficient license capacity

TABLE 84 Insufficient license capacity alarm

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

SCI Alarms

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

- SCI and FTP have been disabled on page 69

Connect to SCI failure

TABLE 85 Connect to SCI failure alarm

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

SCI has been disabled

TABLE 86 SCI has been disabled alarm

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

SCI and FTP have been disabled

TABLE 87 SCI and FTP have been disabled alarm

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

TABLE 87 SCI and FTP have been disabled alarm (continued)

Alarm	SCI and FTP have been disabled
Description	This event occurs when the SCI and FTP are disabled.

NOTE
Refer to SCI Events on page 227.

System Alarms

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

Following are the alarms with the system log severity:

No LS responses

TABLE 88 No LS responses alarm

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

LS authentication failure

TABLE 89 LS authentication failure alarm

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

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

TABLE 90 {produce.short.name} failed to connect to LSalarm

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

Syslog server unreachable

TABLE 91 Syslog server unreachable alarm

Alarm	Syslog server unreachable
Alarm Type	syslogServerUnreachable
Alarm Code	751
Severity	Major
Aggregation Policy	From the event code 751 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 750.
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “syslogServerAddress"="xxx.xxx.xxxx.xxx"

TABLE 91 Syslog server unreachable alarm (continued)

Alarm	Syslog server unreachable
Displayed on the SmartZone web interface	Syslog server [{syslogServerAddress}] is unreachable on {produce.short.name}.
Description	This alarm is triggered when the syslog server is unreachable.
Recommended Actions	Check the network between the controller and the syslog server.

CSV export FTP maximum retry

TABLE 92 CSV export FTP maximum retry alarm

Alarm	CSV export FTP maximum retry
Alarm Type	csvFtpTransferMaxRetryReached
Alarm Code	974
Severity	Major
Aggregation Policy	From the event code 974 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm is auto cleared with the event code 750.
Attribute	“nodeName”=“xx:xx:xx:xx:xx:xx”, “ip”=“xx:xx:xx:xx:xx:xx”, “portID”=“xx:xx:xx:xx:xx:xx”, “filename"="xxx.xxx.xxxx.xxx"
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV file fails to transfer after a maximum of five (5) retries.

CSV export disk threshold exceeded

TABLE 93 CSV export disk threshold exceeded alarm

Alarm	CSV export disk threshold exceeded
Alarm Type	csvDiskThresholdExceeded
Alarm Code	975
Severity	Warning
Aggregation Policy	From the event code 975 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“nodeName”=“xx:xx:xx:xx:xx:xx”, “threshold”=“xx:xx:xx:xx:xx:xx”, “availableDiskSize”=“xx:xx:xx:xx:xx:xx”
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV report size exceeds 80% of its capacity.
Recommended Actions	

CSV export disk max capacity reached

TABLE 94 CSV export disk max capacity reached alarm

Alarm	CSV export disk max capacity reached
Alarm Type	csvDiskMaxCapacityReached

TABLE 94 CSV export disk max capacity reached alarm (continued)

Alarm	CSV export disk max capacity reached
Alarm Code	976
Severity	Critical
Aggregation Policy	From the event code 976 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“nodeName”=“xx:xx:xx:xx:xx:xx”, “allocatedDiskSize”=“xx:xx:xx:xx:xx:xx”
Displayed on the SmartZone web interface	
Description	This alarm is triggered when CSV report size reaches its maximum capacity.
Recommended Actions	

Process restart

TABLE 95 Process restart alarm

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

Service unavailable

TABLE 96 Service unavailable alarm

Alarm	Service unavailable
Alarm Type	serviceUnavailable
Alarm Code	1002
Severity	Critical
Aggregation Policy	From the event code 1002 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, " {produce.short.name}MgmtIp"="2.2.2.2"
Displayed on the web interface	[{processName}] process is not stable on {produce.short.name} [{SZMgmtIp}]
Description	This alarm is triggered when the process repeatedly restarts and is unstable.

TABLE 96 Service unavailable alarm (continued)

Alarm	Service unavailable
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 97 Keepalive failure alarm

Alarm	Keepalive failure
Alarm Type	keepAliveFailure
Alarm Code	1003
Severity	Major
Aggregation Policy	From the event code 1003 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”nc”, “realm”=”NA”, “processName”=”aut”, " {produce.short.name}MgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] on Smart Zone [{SZMgmtIp}] restarted [{processName}] process
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 98 Resource unavailable alarm

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

The last one data plane is disconnected zone affinity profile

TABLE 99 The last one data plane is disconnected zone affinity profile alarm

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

NOTE

Refer to System Events on page 229.

Unconfirmed program detection

TABLE 100 Unconfirmed program detection alarm

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

Switch Alarms

Following are the alarms related to switch severity:

Power supply failure

TABLE 101 Power supply failure alarm

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

Fan failure

TABLE 102 Fan failure alarm

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

Module insertion

TABLE 103 Module insertion alarm

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

Module removal

TABLE 104 Module removal alarm

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

Temperature above threshold warning

TABLE 105 Temperature above threshold warning alarm

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

Stack member unit failure

TABLE 106 Stack member unit failure alarm

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

PoE power allocation failure

TABLE 107 PoE power allocation failure alarm

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

DHCP_Snooping: DHCP offer dropped message

TABLE 108 DHCP_Snooping: DHCP offer dropped message alarm

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

Port put into error disable state

TABLE 109 Port put into error disable state alarm

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

Switch offline

TABLE 110 Switch offline alarm

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

Switch duplicated

TABLE 111 Switch duplicated alarm

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

Reject certificate signing request

TABLE 112 Reject certificate signing request alarm

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

Pending certificate signing request

TABLE 113 Pending certificate signing request alarm

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

Switch CPU major threshold exceed

TABLE 114 Switch CPU major threshold exceed alarm

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

Switch CPU critical threshold exceed

TABLE 115 Switch CPU critical threshold exceed alarm

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

Switch memory major threshold exceed

TABLE 116 Switch memory major threshold exceed alarm

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

Switch memory critical threshold exceed

TABLE 117 Switch memory critical threshold exceed alarm

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

TABLE 117 Switch memory critical threshold exceed alarm (continued)

Alarm	Switch memory critical threshold exceed
Description	This alarm is triggered when the memory usage exceeds the critical threshold limit, which is based on the utilization rate.

Switch custom major threshold exceed

TABLE 118 Switch custom major threshold exceed alarm

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

Switch custom critical threshold exceed

TABLE 119 Switch custom critical threshold exceed alarm

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

Threshold Alarms

Following are the alarms related to threshold system set:

- Rate limit for TOR surpassed on page 85
- The number of users exceeded its limit on page 86
- The number of devices exceeded its limit on page 86
- Over AP maximum capacity on page 87

CPU threshold exceeded

TABLE 120 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 usage percentage threshold can be configured as 60% to 90%.
Recommended Actions	Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to Ruckus support. Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.

Memory threshold exceeded

TABLE 121 Memory threshold exceeded alarm

Alarm	Memory threshold exceeded
Alarm Type	memoryThresholdExceeded
Alarm Code	951
Severity	Critical
Aggregation Policy	From the event code 951 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 954.
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the memory usage exceeds the threshold limit. The disk threshold value for SZ100 is 85% and 90% for vSZ-E.
Recommended Actions	Check CPU/memory/disk information for any unexpected value. Keep monitoring the CPU for higher values than the threshold or set it to only one peak value. If the CPU value is high, please take a snapshot log, containing the information and send it to Ruckus support.

TABLE 121 Memory threshold exceeded alarm (continued)

Alarm	Memory threshold exceeded
	Alternatively, if an application is abnormal, restart the service or restart the controller. This may resolve the issue.

Disk usage threshold exceeded

TABLE 122 Disk usage threshold exceeded alarm

Alarm	Disk usage threshold exceeded
Alarm Type	diskUsageThresholdExceeded
Alarm Code	952
Severity	Critical
Aggregation Policy	From the event code 952 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 955.
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Disk usage threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This alarm is triggered when the disk usage exceeds the threshold limit. The disk threshold value is 80%.
Recommended Actions	Check the backup files for disk usage. Each backup file may occupy a large disk space based on the database size. If there are multiple backup files/ versions in the controller, it is recommended to delete the older backup files to free disk usage. If the problem persists, please take a screen shot and send it to Ruckus support.

The drop of client count threshold exceeded

TABLE 123 The drop of client count threshold exceeded alarm

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

License threshold exceeded

TABLE 124 License threshold exceeded alarm

Alarm	License threshold exceeded
Alarm Type	licenseThresholdExceeded

TABLE 124 License threshold exceeded alarm (continued)

Alarm	License threshold exceeded
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.

HDD health degradation

NOTE
This alarm is not applicable for vSZ-H and vSZ-E.

TABLE 125 HDD health degradation alarm

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

Rate limit for TOR surpassed

TABLE 126 Rate limit for TOR surpassed alarm

Alarm	Rate limit for TOR surpassed
Alarm Type	rateLimitMORSurpassed
Alarm Code	1302
Severity	Critical
Aggregation Policy	From the event code 1302 an alarm is raised for every event. A single event triggers a single alarm.
Auto Clearance	The alarm code is auto cleared with the event code 1301.
Attribute	"mvnoId”=”12”, “wlanId”=”1”, “zoneId”=”10”, “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “srcProcess”=”radiusd”, “UserName”=abc@xyz.com, “realm”=”wlan.3gppnetwor"

TABLE 126 Rate limit for TOR surpassed alarm (continued)

Alarm	Rate limit for TOR surpassed
	"SZMgmtIp"="2.2.2.2", “aaaSrvrIp”=”1.1.1.1” “AAAServerType”=”Auth/Acct”, “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “MOR”=1000, “THRESHOLD”=”500”, “TOR”=”501”
Displayed on the web interface	Maximum Outstanding Requests(MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This alarm is triggered when maximum outstanding requests (MOR) is surpassed.
Recommended Actions	Download the SM log file from the controller web Interface to check the error cause.

The number of users exceeded its limit

TABLE 127 The number of users exceeded its limit

Alarm	The number of users exceeded its limit
Alarm Type	tooManyUsers
Alarm Code	7003
Severity	Major
Aggregation Policy	From the event code 7001 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	This alarm has no attributes.
Displayed on the web interface	The number of users exceeds the specified limit
Description	This alarm is triggered when the number of users exceeds the specified limit.
Recommended Actions	No action is required.

The number of devices exceeded its limit

TABLE 128 The number of devices exceeded its limit alarm

Alarm	The number of devices exceeded its limit
Alarm Type	tooManyDevices
Alarm Code	7004
Severity	Major
Aggregation Policy	From the event code 7002 an alarm is raised for every event. A single event triggers a single alarm.
Attribute	This alarm has no attributes.
Displayed on the web interface	Displayed on the web interface. The number of devices exceeded its limit
Description	This alarm is triggered the number of devices exceeds the specified limit.
Recommended Actions	No action is required.

NOTE
Refer toThreshold Events on page 250.

Over AP maximum capacity

TABLE 129 Over AP maximum capacity alarm

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

Tunnel Alarms - Access Point

Following are the alarms related to tunnel.

AP softGRE gateway not reachable

TABLE 130 AP softGRE gateway not reachable alarm

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

AP is disconnected from secure gateway

TABLE 131 AP is disconnected from secure gateway alarm

Alarm	AP is disconnected from secure gateway
Alarm Type	ipsecTunnelDisassociated
Alarm Code	661

TABLE 131 AP is disconnected from secure gateway alarm (continued)

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

AP secure gateway association failure

TABLE 132 AP secure gateway association failure alarm

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

NOTE

Refer toTunnel Events - Access Point (AP) on page 256 and Tunnel Events - Data Plane on page 261

Events Types

Accounting Events

Following are the events related to accounting.

Accounting server not reachable

TABLE 133 Accounting server not reachable event

Event	Accounting server not reachable
Event Type	accSrvrNotReachable
Event Code	1602
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “accSrvrIp"=”30.30.30.30” "SZMgmtIp"="2.2.2.2"

TABLE 133 Accounting server not reachable event (continued)

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

AP accounting response while invalid config

TABLE 134 AP accounting response while invalid config event

Event	AP accounting response while invalid config
Event Type	apAcctRespWhileInvalidConfig
Event Code	1909
Severity	Debug
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10", “ctrlBladeMac"="aa:bb:cc:dd:ee:ff", "srcProcess"="aut" "realm"="wlan.3gppnetwork.org", “userName”=”abc@xyz.com", " {produce.short.name}MgmtIp"="2.2.2.2",“apIpAddress”=”10.1.4.11”
Displayed on the web interface	[{srcProcess}] sending dummy response for Accounting Packet received from AP [{apIpAddress}] on {produce.short.name} [{SZMgmtIp}], with username [{userName}]. Configuration is incorrect in {produce.short.name} to forward received message nor to generate CDR
Description	This event occurs when the controller sends a dummy response to the AP accounting message 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 135 AP account message drop while no accounting start message event

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

Unauthorized COA/DM message dropped

TABLE 136 Unauthorized COA/DM message dropped event

Event	Unauthorized COA/DM message dropped
Event Type	unauthorizedCoaDmMessageDropped
Event Code	1911
Severity	Critical
Attribute	mvnoId"=12 "wlanId"=1,"zoneId"="10" "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="aut" "realm"="wlan.3gppnetwork.org" “userName”=”abc@xyz.com", “radSrvrIp”=”7.7.7.7”,"SZMgmtIp"="2.2.2.2"
Displayed on the web interface	[{srcProcess}] Dropped CoA/DM Packet received from AAA [{radSrvrIp}] on {produce.short.name} [{SZMgmtIp}], with username [{userName}]. Received message from unauthorized AAA
Description	This event occurs when the controller receives a change of authorization (CoA) or dynamic multipoint (DM) messages from an unauthorized AAA server.

NOTE
Refer to Accounting Alarms on page 29.

AP Communication Events

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

AP discovery succeeded on page 92	AP managed on page 92	AP rejected on page 92
AP firmware updated on page 92	AP firmware update failed on page 93	Updating AP firmware on page 93
Updating AP configuration on page 93	AP configuration updated on page 94	AP configuration update failed on page 94
AP pre-provision model mismatched on page 94	AP swap model mismatched on page 95	AP WLAN oversubscribed on page 95
AP illegal to change country code on page 95	AP configuration get failed on page 96	Rogue AP on page 96
Rogue AP disappeared on page 96	Classified Rogue AP on page 97	AP image signing failed on page 97
Jamming attack on page 97	Key gen fail on page 98	Key dis fail on page 98
Key dis fail GTK on page 98	wpaendec fail on page 98	IPsecses fail on page 99
Fw manual initiation on page 99	AP Management TSF data on page 99	AP TSF failure on page 100
AP Self tests on page 100	Firmware initiation update on page 100	Discontinuous channel on page 101
SSH initiation on page 101	SSH termination on page 101	SSH failure on page 102
TLS initiation on page 102	TLS termination on page 102	TLS failure on page 103
IP sec initiation on page 103	IP sec termination on page 103	IP sec failure on page 104

AP discovery succeeded

TABLE 137 AP discovery succeeded event

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

AP managed

TABLE 138 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 139 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 140 AP firmware updated event

Event	AP firmware updated
Event Type	apFirmwareUpdated

TABLE 140 AP firmware updated event (continued)

Event	AP firmware updated
Event Code	106
Severity	Informational
Attribute	“apMac”=“xxx.xxx.xxx.xxx” , “configID”=“23456781234”, "toVersion"="3.2.0.0.539", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{apName&&apMac}] updated its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP successfully updates the firmware details to the controller.

AP firmware update failed

TABLE 141 AP firmware update failed event

Event	AP firmware update failed
Event Type	apFirmwareUpdateFailed
Event Code	107
Severity	Major
Attribute	“apMac”=“xxx.xxx.xxx.xxx” , “configID”=“23456781234”, "toVersion"="3.2.0.0.x", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{apName&&apMac}] failed to update its firmware from [{fromVersion}] to [{toVersion}].
Description	This event occurs when the AP fails to update the firmware details to the controller.
Auto Clearance	This event triggers the alarm 107, which is auto cleared by the event code 106.

Updating AP firmware

TABLE 142 Updating AP firmware event

Event	Updating AP firmware
Event Type	apFirmwareApplying
Event Code	108
Severity	Informational
Attribute	“apMac”=“xxx.xxx.xxx.xxx” , “configID”=“23456781234”, "toVersion"="3.2.0.0.x", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{apName&&apMac}] firmware is being updated from [{fromVersion}] to [{toVersion}].
Description	This event occurs when AP updates its firmware.

Updating AP configuration

TABLE 143 Updating AP configuration event

Event	Updating AP configuration
Event Type	apConfApplying

TABLE 143 Updating AP configuration event (continued)

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

AP configuration updated

TABLE 144 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 145 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 146 AP pre-provision model mismatched event

Event	AP pre-provision model mismatched
Event Type	apModelDiffWithPreProvConfig
Event Code	112
Severity	Major

TABLE 146 AP pre-provision model mismatched event (continued)

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

AP swap model mismatched

TABLE 147 AP swap model mismatched event

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

AP WLAN oversubscribed

TABLE 148 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 illegal to change country code

TABLE 149 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”

TABLE 149 AP illegal to change country code event (continued)

Event	AP illegal to change country code
Displayed on the web interface	AP [{apName&&apMac}] does not support country code change.
Description	This event occurs when attempting to change the country code for an AP. Changing of country code is not allowed.

AP configuration get failed

TABLE 150 AP configuration get failed event

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

Rogue AP

TABLE 151 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.

Rogue AP disappeared

TABLE 152 Rogue AP disappeared event

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

Classified Rogue AP

TABLE 153 Classified Rogue AP event

Event	Classified Rogue AP
Event Type	generalRogueAPDetected
Event Code	186
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac""=""xxx.xxx.xxx.xxx", "ssid""="xxxxxxxxxx", "channel"="xx", "rogueType"="xxxxx", "roguePolicyName"="xxxxx", "rogueRuleName"="xxxxx"
Displayed on the web interface	AP [{apName&&apMac}] has detected a rogue AP rogue AP[{rogueMac}] with SSID[{ssid}] on channel[{channel}] classified as [{rogueType}] because of rogue classification policy (policy[{roguePolicyName}], rule[{rogueRuleName}]).
Description	This event occurs when the AP detects a rogue AP(malicious/known) that is classified by configurable rogue policy and its rules.

AP image signing failed

TABLE 154 AP image signing failed event

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

NOTE

Refer to AP Communication Events on page 91.

Jamming attack

TABLE 155 Jamming attack event

Event	Jamming attack
Event Type	jammingDetected
Event Code	189
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "rogueMac""=""xxx.xxx.xxx.xxx", "ssid""="xxxxxxxxxx", "channel"="xx" "rogueType"="xxxxx" "roguePolicyName"="xxxxx" "rogueRuleName"="xxxxx"
Displayed on the web interface	A jamming rogue AP[{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}].
Description	This event occurs when an AP detects a radio jamming attack.

Key gen fail

TABLE 156 Key gen fail event

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

Key dis fail

TABLE 157 Key dis fail event

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

Key dis fail GTK

TABLE 158 Key dis fail GTK event

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

wpaendec fail

TABLE 159 WpaEnDec fail event

Event	WpaEnDec fail
Event Type	wpaEnDecFail
Event Code	99003
Severity	Critical

TABLE 159 WpaEnDec fail event (continued)

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

IPsecses fail

TABLE 160 IPsecSes fail event

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

Fw manual initiation

TABLE 161 Fw manual initiation event

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

AP Management TSF data

TABLE 162 AP Management TSF data event

Event	AP Management TSF data
Event Type	APMGMNTTSFdata

TABLE 162 AP Management TSF data event (continued)

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

AP TSF failure

TABLE 163 AP TSF failure event

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

AP Self tests

TABLE 164 AP Self tests event

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

Firmware initiation update

TABLE 165 Firmware initiation update event

Event	Firmware initiation update
Event Type	FwInitiationUpdate
Event Code	99013
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”,

TABLE 165 Firmware initiation update event (continued)

Event	Firmware initiation update
	“apMac”=“xx:xx:xx:xx:xx:xx”, " rsm_fw_update(FW_TYPE_TDTS_RULE) ret=1 no update" “apMac”=“xx:xx:xx:xx:xx:xx”, " rsm_fw_update(FW_TYPE_TDTS_RULE) ret=%d Successful update" “apMac”=“xx:xx:xx:xx:xx:xx”, " rsm_fwd_update(FW_TYPE_TDTS_RULE) ret=1 fail"
Displayed on the web interface	AP [{apMac}] has is firmware update, reason: [{reason}].
Description	This event occurs whenever there is firmware update.

Discontinuous channel

TABLE 166 Discontinuous channel event

Event	Discontinuous channel
Event Type	Disconti Chan
Event Code	99014
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”,Discontinuous change of time through NTP server from SZ.The time got from SCG: %lu, Delta: %.0lf, the Current time in AP: %lu
Displayed on the web interface	AP [{apMac}] syncs it's time with SZ, reason: [{reason}].
Description	This event occurs, whenever AP syncs it's time with SZ.

SSH initiation

TABLE 167 SSH initiation event

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

SSH termination

TABLE 168 SSH termination event

Event	SSH termination
Event Type	sshTermination
Event Code	99019

TABLE 168 SSH termination event (continued)

Event	SSH termination
Severity	Major
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”, "SSH session exited"
Displayed on the web interface	There is exit from established SSH session, AP: [{apMac}].
Description	This event occurs whenever there is exit from established SSH session

SSH failure

TABLE 169 SSH failure event

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

TLS initiation

TABLE 170 TLS initiation event

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

TLS termination

TABLE 171 TLS termination event

Event	TLS termination
Event Type	tlsTermination
Event Code	99022
Severity	Major
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”, "HTTPS Logout successful"
Displayed on the web interface	There is logout from AP [{apMac}] web-GUI session.

TABLE 171 TLS termination event (continued)

Event	TLS termination
Description	This event occurs whenever there is logout from AP web-GUI session or AP gracefully terminates a trusted TLS connection.

TLS failure

TABLE 172 TLS failure event

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

IP sec initiation

TABLE 173 IP sec initiation event

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

IP sec termination

TABLE 174 IP sec termination event

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

IP sec failure

TABLE 175 IP sec failure event

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

AP LBS Events

Following are the events related to AP Location Based Service.

No LS responses

TABLE 176 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 177 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 178 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 179 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 180 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 181 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 182 AP received passive calibration request event

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

AP received passive footfall request

TABLE 183 AP received passive footfall request event

Event	AP received passive footfall request
Event Type	apLBSRcvdPassiveFFReq
Event Code	708
Severity	Informational

TABLE 183 AP received passive footfall request event (continued)

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

AP received unrecognized request

TABLE 184 AP received unrecognized request event

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

NOTE
Refer to AP LBS Alarms on page 36.

AP Mesh Events

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

EMAP downlink connected to MAP on page 108	EMAP downlink disconnected from MAP on page 108	EMAP uplink connected to MAP on page 108
EMAP uplink disconnected from MAP on page 108	MAP disconnected on page 109	MAP downlink connected on page 109
MAP downlink connected to EMAP on page 109	MAP downlink disconnected from EMAP on page 110	RAP downlink connected to MAP on page 110
MAP uplink connected to EMAP on page 110	MAP uplink disconnected from EMAP on page 110	MAP uplink connected to RAP on page 111
MAP uplink connected to MAP on page 111	Mesh state updated to MAP on page 111	Mesh state updated to MAP no channel on page 112
Mesh state updated to RAP on page 112	Mesh state update to RAP no channel on page 112	MAP downlink connected to MAP on page 113
MAP downlink disconnected from MAP on page 113	RAP downlink disconnected from MAP on page 113	

EMAP downlink connected to MAP

TABLE 185 EMAP downlink connected to MAP event

Event	EMAP downlink connected to MAP
Event Type	emapDlinkConnectWithMap
Event Code	405
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	eMAP [{apName&&apMac}] accepted connection from MAP [{mapName&&mapMac}].
Description	This event occurs when the mobile application part (MAP) to Ethernet Mesh AP (EMAP) connection is successful.

EMAP downlink disconnected from MAP

TABLE 186 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 187 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 188 EMAP uplink disconnected from MAP event

Event	EMAP uplink disconnected from MAP
Event Type	emapUlinkDisconnectWithMap
Event Code	408
Severity	Informational

TABLE 188 EMAP uplink disconnected from MAP event (continued)

Event	EMAP uplink disconnected from MAP
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 189 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 190 MAP downlink connected event

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

MAP downlink connected to EMAP

TABLE 191 MAP downlink connected to EMAP event

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

MAP downlink disconnected from EMAP

TABLE 192 MAP downlink disconnected from EMAP event

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

RAP downlink connected to MAP

TABLE 193 RAP downlink connected to MAP event

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

MAP uplink connected to EMAP

TABLE 194 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 195 MAP uplink disconnected from EMAP event

Event	MAP uplink disconnected from EMAP
Event Type	mapUlinkDisconnectToeMap

TABLE 195 MAP uplink disconnected from EMAP event (continued)

Event	MAP uplink disconnected from EMAP
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 196 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 197 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 198 Mesh state updated to MAP event

Event	Mesh state updated to MAP
Event Type	meshStateUpdateToMap
Event Code	421
Severity	Informational

TABLE 198 Mesh state updated to MAP event (continued)

Event	Mesh state updated to MAP
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 199 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 200 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 201 Mesh state update to RAP no channel event

Event	Mesh state update to RAP no channel
Event Type	meshStateUpdateToRapNoChannel

TABLE 201 Mesh state update to RAP no channel event (continued)

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

MAP downlink connected to MAP

TABLE 202 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 203 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 204 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

TABLE 205 AP rebooted by user event

Event	AP rebooted by user
Event Type	apRebootByUser
Event Code	301
Severity	Informational

TABLE 205 AP rebooted by user event (continued)

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

AP rebooted by system

TABLE 206 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 207 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 208 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 209 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 210 AP channel updated event

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

AP country code updated

TABLE 211 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 212 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 213 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 214 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 215 AP deleted event

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

AP heartbeat lost

TABLE 216 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 217 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 218 AP cable modem interface down event

Event	AP cable modem interface down
Event Type	cableModemDown
Event Code	316
Severity	Major

TABLE 218 AP cable modem interface down event (continued)

Event	AP cable modem interface down
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 219 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 220 AP cable modem power-cycled by user event

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

AP smart monitor turn off WLAN

TABLE 221 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)}]

TABLE 221 AP smart monitor turn off WLAN event (continued)

Event	AP smart monitor turn off WLAN
Description	This event occurs when the smart monitor of the AP turns off the WLAN.

AP client load balancing limit reached

TABLE 222 AP client load balancing limit reached event

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

AP client load balancing limit recovered

TABLE 223 AP client load balancing limit recovered event

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

AP WLAN state changed

TABLE 224 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"

TABLE 224 AP WLAN state changed event (continued)

Event	AP WLAN state changed
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 225 AP capacity reached event

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

AP capacity recovered

TABLE 226 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 227 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 228 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 229 AP cable modem set to factory default by user event

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

AP health high latency flag

TABLE 230 AP health high latency flag event

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

AP health low capacity flag

TABLE 231 AP health low capacity flag event

Event	AP health low capacity flag
Event Type	apHealthCapacityFlag

TABLE 231 AP health low capacity flag event (continued)

Event	AP health low capacity flag
Event Code	329
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current V alue"="xxxxx","configuredThreshold"="xxxxx", " radio" = "X.XG"
Displayed on the web interface	AP [{apName&&apMac}] flagged {{radio}} capacity health [{currentValue}] because it crossed the threshold [{configuredThreshold}].
Description	This event occurs when the AP is flagged because the radio has crossed the capacity health threshold configured by the administrator.

AP health high connection failure flag

TABLE 232 AP health high connection failure flag event

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

AP health high client count flag

TABLE 233 AP health high client count flag event

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

AP health high latency clear

TABLE 234 AP health high latency clear event

Event	AP health high latency clear
Event Type	apHealthLatencyClear
Event Code	332

TABLE 234 AP health high latency clear event (continued)

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

AP health low capacity clear

TABLE 235 AP health low capacity clear event

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

AP health high connection failure clear

TABLE 236 AP health high connection failure clear event

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

AP health high client count clear

TABLE 237 AP health high client count clear event

Event	AP health high client count clear
Event Type	apHealthClientCountClear
Event Code	335

TABLE 237 AP health high client count clear event (continued)

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

Primary DHCP AP is down

TABLE 238 Primary DHCP AP is down event

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

Primary DHCP AP is up

TABLE 239 Primary DHCP AP is up event

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

Secondary DHCP AP is down

TABLE 240 Secondary DHCP AP is down event

Event	Secondary DHCP AP is down detected by primary DHCPAP.
Event Type	apSecondaryDHCPAPDown
Event Code	338
Severity	Major

TABLE 240 Secondary DHCP AP is down event (continued)

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

Secondary DHCP AP is up

TABLE 241 Secondary DHCP AP is up event

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

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

TABLE 242 Primary or secondary DHCP AP detects 90% of the configured total IPs event

Event	Primary or secondary DHCP AP detects 90% of the configured total IPs
Event Type	apDHCPIPPoolMaxThresholdReached
Event Code	340
Severity	Warning
Attribute	"zoneName"="ZoneName", "poolId"="xxxx","vlanId"="1", "allocatedIPNum"="5", "totalIPNum"="10", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	In zone [{zoneName}] DHCP IP pool [{poolId}] reached 90% threshold detected by AP MAC [{apMac}]. VLAN ID: [{vlanId}] Allocated IPs: [{allocatedIPNum}], Total IPs: [{totalIPNum}].
Description	This event occurs when the primary or secondary DHCP AP reports that the IP pool has reached 90% of the total number of allocated IP addresses.

Both primary and secondary DHCP server APs are down

TABLE 243 Both primary and secondary DHCP server APs are down event

Event	Both primary and secondary DHCP server APs are down
Event Type	apDHCPServiceFailure
Event Code	341
Severity	Critical

TABLE 243 Both primary and secondary DHCP server APs are down event (continued)

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

AP NAT gateway IP failover detected for particular VLAN pool

TABLE 244 AP NAT gateway IP failover detected for particular VLAN pool event

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

AP NAT gateway IP fall back detected for particular VLAN pool

TABLE 245 AP NAT gateway IP fall back detected for particular VLAN pool event

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

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

TABLE 246 NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool event

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

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

TABLE 247 NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up event

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

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

TABLE 248 AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down event

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

AP health high airtime utilization flag

TABLE 249 AP health high airtime utilization flag event

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

AP health high airtime utilization clear

TABLE 250 AP health high airtime utilization clear event

Event	AP health high airtime utilization clear
Event Type	apHealthAirUtilizationClear
Event Code	348
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "currentValue"="xxxxx", "configuredThreshold"="xxxxx", "radio"="X.XG"
Displayed on the web interface	AP [{apName&&apMac}] cleared {{radio}} airtime utilization health [{currentValue}], which is no longer past the threshold [{configuredThreshold}].

TABLE 250 AP health high airtime utilization clear event (continued)

Event	AP health high airtime utilization clear
Description	This event occurs when an AP's health flag is cleared because it is no longer past the latency threshold configured by the administrator.

AP cluster failover

TABLE 251 AP cluster failover event

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

AP cluster rehome

TABLE 252 AP cluster rehome event

Event	AP cluster rehome
Event Type	apRehomeFailover
Event Code	350
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”, “oldWsgIP”=“xxx.xxx.xxx.xxx”, “newWsgIP”=“xxx.xxx.xxx.xxx”
Displayed on the web interface	AP [{apName&&apMac}] on zone [{zoneName}] is rehomed from {produce.short.name} [{oldCpName||oldWsgIP}] to {produce.short.name} [{cpName||newWsgIP}].
Description	This event occurs when an AP is rehomed from a standby to a primary cluster.

NOTE
Refer to AP State Change Alarms on page 37.

Backhaul switched to primary

TABLE 253 Backhaul switched to primary event

Event	Backhaul switched to primary
Event Type	changeToPrimaryBackhaul
Event Code	9100
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”, currBackhaul = "eth0"

TABLE 253 Backhaul switched to primary event (continued)

Event	Backhaul switched to primary
Displayed on the web interface	AP [{apName&&apMac}] Backhaul switched to primary - [{currBackhaul}]
Description	This event occurs when Backhaul switched to primary.

Backhaul switched to secondary

TABLE 254 Backhaul switched to secondary event

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

LTE network connectivity lost

TABLE 255 LTE network connectivity lost event

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

Ethernet network connectivity lost

TABLE 256 Ethernet network connectivity lost vent

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

LTE DHCP timeout

TABLE 257 LTE DHCP timeout event

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

Ethernet link down

TABLE 258 Ethernet link down event

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

Ethernet link up

TABLE 259 Ethernet link up event

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

SIM switch

TABLE 260 SIM switch event

Event	SIM switch
Event Type	simSwitch
Event Code	9107
Severity	Informational

TABLE 260 SIM switch event (continued)

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

Remote host blacklisted

TABLE 261 Remote host blacklisted event

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

SIM removal

TABLE 262 SIM removal event

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

LTE network registration status

TABLE 263 LTE network registration status event

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

LTE connection status

TABLE 264 LTE connection status event

Event	LTE connection status
Event Type	lteConnectionStatus
Event Code	9111
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”, currSim = "SIM 0", currConnStatus = "3G"
Displayed on the web interface	AP [{apName&&apMac}] [{currSim}] Cellular connection status - [{currConnStatus}]
Description	This event occurs whenever there is a change in the LTE connection status.

AP Authentication Events

Following are the events related to AP authentication.

Radius server reachable

TABLE 265 Radius server reachable event

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

Radius server unreachable

TABLE 266 Radius server unreachable event

Event	Radius server unreachable
Event Type	radiusServerUnreachable
Event Code	2102
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach radius server [{ip}].
Description	This event occurs when AP is unable to reach the RADIUS server.
Auto Clearance	This event triggers the alarm 2102, which is auto cleared by the event code 2101.

LDAP server reachable

TABLE 267 LDAP server reachable event

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

LDAP server unreachable

TABLE 268 LDAP server unreachable event

Event	LDAP server unreachable
Event Type	ldapServerUnreachable
Event Code	2122
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach LDAP server [{ip}].
Description	This event occurs when the AP is unable to reach the LDAP server.
Auto Clearance	This event triggers the alarm 2122, which is auto cleared by the event code 2121.

AD server reachable

TABLE 269 AD server reachable event

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

AD server unreachable

TABLE 270 AD server unreachable event

Event	AD server unreachable
Event Type	adServerUnreachable
Event Code	2142
Severity	Major
Attribute	apMac="xx:xx:xx:xx:xx:xx","ip"="17.0.0.12","fwVersion"="3.2.0.0.x","model"="ZF7982","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apLocation"=""
Displayed on the web interface	AP [{apName&&apMac}] is unable to reach AD server [{ip}].
Description	This event occurs when AP is unable able to reach the active directory.
Auto Clearance	This event triggers the alarm 2142, which is auto cleared by the event code 2141.

Wechat ESP authentication server reachable

TABLE 271 Wechat ESP authentication server reachable event

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

WeChat ESP authentication server unreachable

TABLE 272 WeChat ESP authentication server unreachable event

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

WeChat ESP authentication server resolvable

TABLE 273 WeChat ESP authentication server resolvable event

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

WeChat ESP authentication server unresolvable

TABLE 274 WeChat ESP authentication server unresolvable event

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

WeChat ESP DNAT server reachable

TABLE 275 WeChat ESP DNAT server reachable event

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

WeChat ESP DNAT server unreachable

TABLE 276 WeChat ESP DNAT server unreachable event

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

WeChat ESP DNAT server resolvable

TABLE 277 WeChat ESP DNAT server resolvable event

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

WeChat ESP DNAT server unresolvable

TABLE 278 WeChat ESP DNAT server unresolvable event

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

Authentication Attempts

TABLE 279 Authentication attempt event

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

Authentication Unsuccessful

TABLE 280 Authentication unsuccessful event

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

Authentication Re-attempt

TABLE 281 Authentication re-attempt event

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

Authentication 8021

TABLE 282 Authentication 8021 client event

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

AP Local Session Timeout

TABLE 283 AP local session timeout event

Event	AP Local Session Timeout
Event Type	apLocalSessionTimeout
Event Code	99015

TABLE 283 AP local session timeout event (continued)

Event	AP Local Session Timeout
Severity	Informational
Attribute	“apMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Local AP [{apMac}] session terminates due to session timeout.
Description	This event occurs when local AP session terminates due to session timeout.

AP Remote Session Timeout

TABLE 284 AP Remote session timeout event

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

AP Interactive Session Termination

TABLE 285 AP Interactive Session Termination event

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

AP USB Events

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

AP USB software package downloaded

TABLE 286 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 287 AP USB software package download failed event

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

Authentication Events

The following are the events related to authentication.

Authentication server not reachable

TABLE 288 Authentication server not reachable event

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

Authentication failed over to secondary

TABLE 289 Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Failed Over from Primary [{primary}] to Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the secondary authentication RADIUS server is available after the primary server becomes zombie or dead.

Authentication fallback to primary

TABLE 290 Authentication fallback to primary event

Event	Authentication fallback to primary
Event Type	authFallbackToPrimary
Event Code	1652
Severity	Major
Attribute	“mvnoId”=12 “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" “radProxyIp”=”7.7.7.7” “primary"=”20.20.20.20” “secondary”=”30.30.30.30” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the automatic fallback is enabled. The authentication failover to secondary server has occurred, the revival timer for primary server has expired and the requests falls back to the primary server.

AD/LDAP connected successfully

TABLE 291 AD/LDAP connected successfully event

Event	AD/LDAP connected successfully
Event Type	racADLDAPSuccess
Event Code	1751
Severity	Debug
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”= “1.1.1.1” "SZMgmtIp"="2.2.2.2", “desc”=”Successful connection to AD/LDAP”
Displayed on the web interface	[{srcProcess}] Connect to AD/LDAP[{authSrvrIp}] successfully from SCG[{SZMgmtIp}]
Description	This event occurs when RADIUS connection to AD/LDAP server is successful.

AD/LDAP connectivity failure

TABLE 292 AD/LDAP connectivity failure event

Event	AD/LDAP connectivity failure
Event Type	racADLDAPFail
Event Code	1752
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, "SZMgmtIp"="2.2.2.2" “desc”= "Connection to AD/LDAP fails"
Displayed on the web interface	[{srcProcess}] Connect to AD/LDAP[{authSrvrIp}] fails from SCG[{SZMgmtIp}]
Description	This event occurs when RADIUS fails to connect to AD/LDAP server.

Bind fails with AD/LDAP

TABLE 293 Bind fails with AD/LDAP event

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

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

TABLE 294 Bind success with LDAP, but unable to find clear text password for the user event

Event	Bind success with LDAP but unable to find clear text password for the user
Event Type	racLDAPFailToFindPassword
Event Code	1754
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”= “testuser’ "SZMgmtIp"="2.2.2.2", “desc”=”Fail to find password”
Displayed on the web interface	[{srcProcess}] failed to find password from LDAP [{authSrvrIp}] for SCG[{SZMgmtIp}] for User[{userName}]
Description	This event occurs when binding is successful with LDAP using root credential but is unable to retrieve the clear text password for the user.

RADIUS fails to connect to AD NPS server

TABLE 295 RADIUS fails to connect to AD NPS server event

Event	RADIUS fails to connect to AD NPS server
Event Type	racADNPSFail
Event Code	1755
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”= ”Fails to connect to AD NPS server”
Displayed on the web interface	[{srcProcess}] Fails to connect to AD NPS [{authSrvrIp}] from SCG[{SZMgmtIp}]
Description	This event occurs when RADIUS fails to connect to AD NPS server.

RADIUS fails to authenticate with AD NPS server

TABLE 296 RADIUS fails to authenticate with AD NPS server event

Event	RADIUS fails to authenticate with AD NPS server
Event Type	racADNPSFailToAuthenticate
Event Code	1756
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff”, “mvnoId”=12, “srcProcess”=”RAC”, “authSrvrIp”=“1.1.1.1”, “username”=“testuser’ "SZMgmtIp"="2.2.2.2", “desc”=”Fails to authenticate with AD NPS”
Displayed on the web interface	[{srcProcess}] Fails to authenticate AD NPS[{authSrvrIp}] on SCG [{SZMgmtIp}] for User[{userName}]
Description	This event occurs when RADIUS fails to authenticate with AD NPS server.

NOTE
Refer to Authentication Alarms on page 41.

Successfully established the TLS tunnel with AD/LDAP

TABLE 297 Successfully established the TLS tunnel with AD/LDAP event

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

Fails to establish TLS tunnel with AD/LDAP

TABLE 298 Fails to establish TLS tunnel with AD/LDAP event

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

NOTE

Refer to Authentication Alarms on page 41

Authorization Events

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

- DM received from AAA on page 147
- DM NACK sent to AAA on page 147
- DM sent to NAS on page 147
- DM NACK received from NAS on page 148

DM received from AAA

TABLE 299 DM received from AAA event

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

DM NACK sent to AAA

TABLE 300 DM NACK sent to AAA event

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

DM sent to NAS

TABLE 301 DM sent to NAS event

Event	DM sent to NAS
Event Type	dmSntNAS
Event Code	1643
Severity	Debug

TABLE 301 DM sent to NAS event (continued)

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

DM NACK received from NAS

TABLE 302 DM NACK received from NAS event

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

CoA received from AAA

TABLE 303 CoA received from AAA event

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

CoA NACK sent to AAA

TABLE 304 CoA NACK sent to AAA event

Event	CoA NACK sent to AAA
Event Type	coaNackSntAAA

TABLE 304 CoA NACK sent to AAA event (continued)

Event	CoA NACK sent to AAA
Event Code	1646
Severity	Debug
Attribute	“mvnoId”=”2” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radius” “userName”=”user name" “radSrvrIp”=”7.7.7.7” "rmtRadSrvrIp"="40.40.40.40" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	RADIUS CoA NACK sent by RAC [{radSrvrIp}] to AAA [{rmtRadSrvrIp}] for [{userName}]
Description	This event occurs when radio access control sends a change of authorization, not acknowledged to the AAA server.

CoA sent NAS

TABLE 305 CoA sent NAS event

Event	CoA sent NAS
Event Type	coaSentNas
Event Code	1647
Severity	Debug
Attribute	“mvnoId”=”12” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “userName”=”abc@xyz.com” “radSrvrIp”=”1.1.1.1” “nasIp”=”3.3.3.3” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA requests proxied/forwarded to NAS(AP) [{nasIp}].
Description	This event occurs when the controller forwards/proxy of change of authorization to the NAS server.

CoA NAK received NAS

TABLE 306 CoA NAK received NAS event

Event	CoA NAK received NAS
Event Type	coaNakRcvdNas
Event Code	1648
Severity	Debug
Attribute	“mvnoId”=”12” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “userName”=”abc@xyz.com” “radSrvrIp”=”1.1.1.1” “nasIp”=”3.3.3.3” "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	CoA NAK received from NAS(AP) for forwarded/proxied CoA [{radSrvrIp}]
Description	This event occurs when a change of authorization, not acknowledged is received from the NAS server.

CoA authorize only access reject

TABLE 307 CoA authorize only access reject event

Event	CoA authorize only access reject
Event Type	coaAuthorizeOnlyAccessReject
Event Code	1649
Severity	Critical
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” “userName”=”abc@xyz.com” “realm”= ”wlan.mnc080.mcc405.3gppnetwork.org" "SZMgmtIp"="2.2.2.2" “apType” = “” “ueMacAddr”=”aa:bb:cc:gg:hh:ii” "rmtRadSrvrIp"="40.40.40.40"
Displayed on the web interface	CoA Authorize Only unsuccessful for AAA Server [rmtRadSrvrIp] for UE [ueMacAddr]
Description	This event occurs when the change of authorization is rejected.

CoA RWSG MWSG notification failure

TABLE 308 CoA RWSG MWSG notification failure event

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

Control and Data Plane Interface Events

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

DP connected

TABLE 309 DP connected event

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

GtpManager (DP) disconnected

TABLE 310 GtpManager (DP) disconnected event

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

Session updated at DP

TABLE 311 Session updated at DP event

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

Session update at DP failed

TABLE 312 Session update at DP failed event

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

Session deleted at DP

TABLE 313 Session deleted at DP event

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

Session delete at DP failed

TABLE 314 Session delete at DP failed event

Event	Session delete at DP failed
Event Type	sessDeleteErrAtDblade
Event Code	1208
Severity	Debug
Attribute	“mvnoId”=”12” “wlanId”=”1” “zoneId”=”10” “ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”realm sent by UE” “ctrlBladeIp”=”1.1.1.1” "dataBladeIp"="3.3.3.3" "SZMgmtIp"="2.2.2.2" “ueMacAddr”=”aa:bb:cc:gg:hh:ii” “ueImsi”=”12345” “ueMsisdn”=”98787”

TABLE 314 Session delete at DP failed event (continued)

Event	Session delete at DP failed
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has failed to delete from Data plane [{dataBladeIp}] by Control plane [{ctrlBladeIp}] at {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the session delete request (C-D-SESS-DEL-REQ) results in a timeout or a failed response.

C2d configuration failed

TABLE 315 C2d configuration failed event

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

NOTE
Refer to Control and Data Plane Interface Alarms on page 46.

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

TABLE 316 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 317 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 318 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 319 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 320 Client connection timed out event

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

Client authorization successfully

TABLE 321 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 322 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 323 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 324 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 325 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.

TABLE 325 Client logged out event (continued)

Event	Client logged out
Description	This event occurs when a client session is logged out.

Client roaming disconnected

TABLE 326 Client roaming disconnected event

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

Client blocked

TABLE 327 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 328 Client grace period event

Event	Client grace period
Event Type	clientGracePeriod
Event Code	220
Severity	Informational

TABLE 328 Client grace period event (continued)

Event	Client grace period
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 329 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 330 Onboarding registration failed event

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

Remediation succeeded

TABLE 331 Remediation succeeded event

Event	Remediation succeeded
Event Type	remediationSuccess
Event Code	223

TABLE 331 Remediation succeeded event (continued)

Event	Remediation succeeded
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 332 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 333 Force DHCP disconnected event

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

WDS device joined

TABLE 334 WDS device joined event

Event	WDS device joined
Event Type	wdsDeviceJoin
Event Code	226
Severity	Informational

TABLE 334 WDS device joined event (continued)

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

WDS device left

TABLE 335 WDS device left event

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

Client is blocked because of barring UE rule

TABLE 336 Client is blocked because of barring UE rule event

Event	Client is blocked because of barring UE rule
Event Type	clientBlockByBarringUERule
Event Code	228
Severity	Informational
Attr ibute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Client [clientMac}] of WLAN [{ssid}] from AP [{apName&&apMac}] was blocked because of barring UE rule.
Description	This event occurs when a client is temporally blocked by the UE barring rule.

Client is unblocked by barring UE rule

TABLE 337 Client is unblocked by barring UE rule event

Event	Client is unblocked by barring UE rule
Event Type	clientUnblockByBarringUERule
Event Code	229
Severity	Informational
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx"

TABLE 337 Client is unblocked by barring UE rule event (continued)

Event	Client is unblocked by barring UE rule
Displayed on the web interface	Client [clientMac}] of WLAN [{ssid}] from AP [{apName&&apMac}] was unblocked
Description	This event occurs when a client is unblocked by the UE barring rule.

Start CALEA mirroring client

TABLE 338 Start CALEA mirroring client event

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

Stop CALEA mirroring client

TABLE 339 Stop CALEA mirroring client event

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

Wired client joined

TABLE 340 Wired client joined event

Event	Wired client joined
Event Type	wiredClientJoin
Event Code	2802
Severity	Informational
Attribute	apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ethProfileId"="xxxxx", "ethPort"="x", "iface"="xxxx", "tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxxx","vlanId"="x"

TABLE 340 Wired client joined event (continued)

Event	Wired client joined
Displayed on the web interface	Client [{userName||IP||clientMac}] joined LAN [{ethPort}] from AP [{apName&&apMac}].
Description	This event occurs when a client joins the LAN AP.

Wired client failed to join

TABLE 341 Wired client failed to join event

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

Wired client disconnected

TABLE 342 Wired client disconnected event

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

Wired client authorization successfully

TABLE 343 Wired client authorization successfully event

Event	Wired client authorization successfully
Event Type	wiredClientAuthorization
Event Code	2806
Severity	Informational
Attribute	apMac"="xx:xx:xx:xx:xx:xx", "clientMac"="xx:xx:xx:xx:xx:xx", "ethProfileId"="xxxxx", "ethPort"="x", "iface"="xxxx",

TABLE 343 Wired client authorization successfully event (continued)

Event	Wired client authorization successfully
	"tenantUUID"="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "apName"="xxxx","vlanId"="x", "userName"="xxxx"
Displayed on the web interface	Client [{userName||IP||clientMac}] of LAN [{ethPort}] from AP [{apName&&apMac}] was authorized.
Description	This event occurs when a client on WLAN AP is authorized.

Wired client session expired

TABLE 344 Wired client session expired event

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

Application identified

TABLE 345 Application identified event

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

Application denied

TABLE 346 Application denied event

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

TABLE 346 Application denied event (continued)

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

URL filtering server unreachable

TABLE 347 URL filtering server unreachable event

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

URL filtering server reachable

TABLE 348 URL filtering server reachable event

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

Packet spoofing detected

TABLE 349 Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWireless
Event Code	232
Severity	Major
Attribute	"desc"="xxxxx", "clientMac"="xx:xx:xx:xx:xx:xx", "clientIP"="x.x.x.x","ssid"="xxxxx", "networkInterface" = "xxxxxx","apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Packet spoofing detected [{desc}] from client [{clientMac&&clientIP}] on WLAN [{ssid}] [{networkInterface}] from AP [{apName&&apMac}]

TABLE 349 Packet spoofing detected event (continued)

Event	Packet spoofing detected
Description	This event occurs when packet spoofing is detected from wireless by antispoofing feature.

Packet spoofing detected

TABLE 350 Packet spoofing detected event

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

Packet spoofing detected

TABLE 351 Packet spoofing detected event

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

Packet spoofing detected

TABLE 352 Packet spoofing detected event

Event	Packet spoofing detected
Event Type	packetSpoofingDetectedFromWiredSourceMacSpoofed
Event Code	235
Severity	Major
Attribute	"desc"="xxxxx", "packetDropCount"="xxxx", "networkInterface" = "xxxxxx","apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx"

TABLE 352 Packet spoofing detected event (continued)

Event	Packet spoofing detected
Displayed on the web interface	Packet spoofing detected [{desc}], packets [{packetDropCount}] were dropped on [{networkInterface}] from AP [{apName&&apMac}]
Description	This event occurs when packet spoofing is detected from wired by antispoofing feature. It is a source MAC address spoof.

Cloud Events

The following are the events related to Cloud Based Service.

Cloud Services Enabled

TABLE 353 Cloud services enabled event

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

Cloud Services Disabled

TABLE 354 Cloud services disabled event

Event	Cloud services disabled
Event Type	CloudServicesdisabled
Event Code	4502
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Services have been disabled successfully.
Description	This event occurs when SZ successfully disabled Cloud Services.

Cloud Analytics Enabled

TABLE 355 Cloud analytics enabled event

Event	Cloud analytics enabled
Event Type	CloudAnalyticsEnabled
Event Code	4503
Severity	Informational
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics service has been enabled successfully.
Description	This event occurs when SZ successfully enabled Cloud Analytics service.

Cloud Analytics Disabled

TABLE 356 Cloud analytics disabled event

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

Cloud Services Token Refreshed

TABLE 357 Cloud services token refreshed event

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

Cloud Analytics Token Renewed

TABLE 358 Cloud analytics token renewed event

Event	Cloud analytics token renewed
Event Type	cloudAnalyticsTokenRenewed
Event Code	4602
Severity	Informational

TABLE 358 Cloud analytics token renewed event (continued)

Event	Cloud analytics token renewed
Attribute	No attribute for this event.
Displayed on the web interface	Cloud Analytics token has been renewed successfully.
Description	This event occurs when SZ successfully renewed Cloud Analytics access token.

Cluster Events

Following are the events related to clusters.

Cluster created successfully on page 170	New node joined successfully on page 170	New node failed to join on page 170
Node removal completed on page 170	Node removal failed on page 171	Node out of service on page 171
Cluster in maintenance state on page 171	Cluster back in service on page 172	Cluster backup completed on page 172
Cluster backup failed on page 172	Cluster restore completed on page 173	Cluster restore failed on page 173
Cluster node upgrade completed on page 173	Entire cluster upgraded successfully on page 174	Cluster upgrade failed on page 174
Cluster application stopped on page 174	Cluster application started on page 175	Cluster backup started on page 175
Cluster upgrade started on page 175	Cluster leader changed on page 175	Node bond interface down on page 176
Node bond interface up on page 176	Node IP address changed on page 176	Node physical interface down on page 177
Node physical interface up on page 177	Cluster node rebooted on page 177	NTP time synchronized on page 178
Cluster node shutdown on page 178	Cluster upload started on page 178	Cluster upload completed on page 178
Cluster upload failed on page 179	SSH tunnel switched on page 179	Cluster remove node started on page 179
Node back in service on page 180	Resync NTP time on page 180	Disk usage exceed threshold on page 180
Cluster out of service on page 181	Initiated moving APs in node to a new cluster on page 181	Cluster upload vSZ-D firmware started on page 181
Cluster upload vSZ-D firmware completed on page 182	Cluster upload vSZ-D firmware failed on page 182	Cluster upload AP firmware started on page 182
Cluster upload AP firmware completed on page 182	Cluster upload AP firmware failed on page 183	Cluster add AP firmware started on page 183
Cluster add AP firmware completed on page 183	Cluster add AP firmware failed on page 184	Cluster name is changed on page 184
Unsync NTP Time on page 184	Cluster upload KSP file started on page 185	Cluster upload KSP file completed on page 185
Cluster upload KSP file failed on page 185	Configuration backup started on page 186	Configuration backup succeeded on page 186
Configuration backup failed on page 186	Configuration restore succeeded on page 186	Configuration restore failed on page 187
AP Certificate Expired on page 187	AP Certificate Updated on page 187	Configuration restore started on page 188
Upgrade SSTable failed on page 188	Reindex elastic search finished on page 188	Initiated APs contact APR on page 189
All nodes back in service on page 189	Not management service ready on page 189	Management service ready on page 189
Configuration sync failed on page 190	Node IPv6 address added on page 190	Node IPv6 address deleted on page 190

Cluster created successfully

TABLE 359 Cluster created successfully event

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

New node joined successfully

TABLE 360 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 361 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 362 Node removal completed event

Event	Node removal completed
Event Type	removeNodeSuccess

TABLE 362 Node removal completed event (continued)

Event	Node removal completed
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 363 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 364 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 365 Cluster in maintenance state event

Event	Cluster in maintenance state
Event Type	clusterInMaintenanceState
Event Code	807
Severity	Critical

TABLE 365 Cluster in maintenance state event (continued)

Event	Cluster in maintenance state
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 366 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 367 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 368 Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810
Severity	Major
Attribute	“clusterName”=”xxx”
Displayed on the web interface	Cluster [{clusterName}] backup failed. Reason [{reason}].
Description	This event occurs when a cluster backup fails.

TABLE 368 Cluster backup failed event (continued)

Event	Cluster backup failed
Auto Clearance	This event triggers the alarm 805, which is auto cleared by the event code 809.

Cluster restore completed

TABLE 369 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 370 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 371 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 372 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 373 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 374 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 375 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 376 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 377 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 378 Cluster leader changed event

Event	Cluster leader changed
Event Type	clusterLeaderChanged
Event Code	820
Severity	Informational

TABLE 378 Cluster leader changed event (continued)

Event	Cluster leader changed
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 379 Node bond interface down event

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

Node bond interface up

TABLE 380 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 381 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}].

TABLE 381 Node IP address changed event (continued)

Event	Node IP address changed
Description	This event occurs when the node's network interface IP address changes.

Node physical interface down

TABLE 382 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 383 Node physical interface up event

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

Cluster node rebooted

TABLE 384 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 385 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 386 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 387 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 388 Cluster upload completed event

Event	Cluster upload completed
Event Type	uploadClusterSuccess

TABLE 388 Cluster upload completed event (continued)

Event	Cluster upload completed
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 389 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 390 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 391 Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834
Severity	Informational
Attribute	"clusterName"=”xxx”, "nodeName" =”xxx”, “nodeMac"=”xx:xx:xx:xx:xx:xx”

TABLE 391 Cluster remove node started event (continued)

Event	Cluster remove node started
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 392 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: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 393 Resync NTP time event

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

Disk usage exceed threshold

TABLE 394 Disk usage exceed threshold event

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

Cluster out of service

TABLE 395 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 396 Initiated moving APs in node to a new cluster event

Event	Initiated moving APs in node to a new cluster
Event Type	clusterInitiatedMovingAp
Event Code	844
Severity	Informational
Attribute	"nodeName"="xxx", "clusterName"="xxx"
Displayed on the web interface	Initiated moving APs in node [{nodeName}] of cluster [{clusterName}] to a new cluster.
Description	This event occurs when the command to move the APs in the node to another cluster is received.

NOTE
Events 845, 846 and 847 are not applicable for SZ.

Cluster upload vSZ-D firmware started

TABLE 397 Cluster upload vSZ-D firmware started event

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

Cluster upload vSZ-D firmware completed

TABLE 398 Cluster upload vSZ-D firmware completed event

Event	Cluster upload vSZ-D firmware completed
Event Type	uploadClusterVDPFirmwareSuccess
Event Code	846
Severity	Informational
Attribute	"clusterName"="xxx" "status"="StartTime:yyyy-MM-dd hh:mm:ss, EndTime:yyyy-MM-dd hh:mm:ss, Duration:hh:mm:ss"
Displayed on the web interface	Cluster [{clusterName}] upload vSZ-D firmware completed. [{status}]
Description	This event occurs when the cluster upload process of vSZ-data plane firmware is successful.

Cluster upload vSZ-D firmware failed

TABLE 399 Cluster upload vSZ-D firmware failed event

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

Cluster upload AP firmware started

TABLE 400 Cluster upload AP firmware started event

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

Cluster upload AP firmware completed

TABLE 401 Cluster upload AP firmware completed event

Event	Cluster upload AP firmware completed
Event Type	clusterUploadAPFirmwareSuccess

TABLE 401 Cluster upload AP firmware completed event (continued)

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

Cluster upload AP firmware failed

TABLE 402 Cluster upload AP firmware failed event

Event	Cluster upload AP firmware failed
Event Type	clusterUploadAPFirmwareFailed
Event Code	850
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] upload AP firmware failed. Reason:[{reason}].
Description	This event occurs when the cluster upload process to the AP firmware fails.

Cluster add AP firmware started

TABLE 403 Cluster add AP firmware started event

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

Cluster add AP firmware completed

TABLE 404 Cluster add AP firmware completed event

Event	Cluster add AP firmware completed
Event Type	clusterAddAPFirmwareSuccess
Event Code	852
Severity	Informational
Attribute	"clusterName"="xxx"

TABLE 404 Cluster add AP firmware completed event (continued)

Event	Cluster add AP firmware completed
Displayed on the web interface	Starting add AP firmware in cluster [{clusterName}]
Description	This event occurs when the cluster add process to the AP firmware is successful.

Cluster add AP firmware failed

TABLE 405 Cluster add AP firmware failed event

Event	Cluster add AP firmware failed
Event Type	clusterAddAPFirmwareFailed
Event Code	853
Severity	Major
Attribute	"reason"="xxx", "clusterName"="xxx"
Displayed on the web interface	Cluster [{clusterName}] add AP firmware failed. Reason:[{reason}].
Description	This event occurs when the cluster add process to the AP firmware fails.

Cluster name is changed

TABLE 406 Cluster name is changed event

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

Unsync NTP Time

TABLE 407 Unsync NTP Time event

Event	Unsync NTP Time
Event Type	unsyncNTPTime
Event Code	855
Severity	Major

TABLE 407 Unsync NTP Time event (continued)

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

Cluster upload KSP file started

TABLE 408 Cluster upload KSP file started event

Event	Cluster upload KSP file started
Event Type	clusterUploadKspFileStart
Event Code	856
Severity	Informational
Attribute	"clusterName"="xxx",
Displayed on the web interface	Cluster [{ clusterName}] upload KSP file completed.
Description	This event occurs when the cluster starts the upload process of the *ksp* file.

Cluster upload KSP file completed

TABLE 409 Cluster upload KSP file completed event

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

Cluster upload KSP file failed

TABLE 410 Cluster upload KSP file failed event

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

Configuration backup started

TABLE 411 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 412 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 413 Configuration backup failed event

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

Configuration restore succeeded

TABLE 414 Configuration restore succeeded event

Event	Configuration restore succeeded
Event Type	clusterCfgRestoreSuccess
Event Code	863

TABLE 414 Configuration restore succeeded event (continued)

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

Configuration restore failed

TABLE 415 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 416 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 417 AP Certificate Updated event

Event	AP Certificate Updated
Event Type	apCertificateExpireClear
Event Code	866
Severity	Informational
Attribute	"clusterName"="xxx"

TABLE 417 AP Certificate Updated event (continued)

Event	AP Certificate Updated
Displayed on the web interface	Clear AP certificate expiration alarm.
Description	This event occurs when the AP certificates are updated.

Configuration restore started

TABLE 418 Configuration restore started event

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

Upgrade SSTable failed

TABLE 419 Upgrade SSTable failed event

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

Reindex elastic search finished

TABLE 420 Reindex elastic search finished event

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

Initiated APs contact APR

TABLE 421 Initiated APs contact APR event

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

All nodes back in service

TABLE 422 All nodes back in service event

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

Not management service ready

TABLE 423 Not management service ready event

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

Management service ready

TABLE 424 Management service ready event

Event	Managementl service ready
Event Type	allServiceInService
Event Code	873
Severity	Informational

TABLE 424 Management service ready event (continued)

Event	Managementl service ready
Attribute	“clusterName”=“xx”, “nodeName”=“xx
Displayed on the web interface	All management services on Node [{nodeName}] in cluster [{clusterName}] are ready
Description	This event occurs when all applications of the node is in service and the management service state is marked as in service.

Configuration sync failed

TABLE 425 Configuration sync failedevent

Event	Configuration sync failed
Event Type	clusterRedundancySyncCfgFailed
Event Code	874
Severity	Major
Attribute	“clusterName”=“xx”, “reason”=“xxx”
Displayed on the web interface	Cluster [{clusterName}] configuration sync failed. Reason: [{reason}]
Description	This event occurs when synchronization configuration fails in a cluster redundancy.

Node IPv6 address added

TABLE 426 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 427 Node IPv6 address deleted event

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

NOTE
Refer to Cluster Alarms on page 47.

Configuration Events

Following are events related to configuration.

Configuration updated

TABLE 428 Configuration updated event

Event	Configuration updated
Event Type	cfgUpdSuccess
Event Code	1007
Severity	Informational
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”cnr” “realm”=”NA” “processName”=”aut” "SZMgmtIp"="2.2.2.2" “cause”=”detail of the configuration applied”
Displayed on the web interface	Configuration [{cause}] applied successfully in [{processName}] process at {produce.short.name} [{SZMgmtIp}]
Description	This event occurs when the configuration notification receiver (CNR) process successfully applies the configuration to the modules.

Configuration update failed

TABLE 429 Configuration update failed event

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

TABLE 429 Configuration update failed event (continued)

Event	Configuration update failed
Description	This event occurs when the CNR receives a negative acknowledgment when applying the configuration settings to the module. Possible cause is that a particular process/module is down.

Configuration receive failed

TABLE 430 Configuration receive failed event

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

Incorrect flat file configuration

TABLE 431 Incorrect flat file configuration event

Event	Incorrect flat file configuration
Event Type	incorrectFlatFileCfg
Event Code	1012
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”aut” “realm”=”NA” "SZMgmtIp"="2.2.2.2" “cause”=”mention the configuration that is not received properly” “file”=”mention the config file name”
Displayed on the web interface	[{srcProcess}] detected an configuration parameter is incorrectly configured in file [{file}] at {produce.short.name} [{SZMgmtIp}].
Description	This event occurs when any flat file configuration parameter is not semantically or syntactically correct.

Zone configuration preparation failed

TABLE 432 Zone configuration preparation failed event

Event	Zone configuration preparation failed
Event Type	zoneCfgPrepareFailed
Event Code	1021
Severity	Major
Attribute	"nodeMac"="50:A7:33:24:E7:90","zoneName"="openZone"

TABLE 432 Zone configuration preparation failed event (continued)

Event	Zone configuration preparation failed
Displayed on the web interface	Failed to prepare zone [{zoneName}] configuration required by ap configuration generation
Description	This event occurs when the controller is unable to prepare a zone configuration required by the AP.

AP configuration generation failed

TABLE 433 AP configuration generation failed event

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

End-of-life AP model detected

TABLE 434 End-of-life AP model detected event

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

VLAN configuration mismatch on non-DHCP/NAT WLAN

TABLE 435 VLAN configuration mismatch on non-DHCP/NAT WLAN event

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN.
Event Type	apCfgNonDhcpNatWlanVlanConfigMismatch
Event Code	1024
Severity	Critical
Attribute	"ssid"="xxxx", "configuredVlan"="5", "vlanId"="11", "apMac"="xx:xx:xx:xx:xx:xx"

TABLE 435 VLAN configuration mismatch on non-DHCP/NAT WLAN event (continued)

Event	VLAN configuration mismatch detected between configured and resolved VLAN with DVLAN/VLAN pooling configuration on non-DHCP/NAT WLAN.
Displayed on the web interface	DHCP/NAT gateway AP [{apMac}] detected VLAN configuration mismatch on non-DHCP/NAT WLAN [{ssid}]. Configured VLAN is [{configuredVlan}] and resolved VLAN is [{vlanId}]. Clients may not be able to get IP or access Internet.
Description	This event occurs when the AP detects a non DHCP/NAT WLAN. VLAN configuration mismatches with DVLAN/VLAN pooling configuration on gateway AP.

VLAN configuration mismatch on a DHCP/NAT WLAN

TABLE 436 VLAN configuration mismatch on DHCP/NAT WLAN event

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

NOTE
Refer to Configuration Alarms on page 57.

Datablade Events

The following are the events related to Datablade Based Service.

DP integrity test failed

TABLE 437 DP integrity test failed event

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

DP CLI enable failed

TABLE 438 DP CLI enable failed event

Event	DP CLI enable failed
Event Type	dpCliEnableFailed
Event Code	99201
Severity	Informational
Attribute	"dpKey"="XXXX","source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] CLI enabled failed, [{source}].
Description	This event occurs when the data plane CLI enabled failed.

DP re-authentication

TABLE 439 DP re-authentication event

Event	DP re-authentication
Event Type	dpReAuth
Event Code	99202
Severity	Informational
Attribute	"dpKey"="XXXX","Source"="x.x.x.x/console/WebGUI"

TABLE 439 DP re-authentication event (continued)

Event	DP re-authentication
Displayed on the web interface	Data plane [{dpKey}] attempt to re-authenticate, [{source}].
Description	This event occurs when the data plane attempt to re-authenticate.

DP password min length updated

TABLE 440 DP password min length updated event

Event	DP password min length updated
Event Type	dpPasswordMinLengthUpdated
Event Code	99203
Severity	Informational
Attribute	"dpKey"="XXXX","Source"="x.x.x.x/console/webGUI"
Displayed on the web interface	Data plane [{dpKey}] min password length changed, [{source}].
Description	This event occurs when the data plane min password length changed.

DP password changed

TABLE 441 DP password changed event

Event	DP password changed
Event Type	dpPasswordChanged
Event Code	99204
Severity	Informational
Attribute	"dpKey"="XXXX","Source"="x.x.x.x/console/webGUI"
Displayed on the web interface	Data plane [{dpKey}] password changed, [{source}].
Description	This event occurs when the data plane password changed.

DP enable password changed

TABLE 442 DP enable password changed event

Event	DP enable password changed
Event Type	dpEnablePasswordChanged
Event Code	99205
Severity	Informational
Attribute	"dpKey"="XXXX","Source"="x.x.x.x/console"
Displayed on the web interface	Data plane [{dpKey}] enable password changed, [{source}].
Description	This event occurs when the data plane enable password changed.

DP https authentication failed

TABLE 443 DP https authentication failed event

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

DP certificate uploaded

TABLE 444 DP certificate uploaded event

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

DP Scg FQDN updated

TABLE 445 DP Scg FQDN updated event

Event	DP Scg FQDN updated
Event Type	dpScgFqdnUpdated
Event Code	99208
Severity	Informational
Attribute	"dpKey"="XXXX","fqdn"="xxx.xxx.xxx"
Displayed on the web interface	SZ [{scgIP}] FQDN [{fqdn}] setting on DP [{dpKey}].
Description	This event occurs when the SZ FQDN setting on data plane.

DP initial upgrade

TABLE 446 DP initial upgrade event

Event	DP initial upgrade
Event Type	dpInitUpgrade
Event Code	99210
Severity	Informational

TABLE 446 DP initial upgrade event (continued)

Event	DP initial upgrade
Attribute	"dpKey"="XXXX", "source"="xxx"
Displayed on the web interface	Data plane [{dpKey}] initiate to upgrade, [{source}].
Description	This event occurs when the data plane initiate to upgrade.

DP discontinuous time change NTP server DP Ntp time sync

TABLE 447 DP discontinuous time change NTP server DP Ntp time sync event

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

DP user login

TABLE 448 DP user login event

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

DP user login failed

TABLE 449 DP user login failed event

Event	DP user login failed
Event Type	dpUserLoginFailed
Event Code	99213
Severity	Informational
Attribute	"dpKey"="XXXX","Source"="x.x.x.x/console"
Displayed on the web interface	User login into data plane [{dpKey}] and failed, Source: [{source}].
Description	This event occurs when the user login into data plane and failed.

DP user logout

TABLE 450 DP user logout event

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

DP account locked

TABLE 451 DP account locked event

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

DP session idle updated

TABLE 452 DP session idle updated event

Event	DP session idle updated
Event Type	dpSessionIdleUpdated
Event Code	99220
Severity	Informational
Attribute	"dpKey"="XXXX","sessionIdle"="xx","Source"="console/webGui"
Displayed on the web interface	Data plane [{dpKey}] session timeout [{sessionIdle}] change, [{source}].
Description	This event occurs when the data plane session timeout change.

DP session idle terminated

TABLE 453 DP session idle terminated event

Event	DP session idle terminated
Event Type	dpSessionIdleTerminated
Event Code	99221
Severity	Informational

TABLE 453 DP session idle terminated event (continued)

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

DP SSH tunnel failed

TABLE 454 DP SSH tunnel failed event

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

DP https connection failed

TABLE 455 DP https connection failed event

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

DP IPsec tunnel create failed

TABLE 456 DP IPsec tunnel create failed event

Event	DP IPsec tunnel create failed
Event Type	dpIPsecTunnCreateFailed
Event Code	99240
Severity	Informational
Attribute	"dpKey"="XXXX","dpIP"="x.x.x.x",apIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpKey&&dpIP}] IPsec tunnel establishment failed, AP [{apIP}].
Description	This event occurs when the data plane IPsec tunnel establishment failed.

Data Plane Events

Following are the events related to data plane.

Data plane discovered on page 201	Data plane discovery failed on page 202	Data plane configuration updated on page 202
Data plane configuration update failed on page 202	Data plane heartbeat lost on page 203	Data plane IP address updated on page 203
Data plane updated to a new control plane on page 203	Data plane status update failed on page 204	Data plane statistics update failed on page 204
Data plane connected on page 204	Data plane disconnected on page 205	Data plane physical interface down on page 205
Data plane physical interface up on page 205	Data plane packet pool is under low water mark on page 206	Data plane packet pool is under critical low water mark on page 206
Data plane packet pool is above high water mark on page 206	Data plane core dead on page 207	Data plane process restarted on page 207
Data plane discovery succeeded on page 207	Data plane managed on page 208	Data plane deleted on page 208
Data plane license is not enough on page 208	Data plane upgrade started on page 209	Data plane upgrading on page 209
Data plane upgrade succeeded on page 209	Data plane upgrade failed on page 209	Data plane of data center side successfully connects to the CALEA server on page 210
Data plane of data center side fails to connect to the CALEA server on page 210	Data plane successfully connects to the other data plane on page 211	Data plane fails to connect to the other data plane on page 211
Data plane disconnects to the other data plane on page 211	Start CALEA mirroring client in data plane on page 212	Data plane DHCP IP pool usage rate is 100 percent on page 212
Data plane DHCP IP pool usage rate is 80 percent on page 213	Data plane NAT session capacity usage rate is 80 percent on page 213	Data plane NAT session capacity usage rate is 100 percent on page 214
Data plane DHCP IP capacity usage rate is 80 percent on page 214	Data plane DHCP IP capacity usage rate is 100 percent on page 214	dpIpmiThempBB on page 215
dpIpmiThempP on page 215	dpIpmiFan on page 216	dpIpmiREThempBB on page 216
dpIpmiREThempP on page 217	dpIpmiREFan on page 217	Data plane backup success on page 217
Data plane backup failed on page 218	Data plane restore success on page 218	Data plane restore failed on page 218
Remote Administration Start on page 219	Remote Administration Stop on page 219	

Data plane discovered

TABLE 457 Data plane discovered event

Event	Data plane discovered
Event Type	dpDiscoverySuccess (server side detect)
Event Code	501
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] sent a connection request to {produce.short.name} [{cpName||wsgIP}].
Description	This event occurs when the data plane successfully connects to the controller.

Data plane discovery failed

TABLE 458 Data plane discovery failed event

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

Data plane configuration updated

TABLE 459 Data plane configuration updated event

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

Data plane configuration update failed

TABLE 460 Data plane configuration update failed event

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

Data plane rebooted

NOTE
This event is not applicable for SZ.

TABLE 461 Data plane rebooted event

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

Data plane heartbeat lost

TABLE 462 Data plane heartbeat lost event

Event	Data plane heartbeat lost
Event Type	dpLostConnection (detected on the server side)
Event Code	507
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”,
Displayed on the web interface	Data plane [{dpName&&dpKey}] heartbeat lost.
Description	This event occurs when the data plane heartbeat lost.

Data plane IP address updated

TABLE 463 Data plane IP address updated event

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

Data plane updated to a new control plane

TABLE 464 Data plane updated to a new control plane event

Event	Data plane updated to a new control plane
Event Type	dpChangeControlBlade

TABLE 464 Data plane updated to a new control plane event (continued)

Event	Data plane updated to a new control plane
Event Code	509
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “oldwsgIP”=”xxx.xxx.xxx.xxx”, “newwsgIP”=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] switched from {produce.short.name} [{oldCpName||oldwsgIP}] to [{cpName||newwsgIP}].
Description	This event occurs when the data plane connects to a new controller instance.

Data plane status update failed

TABLE 465 Data plane status update failed event

Event	Data plane status update failed
Event Type	dpUpdateStatusFailed
Event Code	510
Severity	Minor
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to update its status to {produce.short.name} [{cpName||wsgIP}].
Description	This event occurs when the data plane fails to update its status on the controller.

Data plane statistics update failed

TABLE 466 Data plane statistics update failed event

Event	Data plane statistics update failed
Event Type	dpUpdateStatisticFailed
Event Code	511
Severity	Minor
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] failed to update its statistics to {produce.short.name} [{cpName||wsgIP}].
Description	This event occurs when the data plane fails to update statistics to the controller.

Data plane connected

TABLE 467 Data plane connected event

Event	Data plane connected
Event Type	dpConnected
Event Code	512
Severity	Informational
Attribute	“dpKey”=”xx:xx:xx:xx:xx:xx”, “wsgIP"=”xxx.xxx.xxx.xxx”

TABLE 467 Data plane connected event (continued)

Event	Data plane connected
Displayed on the web interface	Data plane [{dpName&&dpKey}] connected to {produce.short.name} [{cpName||wsgIP}].
Description	This event occurs when the data plane connects to the controller.

Data plane disconnected

TABLE 468 Data plane disconnected event

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

Data plane physical interface down

TABLE 469 Data plane physical interface down event

Event	Data plane physical interface down
Event Type	dpPhyInterfaceDown
Event Code	514
Severity	Critical
Attribute	“portID”=”xx”, “dpKey”=”xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Network link of port [{portID}] on data plane [{dpName&&dpKey}] is down.
Description	This event occurs when the network link of the data plane is down.
Auto Clearance	This event triggers the alarm 504, which is auto cleared by the event code 515.

Data plane physical interface up

TABLE 470 Data plane physical interface up event

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

TABLE 470 Data plane physical interface up event (continued)

Event	Data plane physical interface up
Description	This event occurs when the network link of the data plane is UP.

Data plane packet pool is under low water mark

TABLE 471 Data plane packet pool is under low water mark event

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

Data plane packet pool is under critical low water mark

TABLE 472 Data plane's packet pool is under critical low water mark event

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

Data plane packet pool is above high water mark

TABLE 473 Data plane packet pool is above high water mark event

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

Data plane core dead

TABLE 474 Data plane core dead event

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

Data plane process restarted

TABLE 475 Data plane process restarted event

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

NOTE
Event 530 is not applicable for SZ.

Data plane discovery succeeded

TABLE 476 Data plane discovery succeeded event

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

NOTE
Event 532 is not applicable for SZ.

Data plane managed

TABLE 477 Data plane managed event

Event	Data plane managed
Event Type	dpStatusManaged
Event Code	532
Severity	Informational
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, “wsgIP”=“xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] approved by {produce.short.name} [{wsgIP}].
Description	This event occurs when data plane is approved by the {produce.short.name}.

NOTE
Events 537 to 553 are not applicable for SZ.

Data plane deleted

TABLE 478 Data plane deleted event

Event	Data plane deleted
Event Type	dpDeleted
Event Code	537
Severity	Informational
Attribute	“dpKey”=“xxx.xxx.xxx.xxx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] deleted.
Description	This event occurs when data plane is deleted.

Data plane license is not enough

TABLE 479 Data plane license is not enough event

Event	Data plane license is not enough
Event Type	dpLicenseInsufficient
Event Code	538
Severity	Major
Attribute	"count"=<delete-vdp-count>
Displayed on the web interface	Data plane license is not enough, [{count}] instance of data plane will be deleted.
Description	This event occurs when data plane licenses are insufficient.

Data plane upgrade started

TABLE 480 Data plane upgrade started event

Event	Data plane upgrade started
Event Type	dpUpgradeStart
Event Code	550
Severity	Informational
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}]started the upgrade process.
Description	This event occurs when data plane starts the upgrade process.

Data plane upgrading

TABLE 481 Data plane upgrading event

Event	Data plane upgrading
Event Type	dpUpgrading
Event Code	551
Severity	Informational
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] is upgrading.
Description	This event occurs when data plane starts to upgrade programs and configuration.

Data plane upgrade succeeded

TABLE 482 Data plane upgrade succeeded event

Event	Data plane upgrade succeeded
Event Type	dpUpgradeSuccess
Event Code	552
Severity	Informational
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data plane [{dpName&&dpKey}] has been upgraded successfully..
Description	This event occurs when data plane upgrade is successful.

Data plane upgrade failed

TABLE 483 Data plane upgrade failed event

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

TABLE 483 Data plane upgrade failed event (continued)

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

NOTE
Refer to Data Plane Alarms on page 60.

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

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 484 Data plane of data center side successfully connects to the CALEA server event

Event	Data plane of data center side successfully connects to the CALEA server
Event Type	dpDcToCaleaConnected
Event Code	1257
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "caleaServerIP"="xxx.xxx.xxx.xxx", "dpIP"="xx.xx.xx.xx", "reason"="xxxxxx"
Displayed on the web interface	Data Plane of Data Center side [{dpName&&dpKey}] successfully connects to the CALEA server[{caleaServerIP}].
Description	This event occurs when the data plane successfully connects to the CALEA server.

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

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 485 Data plane of data center side fails to connect to the CALEA server event

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

Data plane successfully connects to the other data plane

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 486 Data plane successfully connects to the other data plane event

Event	Data plane successfully connects to the other data plane
Event Type	dpP2PTunnelConnected
Event Code	1260
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane [{dpName&&dpKey}] successfully connects to the other Data Plane[{targetDpKey&&targetDpIp}]
Description	This event occurs when the data plane connects to another data plane.

Data plane fails to connect to the other data plane

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 487 Data plane fails to connect to the other data plane event

Event	Data plane fails to connect to the other data plane
Event Type	dpP2PTunnelConnectFail
Event Code	1261
Severity	Warning
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx", "targetDpIp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] fails connects to the other Data Plane[{targetDpKey&&targetDpIp}]
Description	This event occurs when the data plane fails to connect to another data plane.
Auto Clearance	This event triggers the alarm 1261, which is auto cleared by the event code 1260.

Data plane disconnects to the other data plane

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 488 Data plane disconnects to the other data plane event

Event	Data plane disconnects to the other data plane
Event Type	dpP2PTunnelDisconnected
Event Code	1262
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx","targetDpIp"="xxx.xxx.xxx.xxx"

TABLE 488 Data plane disconnects to the other data plane event (continued)

Event	Data plane disconnects to the other data plane
Displayed on the web interface	Data Plane[{dpName&&dpKey}] disconnects to the other Data Plane[{targetDpKey&&targetDpIp}]
Description	This event occurs when the data plane disconnects from another data plane.

Start CALEA mirroring client in data plane

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 489 Start CALEA mirroring client in data plane event

Event	Start CALEA mirroring client in data plane
Event Type	dpStartMirroringClient
Event Code	1263
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx"
Displayed on the web interface	Start CALEA mirroring client [{userName||IP||clientMac}] on WLAN [{ssid}] from AP [{apName&&apMac}]
Description	This event occurs when the CALEA server starts mirroring the client image.

Stop CALEA mirroring client in data plane

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 490 Stop CALEA mirroring client in data plane event

Event	Stop CALEA mirroring client in data plane
Event Type	dpStopMirroringClient
Event Code	1264
Severity	Warning
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx"
Displayed on the web interface	Stop CALEA mirroring client [{userName||IP||clientMac}] on WLAN [{ssid||authType}] from AP [{apName&&apMac}]. TxBytes[{txBytes}]
Description	This event occurs when the CALEA server stops mirroring the client image.

Data plane DHCP IP pool usage rate is 100 percent

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 491 Data plane DHCP IP pool usage rate is 100 percent event

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

Data plane DHCP IP pool usage rate is 80 percent

NOTE
This section is not applicable for SZ300/SZ100.

TABLE 492 Data plane DHCP IP pool usage rate is 80 percent event

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

Data plane NAT session capacity usage rate is 80 percent

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 493 Data plane NAT session capacity usage rate is 80 percent event

Event	Data plane NAT session capacity usage rate is 80 percent
Event Type	dpNatSessionCapacityUsageRate80
Event Code	1283
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] NAT Session Capacity usage rate is 80 percent. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane NAT session capacity usage rate is 80%.

Data plane NAT session capacity usage rate is 100 percent

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 494 Data plane NAT session capacity usage rate is 100 percent event

Event	Data plane NAT session capacity usage rate is 100 percent
Event Type	dpNatSessionCapacityUsageRate100
Event Code	1284
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] NAT Session Capacity usage rate is 100 percent. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

Data plane DHCP IP capacity usage rate is 80 percent

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 495 Data plane DHCP IP capacity usage rate is 80 percent event

Event	Data plane DHCP IP capacity usage rate is 80 percent
Event Type	dpDhcpIpCapacityUsageRate80
Event Code	1285
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] DHCP IP Capacity usage rate is 80 percent. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane DHCP IP capacity usage rate is 80%.

Data plane DHCP IP capacity usage rate is 100 percent

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 496 Data plane DHCP IP capacity usage rate is 100 percent event

Event	Data plane DHCP IP capacity usage rate is 100 percent
Event Type	dpDhcpIpCapacityUsageRate100
Event Code	1286
Severity	Major

TABLE 496 Data plane DHCP IP capacity usage rate is 100 percent event (continued)

Event	Data plane DHCP IP capacity usage rate is 100 percent
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] DHCP IP Capacity usage rate is 100 percent. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

NOTE
Refer to Data Plane Alarms on page 60.

dpIpmiThempBB

NOTE
Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

TABLE 497 dpIpmiThempBB event

Event	dpIpmiThempBB
Event Type	dpIpmiThempBB
Event Code	2902
Severity	Major
Attribute	"dpKey"="xxxxxxx”,“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Baseboard temperature [{status}] on data plane [{dpName&&dpKey}]
Description	This event occurs when the baseboard temperature status on the data plane is sent. Baseboard threshold temperatures are in the range of 100 Celsius to 610 Celsius. The default threshold is 610C.

dpIpmiThempP

NOTE
Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

TABLE 498 dpIpmiThempP event

Event	dpIpmiThempP
Event Type	dpIpmiThempP
Event Code	2907
Severity	Major
Attribute	"dpKey"="xxxxxxx”,“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Processor [{id}] temperature [{status}] on data plane [{dpName&&dpKey}].

TABLE 498 dpIpmiThempP event (continued)

Event	dpIpmiThempP
Description	This event occurs when the processor temperature status on the data plane is sent. The threshold value is in the range of 10 to 110 Celsius. The default threshold is 110C.

dpIpmiFan

NOTE
Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

TABLE 499 dpIpmiFan event

Event	dpIpmiFan
Event Type	dpIpmiFan
Event Code	2909
Severity	Major
Attribute	"dpKey"="xxxxxxx",“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	System fan [{id}] module [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the system fan module status on the data plane is sent.

dpIpmiREThempBB

NOTE
Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

TABLE 500 dpIpmiREThempBB event

Event	dpIpmiREThempBB
Event Type	dpIpmiREThempBB
Event Code	2927
Severity	Informational
Attribute	"dpKey"="xxxxxxx",“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Baseboard temperature [{status}] on data plane [{dpName&&dpKey}].
Description	This event occurs when the baseboard temperature comes back to the normal status.

dpIpmiREThempP

NOTE
Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

TABLE 501 dpIpmiREThempP event

Event	dpIpmiREThempP
Event Type	dpIpmiREThempP
Event Code	2932
Severity	Informational
Attribute	"dpKey"="xxxxxxx",“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Processor [{id}] temperature [{status}] on data plane [{dpName&&dpKey}]].
Description	This event occurs when the processor temperature comes back to the normal status.

dpIpmiREFan

NOTE
Events 2902, 2907, 2909, 2927, 2932 and 2934 are applicable for SZ100 D. vSZ has this set of events since vSZ manages SZ100-D.

TABLE 502 dpIpmiREFan event

Event	dpIpmiREFan
Event Type	dpIpmiREFan
Event Code	2934
Severity	Informational
Attribute	"dpKey"="xxxxxxx",“id”=“x”, “status”=“xxxxx”, “nodeMac”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	System fan [{id}] module [{status}] on data plane [{dpName&&dpKey}]].
Description	This event occurs when system fan module comes back to the normal status.

NOTE

Refer to Data Plane Alarms on page 60

Data plane backup success

TABLE 503 Data plane backup success event

Event	Data plane backup success
Event Type	dpBackupSuccess
Event Code	1290
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”

TABLE 503 Data plane backup success event (continued)

Event	Data plane backup success
Displayed on the web interface	Data Plane [{dpName&&dpKey}] backup successful.
Description	This event occurs when Data plane backup is successful.

Data plane backup failed

TABLE 504 Data plane backup failed event

Event	Data plane backup failed
Event Type	dpBackupFailed
Event Code	1291
Severity	Critical
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane [{dpName&&dpKey}] backup failed.
Description	This event occurs when Data plane backup fails.

Data plane restore success

TABLE 505 Data plane restore success event

Event	Data plane restore success
Event Type	dpRestoreSuccess
Event Code	1292
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane [{dpName&&dpKey}] restore successful.
Description	This event occurs when Data plane restore is successful.

Data plane restore failed

TABLE 506 Data plane restore failed event

Event	Data plane restore failed
Event Type	dpRestoreFailed
Event Code	1293
Severity	Critical
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”
Displayed on the web interface	Data Plane [{dpName&&dpKey}] restore failed.
Description	This event occurs when Data plane restore fails.

Remote Administration Start

TABLE 507 Remote administration event

Event	Remote administration
Event Type	dpremoteadministration
Event Code	99250
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	No web interface for this event.
Description	This event occurs when data plane SSHD starts.

Remote Administration Stop

TABLE 508 Remote administration event

Event	Remote administration event
Event Type	remoteadministration
Event Code	99251
Severity	Major
Attribute	No attributes for this event.
Displayed on the web interface	No web interface for this event.
Description	This event occurs when data plane SSHD stops.

IPMI Events

NOTE
This section is not applicable for vSZ-E.

Following are the events related to IPMIs.

ipmiThempBB

TABLE 509 ipmiThempBB event

Event	ipmiThempBB
Event Type	ipmiThempBB
Event Code	902
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	Baseboard temperature [{status}] on controlplane [{nodeMac}]
Description	This event occurs when the baseboard temperature status is sent. Baseboard threshold temperatures are in the range of 10^0 Celsius to 61^0 Celsius. The default threshold is 61^0C.
Auto Clearance	This event triggers the alarm 902, which is auto cleared by the event code 927.

ipmiThempP

TABLE 510 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 in the range of 1^0 to 11^0 Celsius. The default threshold is 11^0C.
Auto Clearance	This event triggers the alarm 907, which is auto cleared by the event code 932.

ipmiFan

TABLE 511 ipmiFan event

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

ipmiFanStatus

TABLE 512 ipmiFanStatus event

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

ipmiRETHempBB

TABLE 513 ipmiRETHempBB event

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

ipmiRETHempP

TABLE 514 ipmiRETHempP event

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

ipmiREFan

TABLE 515 ipmiREFan event

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

ipmiREFanStatus

TABLE 516 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.

NOTE
Refer to IPMI Alarms on page 64.

Licensing Interface Events

Following are the events related to licensing.

- Data plane NAT session capacity license has been removed on page 227
- Insufficient license capacity on page 227

License sync succeeded

TABLE 517 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 518 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 519 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 520 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 521 License data changed event

Event	License data changed
Event Type	licenseChanged
Event Code	1254
Severity	Informational
Attribute	"nodeName"="xxxxxxxx"
Displayed on the web interface	Node [{nodeName}] license data has been changed.
Description	This event occurs when the controller license data is modified.

License going to expire

TABLE 522 License going to expire event

Event	License going to expire
Event Type	licenseGoingToExpire
Event Code	1255
Severity	Major
Attribute	“nodeName”=“xxx”, “licenseType”=“ xxx”
Displayed on the web interface	The [{licenseType}] on node [{nodeName}] will expire on [{associationTime}].
Description	This event occurs when the validity of the license is going to expire.

Insufficient license capacity

TABLE 523 Insufficient license capacity event

Event	Insufficient license capacity
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1256
Severity	Major

TABLE 523 Insufficient license capacity event (continued)

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

Data plane DHCP IP license insufficient

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 524 Data plane DHCP IP license insufficient event

Event	Data plane DHCP IP license insufficient
Event Type	dpDhcpIpLicenseNotEnough
Event Code	1277
Severity	Major
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This event occurs when Data Plane DHCP IP license insufficient. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane DHCP IP address license is insufficient.

Data plane NAT session license insufficient

NOTE
This event is not applicable for SZ300/SZ100.

TABLE 525 Data plane NAT session license insufficient event

Event	Data plane NAT session license insufficient
Event Type	dpNatSessionLicenseNotEnough
Event Code	1278
Severity	Major
Attribute	"totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	This event occurs when Data Plane NAT session license insufficient. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane NAT session license is insufficient.

AP number limit exceeded

TABLE 526 AP number limit exceeded event

Event	AP number limit exceeded
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1280
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing AP connections to terminate.
Description	This event occurs when an approved AP is rejected due to number of APs having exceeded the limit.

Insufficient license capacity

TABLE 527 Insufficient license capacity event

Event	Insufficient license capacity
Event Type	urlFilteringLicenseInsufficient
Event Code	1281
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{licenseType}] licenses have been detected, which will cause the URL Filtering feature to be disabled.
Description	This event occurs when the number of the APs exceeds the number of URL filtering licenses purchased.

Data plane DHCP IP capacity license has been removed

NOTE
This section is not applicable for SZ300/SZ100.

TABLE 528 Data plane DHCP IP capacity license has been removed event

Event	Data plane DHCP IP capacity license has been removed
Event Type	dpDhcpIpLicenseRemoved
Event Code	1287
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] DHCP IP Capacity has been removed one unit. Current assignment (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane DHCP IP capacity license is removed.

Data plane NAT session capacity license has been removed

NOTE
This section is not applicable for SZ300/SZ100.

TABLE 529 Data plane NAT session capacity license has been removed event

Event	Data plane NAT session capacity license has been removed
Event Type	dpNatSessionLicenseRemoved
Event Code	1288
Severity	Major
Attribute	“dpKey”=“xx:xx:xx:xx:xx:xx”, "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] NAT Session Capacity has been removed one unit. Current assignment (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when data plane NAT session capacity license is removed.

NOTE
Refer to Licensing Interface Alarms on page 66.

Insufficient license capacity

TABLE 530 Insufficient license capacity event

Event	Insufficient license capacity
Event Type	switchConnectionTerminatedDueToInsufficientLicense
Event Code	1289
Severity	Major
Attribute	"licenseType”=“ xxx”
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing switch connections to terminate.
Description	This event occurs when some connected switches were rejected due to insufficient license capacity.

SCI Events

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

Connect to SCI

TABLE 531 Connect to SCI event

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

Disconnect to SCI

TABLE 532 Disconnect to SCI event

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

Connect to SCI failure

TABLE 533 Connect to SCI failure event

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

SCI has been disabled

TABLE 534 SCI has been disabled event

Event	SCI has been disabled
Event Type	disabledSciDueToUpgrade
Event Code	4004

TABLE 534 SCI has been disabled event (continued)

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

SCI and FTP have been disabled

TABLE 535 SCI and FTP have been disabled event

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

NOTE
Refer to SCI Alarms on page 68.

Session Events

Following event is related to user equipment TTG session.

- Delete all sessions on page 229

Delete all sessions

TABLE 536 Delete all sessions event

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

System Events

Following are the events related to system log severity.

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

No LS responses

TABLE 537 No LS responses event

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

LS authentication failure

TABLE 538 LS authentication failure event

Event	LS authentication failure
Event Type	scgLBSAuthFailed
Event Code	722

TABLE 538 LS authentication failure event (continued)

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

{produce.short.name} connected to LS

TABLE 539 {produce.short.name} connected to LS event

Event	{produce.short.name} connected to LS
Event Type	scgLBSConnectSuccess
Event Code	723
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “url”=“”, “port”=“”, “SZMgmtIp”=“”
Displayed on the web interface	{produce.short.name}[{SZMgmtIp}] connected to LS: url=[{url}], port=[{port}]
Description	This event occurs when the controller successfully connects to the location based service.

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

TABLE 540 {produce.short.name} failed to connect to LS event

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

{produce.short.name} received passive request

TABLE 541 {produce.short.name} received passive request event

Event	{produce.short.name} received passive request
Event Type	scgLBSStartLocationService
Event Code	725
Severity	Informational

TABLE 541 {produce.short.name} received passive request event (continued)

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

{produce.short.name} sent controller information report

TABLE 542 {produce.short.name} sent controller information report event

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

{produce.short.name} received management request

TABLE 543 {produce.short.name} received management request event

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

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

TABLE 544 {produce.short.name} sent AP info by venue report event

Event	{produce.short.name} sent AP info by venue report
Event Type	scgLBSSendAPInfobyVenueReport
Event Code	729
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “venue”=“”,”count”=“”, “SZMgmtIp”=“”
Displayed on the web interface	{produce.short.name}[{SZMgmtIp}] sent AP Info by Venue Report: venue=[{venue}], count =[{count}]

TABLE 544 {produce.short.name} sent AP info by venue report event (continued)

Event	{produce.short.name} sent AP info by venue report
Description	This event occurs when the controller sends the venue report regarding AP information.

{produce.short.name} sent query venues report

TABLE 545 {produce.short.name} sent query venues report event

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

{produce.short.name} sent associated client report

TABLE 546 {produce.short.name} sent associated client report event

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

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

TABLE 547 {produce.short.name} forwarded calibration request to AP event

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

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

TABLE 548 {produce.short.name} forwarded footfall request to AP event

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

{produce.short.name} received unrecognized request

TABLE 549 {produce.short.name} received unrecognized request event

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

Syslog server reachable

TABLE 550 Syslog server reachable event

Event	Syslog server reachable
Event Type	syslogServerReachable
Event Code	750
Severity	Informational
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, “ syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is reachable on {produce.short.name}.
Description	This event occurs when the syslog server can be reached.

Syslog server unreachable

TABLE 551 Syslog server unreachable event

Event	Syslog server unreachable
Event Type	syslogServerUnreachable
Event Code	751
Severity	Major
Attribute	“nodeMac”=“xx:xx:xx:xx:xx:xx”, "syslogServerAddress"="xxx.xxx.xxxx.xxx"
Displayed on the web interface	Syslog server [{syslogServerAddress}] is unreachable on {produce.short.name}.
Description	This event occurs when the syslog server is unreachable.
Auto Clearance	This event triggers the alarm 751, which is auto cleared by the event code 750.

Syslog server switched

TABLE 552 Syslog server switched event

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

System service failure

TABLE 553 System service failure event

Event	System service failure
Event Type	systemservicefailure
Event Code	753
Severity	Critical
Attribute	No attribute for this event.
Displayed on the web interface	msg - Service [sysService] on node [hostName] failed and respawning
Description	This event occurs when the service is not available.

Generate AP config for plane load rebalance succeeded

TABLE 554 Generate AP config for plane load rebalance succeeded event

Event	Generate AP config for plane load rebalance succeeded
Event Type	planeLoadingRebalancingSucceeded

TABLE 554 Generate AP config for plane load rebalance succeeded event (continued)

Event	Generate AP config for plane load rebalance succeeded
Event Code	770
Severity	Informational
Attribute	
Displayed on the web interface	Generate new AP configs for plane's loading re-balancing succeeded.
Description	This event occurs when the user executes the load of data plane for re-balancing and generates a new AP configuration successfully.

Generate AP config for plane load rebalance failed

TABLE 555 Generate AP config for plane load rebalance failed event

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

FTP transfer

TABLE 556 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 557 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 557 FTP transfer error event (continued)

Event	FTP transfer error
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 558 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 559 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 560 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 561 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 562 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 563 Process restart event

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

Service unavailable

TABLE 564 Service unavailable event

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

Keepalive failure

TABLE 565 Keepalive failure event

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

Resource unavailable

TABLE 566 Resource unavailable event

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

All data planes in the zone affinity profile are disconnected

NOTE
Events 1257 to 1267 are not applicable to SZ300/SZ100.

TABLE 567 All data planes in the zone affinity profile are disconnected event

Event	All data planes in the zone affinity profile are disconnected
Event Type	zoneAffinityLastDpDisconnected
Event Code	1267
Severity	Major
Attribute	"dpName="xxxxxxxx", "dpKey"="xx:xx:xx:xx:xx:xx", "zoneAffinityProfileId"="xxxxxxxx"
Displayed on the web interface	The Last one Data Plane [{dpName&&dpKey}] is disconnected Zone Affinity profile [{zoneAffinityProfileId}].
Description	This event occurs when all the data planes disconnect from the zone affinity profile.

CALEA UE Matched

TABLE 568 CALEA UE Matched event

Event	CALEA UE Matched
Event Type	dpCaleaUeInterimMatched
Event Code	1268
Severity	Informational
Attribute	"clientMac"="xx:xx:xx:xx:xx:xx", "ssid"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "apIpAddress"="xx.xx.xx.xx", "dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "txBytes"="xxxxx", "rxBytes"="xxxxx"
Displayed on the web interface	CALEA matches client [{clientMac}] on WLAN [{ssid||authType}]from AP [{apName&&apMac}]. TxBytes[{txBytes}], RxBytes[{rxBytes}].
Description	This event occurs when the data plane CALEA user equipment and client matches.

ZD AP migrating

TABLE 569 ZD AP migrating event

Event	ZD AP migrating
Event Type	zdAPMigrating
Event Code	2001
Severity	Informational
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033","model"="R700", “firmware”=“3.2.0.0.x”
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is upgrading with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP is upgrading with {produce.short.name} AP firmware image.

ZD AP migrated

TABLE 570 ZD AP migrated event

Event	ZD AP migrated
Event Type	zdAPMigrated
Event Code	2002
Severity	Informational
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="R700", “firmware”=“3.2.0.0.x”,
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] has been upgraded with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP has upgraded its firmware with the {produce.short.name} AP firmware image.

ZD AP rejected

TABLE 571 ZD AP rejected event

Event	ZD AP rejected
Event Type	zdAPRejected
Event Code	2003
Severity	Warning
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033", "model"="R700"
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is not being upgraded with {produce.short.name} AP firmware because of ACL setting.
Description	This event occurs when the ZoneDirector AP is not upgraded with {produce.short.name} AP firmware because of the ACL setting.

ZD AP migration failed

TABLE 572 ZD AP migration failed event

Event	ZD AP migration failed
Event Type	zdAPMigrationFailed
Event Code	2004
Severity	Major
Attribute	"apMac"=" C0:C5:20:12:2B:2C ", "serialNumber"="501003003033","model"="R700", “firmware”=“3.2.0.0.x”
Displayed on the web interface	ZD-AP [{apMac}] / [{serialNumber}] model [{model}] is failed to upgrade with {produce.short.name} AP firmware version - [{firmware}]
Description	This event occurs when a ZoneDirector AP fails to upgrade with [produce.short.name} AP firmware image.

Database error

TABLE 573 Database error event

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

Database error

TABLE 574 Database error event

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

SZ Login Fail

TABLE 575 SZ login fail event

Event	SZ login fail
Event Type	szLoginFail
Event Code	8007
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on failed from [{ip}].
Description	Administrator logged on failed SZ.

SZ Login

TABLE 576 SZ login event

Event	SZ login
Event Type	szLogin
Event Code	8008
Severity	Informational

TABLE 576 SZ login event (continued)

Event	SZ login
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on from [{ip}].
Description	Administrator logged on SZ.

SZ Logout

TABLE 577 SZ logout event

Event	SZ logout
Event Type	szLogout
Event Code	8009
Severity	Informational
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged off from [{ip}].
Description	Administrator logged off SZ.

Password expiration

TABLE 578 Password expiration event

Event	Password expiration
Event Type	passwordExpiration
Event Code	8010
Severity	Informational
Attribute	userId = "x", time = "mm:dd:yyyy hh:mm:ss"
Displayed on the web interface	Administrative account [{userId}] password has expired as of [{time}].
Description	This event occurs when the password expires.

Admin account lockout

TABLE 579 Admin account lockout event

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

Admin session expired

TABLE 580 Admin session expired event

Event	Admin session expired
Event Type	AdminSessionExpired
Event Code	8012
Severity	Informational
Attribute	userName = "x"
Displayed on the web interface	Administrative account [{userName}] login session has timed out.
Description	This event occurs when the session is timed out due to inactivity or because of absolute session timeout.

Disable inactive admins

TABLE 581 Disable inactive admins event

Event	Disable inactive admins
Event Type	DisableInactiveAdmins
Event Code	8013
Severity	Informational
Attribute	userName = "x", inactiveDays="x"
Displayed on the web interface	Administrative account [{userName}] has been disabled due to not logining for [{inactiveDays}] days.
Description	This event occurs when the account is disabled for a period of time.

Two factor auth failed

TABLE 582 Two factor auth failed event

Event	Two factor auth failed
Event Type	TwoFactorAuthFailed
Event Code	8014
Severity	Warning
Attribute	userName = "x"
Displayed on the web interface	Administrative account [{userName}] failed to response the SMS one time password code.
Description	This event occurs when the account fails to send a one time password code as a SMS text.

NOTE
Refer to System Events.

Unconfirmed program detection

TABLE 583 Unconfirmed program detection event

Event	Unconfirmed program detection
Event Type	Unconfirmed Program Detection
Event Code	1019
Severity	Warning
Attribute	"nodeName"="xxx","status"="xxxxx"
Displayed on the web interface	Detect unconfirmed program on control plane [{nodeName}]. [{status}]
Description	This event occurs when an unconfirmed program is detected.

Switch Events

Following are the events related to swtich severity:

Switch critical message

TABLE 584 Switch critical message event

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

Switch alert message

TABLE 585 Switch alert message event

Event	Switch alert message
Event Type	SwitchAlertMessage
Event Code	20001
Severity	Major
Description	This event occurs when there is a switch alert message.

Switch warning message

TABLE 586 Switch warning message event

Event	Switch warning message
Event Type	SwitchWarningMessage
Event Code	20003
Severity	Warning
Description	This event occurs when there is a switch warning message.

Switch CPU warning threshold exceed

TABLE 587 Switch CPU warning threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	warningCpuThresholdExceed
Event Code	22010
Severity	Warning
Attribute	“switchSerialNumber”=“x”, cpuUsage=”x%” (1% - Major Threshold),switchName = “x”, switchMac = “xx:xx:xx:xx:xx:xx”
Displayed on the web interface	[CPU Usage – {switchSerialNumber}] CPU warning threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the warning threshold.

Switch CPU major threshold exceed

TABLE 588 Switch CPU major threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	majorCpuThresholdExceed
Event Code	22011
Severity	Major
Attribute	“switchSerialNumber”=“x”, cpuUsage=”x%” (Warning Threshold – Critical Threshold),switchName = “x”, switchMac = “xx:xx:xx:xx:xx:xx”
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU major threshold {cpuUsage} exceeded on Switch {switchName&switchMac}

TABLE 588 Switch CPU major threshold exceed event (continued)

Event	Switch CPU warning threshold exceed
Description	This event occurs when CPU usage of the Switch crosses the major threshold.

Switch CPU critical threshold exceed

TABLE 589 Switch CPU critical threshold exceed event

Event	Switch CPU critical threshold exceed
Event Type	criticalCpuThresholdExceed
Event Code	22012
Severity	Critical
Attribute	“switchSerialNumber”=“x”, cpuUsage=”x%” (Major Threshold - 100%),switchName = “x”, switchMac = “xx:xx:xx:xx:xx:xx”
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU critical threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the critical threshold.

Switch memory warning threshold exceed

TABLE 590 Switch memory warning threshold exceed event

Event	Switch memory warning threshold exceed
Event Type	warningMemoryThresholdExceed
Event Code	22020
Severity	Warning
Attribute	“switchSerialNumber”=“x”, memoryUsage=”x%” (1% - Major Threshold), switchName = “x”, switchMac = “xx:xx:xx:xx:xx:xx”
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory warning threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the warning threshold.

Switch memory major threshold exceed

TABLE 591 Switch memory major threshold exceed event

Event	Switch memory major threshold exceed
Event Type	majorMemoryThresholdExceed
Event Code	22021
Severity	Major
Attribute	“switchSerialNumber”=“x”, memoryUsage=”x%” (Warning Threshold – Critical Threshold),switchName = “x”, switchMac = “xx:xx:xx:xx:xx:xx”
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}

TABLE 591 Switch memory major threshold exceed event (continued)

Event	Switch memory major threshold exceed
Description	This event occurs when memory usage of the Switch crosses the major threshold.

Switch memory critical threshold exceed

TABLE 592 Switch memory critical threshold exceed event

Event	Switch memory critical threshold exceed
Event Type	criticalMemoryThresholdExceed
Event Code	22022
Severity	Critical
Attribute	**“switchSerialNumber”=“x”, memoryUsage=”x%” (Major Threshold – 100%),switchName = “x”, switchMac = “xx:xx:xx:xx:xx:xx”**
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory critical threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the critical threshold of 100%.

Switch custom warning threshold exceed

TABLE 593 Switch custom warning threshold exceed event

Event	Switch custom warning threshold exceed
Event Type	hitWarningSwitchCombinedEvent
Event Code	22030
Severity	Warning
Attribute	UserDefinedDescription = ”x”
Displayed on the web interface	[Custom Warning Event] {userDefinedDescription}
Description	This event occurs when the Switch custom warning event crosses the threshold.

Switch custom major threshold exceed

TABLE 594 Switch custom major threshold exceed event

Event	Switch custom major threshold exceed
Event Type	hitMajorSwitchCombinedEvent
Event Code	22031
Severity	Major
Attribute	UserDefinedDescription = ”x”
Displayed on the web interface	[Custom Major Event] {userDefinedDescription}
Description	This event occurs when the Switch custom major event crosses the threshold.

Switch custom critical threshold exceed

TABLE 595 Switch custom critical threshold exceed event

Event	Switch custom critical threshold exceed
Event Type	hitCriticalSwitchCombinedEvent
Event Code	22032
Severity	Critical
Attribute	UserDefinedDescription = ”x”
Displayed on the web interface	[Custom Critical Event] {userDefinedDescription}
Description	This event occurs when the Switch custom critical event crosses the threshold.

GetCACert Request

TABLE 596 GetCACert Request event

Event	GetCACert Request
Event Type	getCACertRequest
Event Code	22000
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] GetCACert Request.
Description	This event occurs when there is a SCEP GetCACert Request.

Certificate signing request

TABLE 597 Certificate signing request event

Event	Certificate signing request
Event Type	certificateSigningRequest
Event Code	22001
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Certificate Signing Request.
Description	This event occurs when there is a SCEP Certificate Signing Request.

Accept certificate signing request

TABLE 598 Accept certificate signing request event

Event	Accept certificate signing request
Event Type	acceptCertificateSigningRequest
Event Code	22002
Severity	Informational

TABLE 598 Accept certificate signing request event (continued)

Event	Accept certificate signing request
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Accept Certificate Signing Request.
Description	This event occurs when there is a SCEP Accept Certificate Signing Request.

Reject certificate signing request

TABLE 599 Reject certificate signing request event

Event	Reject certificate signing request
Event Type	rejectCertificateSigningRequest
Event Code	22003
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Reject Certificate Signing Request.
Description	This event occurs when there is a SCEP Reject Certificate Signing Request.

Pending certificate signing request

TABLE 600 Pending certificate signing request event

Event	Pending certificate signing request
Event Type	pendingCertificateSigningRequest
Event Code	22004
Severity	Major
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Pending Certificate Signing Request.
Description	This event occurs when there is a SCEP Pending Certificate Signing Request.

Threshold Events

Following are the events related to threshold limits.

CPU threshold exceeded

TABLE 601 CPU threshold exceeded event

Event	CPU threshold exceeded
Event Type	cpuThresholdExceeded
Event Code	950
Severity	Critical
Attribute	“nodeName”=”xxx”, “nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	CPU threshold [{perc}%] exceeded on control plane [{nodeName}-C]
Description	This event occurs when the CPU usage exceeds the threshold limit of 80%.
Auto Clearance	This event triggers the alarm 950, which is auto cleared by the event code 953.

Memory threshold exceeded

TABLE 602 Memory threshold exceeded event

Event	Memory threshold exceeded
Event Type	memoryThresholdExceeded
Event Code	951
Severity	Critical
Attribute	“nodeName”=”xxx”,“nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Memory threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This event occurs when the memory usage exceeds the threshold limit of 85%.
Auto Clearance	This event triggers the alarm 951, which is auto cleared by the event code 954.

Disk usage threshold exceeded

TABLE 603 Disk usage threshold exceeded event

Event	Disk usage threshold exceeded
Event Type	diskUsageThresholdExceeded
Event Code	952

TABLE 603 Disk usage threshold exceeded event (continued)

Event	Disk usage threshold exceeded
Severity	Critical
Attribute	“nodeName”=”xxx”,“nodeMac”=”xx:xx:xx:xx:xx:xx”, “perc”=”XX”
Displayed on the web interface	Disk usage threshold [{perc}%] exceeded on control plane [{nodeName}-C].
Description	This event occurs when the disk usage exceeds the threshold limit of 80%.
Auto Clearance	This event triggers the alarm 952, which is auto cleared by the event code 955.

CPU threshold back to normal

TABLE 604 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 605 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 606 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 606 Disk threshold back to normal event (continued)

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

The drop of client count threshold exceeded

TABLE 607 The drop of client count threshold exceeded event

Event	The drop of client count threshold exceeded
Event Type	clientCountDropThresholdExceeded
Event Code	956
Severity	Warning
Attribute	“perc”=“XX”
Displayed on the web interface	The drop of client count exceeded threshold [{perc}%] in cluster.
Description	This event occurs when client count exceeds the criterion value of 1500 and the drop percentage exceeds the threshold limit of 60%.

License threshold exceeded

TABLE 608 License threshold exceeded event

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

HDD health degradation

NOTE
This event is not applicable for vSZ-H and vSZ-E.

TABLE 609 HDD health degradation event

Event	HDD health degradation
Event Type	HDDHealthDegradation
Event Code	961
Severity	Critical
Attribute	"nodeName"="xxx","status"="xxxxx"
Displayed on the web interface	Hard drive detects health degradation [{status}] on control plane [{nodeName}], please backup the system to prevent losing the data on disk
Description	This event occurs when the hard drive detects health degradation.

Rate limit threshold surpassed

TABLE 610 Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” "SZMgmtIp"="2.2.2.2" “aaaSrvIp”=”1.1.1.1” “AAAServerType”=”Auth/Acct” “MOR”=1000 “THRESHOLD”=”500” “TOR”=”501”
Displayed on the web interface	Threshold surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]
Description	This event occurs when the rate limit threshold is surpassed. The threshold limit for this event is dependent of the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds the limit of 701.

Rate limit threshold restored

TABLE 611 Rate limit threshold restored event

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

Rate limit for TOR surpassed

TABLE 612 Rate limit for TOR surpassed event

Event	Rate limit for TOR surpassed
Event Type	rateLimitTORSurpassed
Event Code	1302
Severity	Critical
Attribute	“ctrlBladeMac”=”aa:bb:cc:dd:ee:ff” “srcProcess”=”radiusd” "SZMgmtIp"="2.2.2.2" “aaaSrvrIp”=”1.1.1.1” “AAAServerType”=”Auth/Acct” “MOR”=1000 “THRESHOLD”=”500” “TOR”=”501”

TABLE 612 Rate limit for TOR surpassed event (continued)

Event	Rate limit for TOR surpassed
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{aaaSrvrIp}] and ServerType [{AAAServerType}]. Dropping requests to be proxied to AAA.
Description	This event occurs when the rate limit for total outstanding requests (TOR) is surpassed. Threshold limits for this event is dependent of the maximum outstanding request (MOR) value as configured in the web interface of Authentication or Accounting Service. For example, if the MOR value is 1000, and threshold limit is set to 70%, then this event will be raised when total outstanding requests for this server exceeds 1000.
Auto Clearance	This event triggers the alarm1302, which is auto cleared by the event code 1301.

The number of users exceed its limit

TABLE 613 The number of users exceed its limit

Event	The number of users exceed its limit
Event Type	tooManyUsers
Event Code	7001
Severity	Major
Attribute	This event has no attributes.
Displayed on the web interface	The number of users exceed its limits. The threshold limit for SZ100 is 114000 and 38000 for vSZ-E.
Description	This event occurs when the number of users exceeds the specified limit.

The number of devices exceeded its limit

TABLE 614 The number of devices exceeded its limit event

Event	The number of devices exceeded its limit
Event Type	tooManyDevices
Event Code	7002
Severity	Major
Attribute	This event has not attributes.
Displayed on the web interface	The number of devices exceeded its limit
Description	This event occurs when the number of devices exceeds the specified limit. The threshold limit for SZ100 is 342000 and 152000 for vSZ-E.

NOTE

Refer to Threshold Alarms on page 82.

Over AP maximum capacity

TABLE 615 Over AP maximum capacity event

Event	Over AP maximum capacity
Event Type	apCapacityReached
Event Code	962
Severity	Warning
Attribute	
Displayed on the web interface	The volume of AP is over system capacity.
Description	This event occurs when the volume of AP is over system capacity.

Tunnel Events - Access Point (AP)

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

Data plane accepted a tunnel request

NOTE
This event is not applicable for vSZ-E.

TABLE 616 Data plane accepted a tunnel request event

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

TABLE 616 Data plane accepted a tunnel request event (continued)

Event	Data plane accepted a tunnel request
Description	This event occurs when the data plane accepts a tunnel request from the AP.

Data plane rejected a tunnel request

NOTE
This event is not applicable for vSZ-E.

TABLE 617 Data plane rejected a tunnel request event

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

Data plane terminated a tunnel

NOTE
This event is not applicable for vSZ-E.

TABLE 618 Data plane terminated a tunnel event

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

AP created a tunnel

NOTE
This event is not applicable for vSZ-E.

TABLE 619 AP created a tunnel event

Event	AP created a tunnel
Event Type	apBuildTunnelSuccess
Event Code	608
Severity	Informational

TABLE 619 AP created a tunnel event (continued)

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

AP tunnel disconnected

NOTE
This event is not applicable for vSZ-E.

TABLE 620 AP tunnel disconnected event

Event	AP tunnel disconnected
Event Type	apTunnelDisconnected
Event Code	610
Severity	Informational
Attribute	“apMac”=”xx:xx:xx:xx:xx:xx”, “dpIP”=”xxx.xxx.xxx.xxx”, “reason”=”xxxxx”
Displayed on the web interface	AP [{apName&&apMac}] disconnected from data plane [{dpIP}]. Reason: [{reason}]
Description	This event occurs when AP disconnects from the data plane.

AP SoftGRE tunnel fails over primary to secondary

TABLE 621 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 622 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"

TABLE 622 AP SoftGRE tunnel fails over secondary to primary event (continued)

Event	AP SoftGRE tunnel fails over secondary to primary
Displayed on the web interface	AP [{apName&&apMac}] fails over from secondaryGRE[{secondaryGRE}] to primaryGRE[{primaryGRE}].
Description	This event occurs when AP moves from a secondary to a primary GRE.

AP SoftGRE gateway reachable

TABLE 623 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 624 AP SoftGRE gateway not reachable event

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

Data plane set up a tunnel

NOTE
This event is not applicable for vSZ-E.

TABLE 625 Data plane set up a tunnel event

Event	Data plane set up a tunnel
Event Type	dpSetUpTunnel
Event Code	627
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "apMac"="xx:xx:xx:xx:xx:xx"

TABLE 625 Data plane set up a tunnel event (continued)

Event	Data plane set up a tunnel
Displayed on the web interface	Data plane [{dpName&&dpKey}] set up a tunnel from AP [{apName&&apMac}].
Description	This event occurs when the data plane sets up a tunnel from the AP.

AP secure gateway association success

TABLE 626 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 627 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 628 AP secure gateway association failure event

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

NOTE
Refer to Tunnel Alarms - Access Point on page 87.

Tunnel Events - Data Plane

NOTE
Events 615, 616, 617, 620, 622, 624 and 625 are not applicable for SZ.

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

DP sGRE GW unreachable

TABLE 629 DP sGRE GW unreachable event

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

DP sGRE keep alive timeout

TABLE 630 DP sGRE keep alive timeout event

Event	DP sGRE keep alive timeout
Event Type	dpSgreKeepAliveTimeout
Event Code	616
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected KeepAlive packet to Core Gateway [{GatewayIP}] is lost due to timeout

TABLE 630 DP sGRE keep alive timeout event (continued)

Event	DP sGRE keep alive timeout
Description	This event occurs when the data plane detects that a keep alive packet to the core network gateway is lost due to a timeout.

DP sGRE GW inactive

TABLE 631 DP sGRE GW inactive event

Event	DP softGRE GW inactive
Event Type	dpSgreGWInact
Event Code	617
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected [{GatewayIP}] is inactive because there is no RX traffic
Description	This event occurs when the data plane detects that a core network gateway is inactive.

DP DHCPRelay no response

TABLE 632 DP DHCPRelay no response event

Event	DP DHCPRelay no response
Event Type	dpDhcpRelayNoResp
Event Code	618
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dhcpIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected no response from DHCP server [{dhcpIP}] for a while
Description	This event occurs when the data plane does not get a a response from the DHCP server.

DP DHCPRelay failover

TABLE 633 DP DHCPRelay failover event

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

DP sGRE new tunnel

TABLE 634 DP sGRE new tunnel event

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

DP sGRE keepalive recovery

TABLE 635 DP sGRE keepalive recovery event

Event	DP sGRE keepalive recovery
Event Type	dpSgreKeepAliveRecovery
Event Code	622
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected KeepAlive packet to Core Gateway [{gatewayIP}] is now responsive.
Description	The event occurs when the core gateway resumes answering to keepalive.

DP DHCPRelay response recovery

TABLE 636 DP DHCPRelay response recovery event

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

DP sGRE GW reachable

TABLE 637 DP sGRE GW reachable event

Event	DP sGRE GW reachable
Event Type	dpSgreGWReachable
Event Code	624

TABLE 637 DP sGRE GW reachable event (continued)

Event	DP sGRE GW reachable
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected Core Gateway [{gatewayIP}] is now reachable
Description	This event occurs when the core gateway is reachable.

DP sGRE GW active

TABLE 638 DP sGRE GW active event

Event	DP sGRE GW active
Event Type	dpSgreGWAct
Event Code	625
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected [{gatewayIP}] is now active
Description	This event occurs when core gateway changes to an active mode.

NOTE
Refer to Tunnel Alarms - Access Point on page 87.

Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com