RUCKUS™
an ARRIS company

Ruckus SmartZone 100 and Virtual SmartZone-Essentials Alarm and Event Reference Guide

Supporting SmartZone 5.1

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are 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@arris.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.

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
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

TABLE 2 Terms used (continued)

Term	Description
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

Revision History

SmartZone Version 5.1

New SZ100 Alarms in Release 5.1

TABLE 3 Alarms added in release 5.1

Alarm Code	Alarm
962	apCapacityReached
1019	Unconfirmed Program Detection
1289	switchConnectionTerminatedDueToInsufficientLicense
9109	simRemoval
20000	PowerSupplyfailure
20001	FanFailure
20002	ModuleInsertion
20003	ModuleRemoval
20004	TemperatureAboveThresholdWarning
20005	StackMemberUnitFailure
20006	PoePowerAllocationFailure
20007	DhcpOfferDroppedMessage
20008	PortPutIntoErrorDisableState
21000	SwitchOffline
21001	OverSwitchMaxCapacity
21002	SwitchDuplicated
22003	rejectCertificateSigningRequest
22004	pendingCertificateSigningRequest
22011	Switch CPU Major Threshold Exceed
22012	Switch CPU Critical Threshold Exceed
22021	Switch Memory Major Threshold Exceed

TABLE 3 Alarms added in release 5.1 (continued)

Alarm Code	Alarm
22022	Switch Memory Critical Threshold Exceed
22031	Switch Custom Major Event
22032	Switch Custom Critical Event

New SZ100 Events in Release 5.1

Event Code	Event
189	jammingDetected
232	packetSpoofingDetectedFromWireless
233	packetSpoofingDetectedFromWirelessSourceMacSpoofed
234	packetSpoofingDetectedFromWired
235	packetSpoofingDetectedFromWiredSourceMacSpoofed
962	apCapacityReached
1019	Unconfirmed Program Detection
1289	switchConnectionTerminatedDueToInsufficientLicense
1290	dpBackupSuccess
1291	dpBackupFailed
1292	dpRestoreSuccess
1293	dpRestoreFailed
22000	getCACertRequest
22001	certificateSigningRequest
22002	acceptCertificateSigningRequest
22003	rejectCertificateSigningRequest
22004	pendingCertificateSigningRequest
22010	warningCpuThreshouldExceed
22011	majorCpuThreshouldExceed
22012	criticalCpuThreshouldExceed
22020	warningCpuThreshouldExceed
22021	majorMemoryThreshouldExceed
22022	criticalMemoryThreshouldExceed
22030	hitWarningSwitchCombinedEvent
22031	hitMajorSwitchCombinedEvent
22032	hitCriticalSwitchCombinedEvent
9100	changeToPrimaryBackhaul
9101	changeToSecondaryBackhaul
9102	lteConnectivityFailed
9103	ethernetConnectivityFailed
9104	lteDhcpTimeout
9105	ethernetLinkDown
9106	ethernetLinkUp
9107	simSwitch

Event Code	Event
9108	remoteHostBlacklisted
9109	simRemoval
9110	lteNetworkRegistrationStatus
9111	lteConnectionStatus

SmartZone Version 5.0

New Alarms in Release 5.0

TABLE 4 Alarms added in release 5.0

Alarm Code	Alarm
868	upgradeSSTableFailed
961	HDDHealthDegradation
1026	apCfgDhcpNatDwpdEthPortConfigOverride
1027	sZCfgDhcpNatManualEthPortConfigOverride
1277	dpDhcpIpLicenseNotEnough
1278	dpNatSessionLicenseNotEnough

TABLE 5 Deprecated alarm in release 5.0

Alarm Code	Alarm
1016	hipFailover

New Events in Release 5.0

Event Code	Event
961	HDDHealthDegradation
1277	dpDhcpIpLicenseNotEnough
1278	dpNatSessionLicenseNotEnough
1283	dpNatSessionCapacityUsageRate80
1284	dpNatSessionCapacityUsageRate100
1285	dpDhcpIpCapacityUsageRate80
1286	dpDhcpIpCapacityUsageRate100
1287	dpDhcpIpLicenseRemoved
1288	dpNatSessionLicenseRemoved
8012	AdminSessionExpired
8013	DisableInactiveAdmins
8014	TwoFactorAuthFailed
20000	SwitchCriticalMessage
20001	SwitchAlertMessage
20002	SwitchWarningMessage

SmartZone 3.6.1

New Alarms in Release 3.6.1

Alarm Code	Alarm
956	clientCountDropThresholdExceeded

New Events in Release 3.6.1

Event Code	Event
956	clientCountDropThresholdExceeded
1280	apConnectionTerminatedDueToInsufficientLicense
1281	urlFilteringLicenseInsufficient
2902	dpIpmiThempBB
2909	dpIpmiFan
2927	dpIpmiREThempBB
2932	dpIpmiREThempP
2934	dpIpmiREFan
8010	passwordExpiration
8011	adminAccountLockout

SmartZone Version 3.6

New Events in Release 3.6

Event Code	Event
186	generalRogueAPDetected
187	apSigningInformation
349	apClusterFailover
350	apRehomeFailover
872	allServiceOutOfService
873	allServiceInService
874	clusterRedundancySyncCfgFailed
8001	application of user is identified
8002	application of user is denied
8003	urlFilteringServerUnreachable
8004	urlFilteringServerReachable

SmartZone Version 3.5.1

The following are the changes for version 3.5.1.

New Event

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

SmartZone Version 3.5

The following are the changes for version 3.5.

Deprecated Alarm and Event

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

New Alarm

Description for Alarm 346 is changed.

Alarm Code	Alarm
341	apDHCPServiceFailure
346	apNATFailureDetectedbySZ
855	unsyncNTPTime
858	clusterUploadKspFileFailed
974	csvFtpTransferMaxRetryReached
975	csvDiskThreshholdExceeded
976	csvDiskMaxCapacityReached
1024	apCfgNonDhcpNatWlanVlanConfigMismatch
1025	apCfgDhcpNatWlanVlanConfigMismatch
1258	dpDcToCaleaConnectFail
1261	dpP2PTunnelConnectFail
1265	dpDhcpIpPoolUsageRate100
1267	zoneAffinityLastDpDisconnected
1762	racADLDAPTLSFailed

Alarm Code	Alarm
4003	disabledSciDueToUpgrade
4004	disabledSciDueToUpgrade
4005	disabledSciAndFtpDueToMutuallyExclusive

New Event

Event Code	Event
117	apGetConfigFailed
228	clientBlockByBarringUERule
229	clientUnblockByBarringUERule
328	apHealthLatencyFlag
329	apHealthCapacityFlag
330	apHealthConnectionFailureFlag
331	apHealthClientCountFlag
332	apHealthLatencyClear
333	apHealthCapacityClear
334	apHealthConnectionFailureClear
335	apHealthClientCountClear
336	apDHCPFailoverDetected
337	apDHCPFallbackDetected
338	apSecondaryDHCPAPDown
339	apSecondaryDHCPAPUp
340	apDHCPIPPoolMaxThresholdReached
341	apDHCPServiceFailure
342	apNATFailoverDetected
343	apNATFallbackDetected
344	apNATVlanCapacityAffected
345	apNATVlanCapacityRestored
346	apNATFailureDetectedbySZ
347	apHealthAirUtilizationFlag
348	apHealthAirUtilizationClear
855	unsyncNTPTime
869	ReindexElasticSearchfinished
870	clusterInitContactApr
972	csvFtpTransfer
973	csvFtpTransferError
974	csvFtpTransferMaxRetryReached
975	csvDiskThreshholdExceeded
976	csvDiskMaxCapacityReached
977	csvDiskThreshholdBackToNormal
1024	apCfgNonDhcpNatWlanVlanConfigMismatch
1025	apCfgDhcpNatWlanVlanConfigMismatch

Event Code	Event
1257	dp DcToCaleaConnected
1258	dpDcToCaleaConnectFail
1259	dpDcToCaleaDisconnected
1268	dpCaleaUeInterimMatched
1260	dpP2PTunnelConnected
1261	dpP2PTunnelConnectFail
1262	dpP2PTunnelDisconnected
1263	dpStartMirroringClient
1264	dpStopMirroringClient
1265	dpDhcpIpPoolUsageRate100
1266	dpDhcpIpPoolUsageRate80
1267	zoneAffinityLastDpDisconnected
1761	racADLDAPTLSSuccess
1762	racADLDAPTLSFailed
4001	connectedToSci
4002	disconnectedFromSci
4003	disabledSciDueToUpgrade
4004	disabledSciDueToUpgrade
4005	disabledSciAndFtpDueToMutuallyExclusive

SmartZone Version 3.4.1

No changes to this version.

SmartZone Version 3.4

The following are the changes for version 3.4.

New Alarm

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

Displayed on the Web Interface

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

New Event

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

SmartZone Version 3.2.1

The following are the changes for version 3.2.1.

New Alarm

Alarm Code	Alarm
865	apCertificateExpire

New Event

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

Event on Web Interface

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

SmartZone Version 3.2

The following are the changes for version 3.2.

New Alarm

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

Attribute Change

Module	Attribute	Attribute Change
DataPlane	dpMac	dpKey

Renamed Alarm

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

New Event

Event Code	Event
370	apUsbSoftwarePackageDownloaded
371	apUsbSoftwarePackageDownloadFailed
516	dpPktPoolLow
517	dpPktPoolCriticalLow
518	dpPktPoolRecover
519	dpCoreDead
530	dpDiscoverySuccess
532	dpStatusManaged
537	dpDeleted
538	dpLicenseInsufficient
550	dpUpgradeStart
551	dpUpgrading
552	dpUpgradeSuccess
553	dpUpgradeFailed
615	dpSgreGWUnreachable
616	dpSgreKeepAliveTimeout
617	dpSgreGWInact
620	dpSgreNewTunnel
622	dpSgreKeepAliveRecovery
624	dpSgreGWReachable
625	dpSgreGWAct
750	syslogServerReachable
751	syslogServerUnreachable
752	syslogServerSwitched
770	planeLoadingRebalancingSucceeded
771	planeLoadingRebalancingFailed
845	clusterUploadVDPFirmwareStart
846	uploadClusterVDPFirmwareSuccess
847	uploadClusterVDPFirmwareFailed
1255	licenseGoingToExpire
1256	apConnectionTerminatedDueToInsufficientLicense

Event Code	Event
1751	racADLDAPSuccess
1752	racADLDAPFail
1753	racADLDAPBindFail
1754	racLDAPFailToFindPassword
1755	racADNPSFail
1756	racADNPSFailToAuthenticate
2151	espAuthServerReachable
2152	espAuthServerUnreachable
2153	espAuthServerResolvable
2154	espAuthServerUnResolvable
2161	espDNATServerReachable
2162	espDNATServerUnreachable
2163	espDNATServerResolvable
2164	espDNATServerUnresolvable

Severity Change

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

Attribute Change

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

Renamed Event

Event Code	Event Name	Renamed To
320	AP CLB limit reached	AP client load balancing limit reached
321	AP CLB limit recovered	AP client load balancing limit recovered
619	DP DHCPRelay failOver	DP DHCPRelay failover

Event Code	Event Name	Renamed To
1202	DP Disconnected	GtpManager (DP) disconnected

Auto Clearance of Event

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

SmartZone Version 3.1.1

The following are the changes for version 3.1.1.

New Alarm

Alarm Code	Alarm
661	ipsecTunnelDisassociated
662	ipsecTunnelAssociateFailed

New Event

Event Code	Event
326	cmResetByUser
327	cmResetFactoryByUser
660	ipsecTunnelAssociated
661	ipsecTunnelDisAssociated
662	ipsecTunnelAssociateFailed
844	clusterInitiatedMovingAp
2101	radiusServerReachable
2102	radiusServerUnreachable
2121	ldapServerReachable
2122	ldapServerUnreachable
2141	adServerReachable
2142	adServerUnreachable
2201	zoneInitiatedMovingAp
2501	nodeIPv6Added
2502	nodeIPv6Deleted

Re-added Event

Event Code	Event
101	apDiscoverySuccess

Renamed Event

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

Deprecated Event

Event Code	Event Name
1604	authSuccess
1605	authFailed

RuckOS Version 3.1

The following are the changes for version 3.1.

New Alarm

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

Deprecated Alarm

Alarm Code	Alarm
1008	cfgUpdFailed
1909	apAcctRespWhileInvalidConfig

Renamed Alarm Type

Alarm Code	Alarm Type	Renamed To
843	clusterOutofService	clusterOutOfService

Renamed Alarm

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

New Event

Event Code	Event
223	remediationSuccess
224	remediationFailure
325	cableModemUp
520	dpProcessRestart
627	dpSetUpTunnel
860	clusterCfgBackupStart
861	clusterCfgBackupSuccess
862	clusterCfgBackupFailed
863	clusterCfgRestoreSuccess
864	clusterCfgRestoreSuccess
902	ipmiThempBB
927	ipmiREThempBB
932	ipmiREThempP
934	ipmiREFan
937	ipmiREFanStatus
953	cpuThresholdBackToNormal
954	memoryThresholdBackToNormal
955	diskUsageThresholdBackToNormal
1651	authFailedOverToSecondary
1652	authFallbackToPrimary
7001	tooManyUsers
7002	tooManyDevices

Renamed Event

Event Code	Event Name	Renamed To
181	Ssid-spoofing rogue AP	SSID-spoofing rogue AP

Event Code	Event Name	Renamed To
209	Client Roaming	Client roaming
220	Client Grace Period	Client grace period
308	AP channel updated because Dynamic Frequency Selection (DFS) detected a radar event	AP channel updated because dynamic frequency selection (DFS) detected a radar event
317	AP Brownout	AP brownout
323	AP capacity Reached	AP capacity reached
405	eMAP downlink connected to MAP	EMAP downlink connected to MAP
406	eMAP downlink disconnected from MAP	EMAP downlink disconnected from MAP
407	eMAP uplink connected to MAP	EMAP uplink connected to MAP
408	eMAP uplink disconnected from MAP	EMAP uplink disconnected from MAP
422	Mesh state updated to MAP No Channel	Mesh state updated to MAP no channel
424	Mesh state update to RAP No Channel	Mesh state update to RAP no channel
515	Data plane physical Interface Up	Data plane physical interface up
615	DP SoftgreGW Unreachable	DP softGRE GW unreachable
618	DP DhcpRelay No Resp	DP DHCPRelay no response
619	DP DhcpRelay FailOver	DP DHCPRelay failOver
623	DP DhcpRelay Resp Recovery	DP DHCPRelay response recovery
701	No LS Responses	No LS responses
707	AP received Passive Calibration Request	AP received passive calibration request
708	AP received Passive Footfall Request	AP received passive footfall request
709	AP received Unrecognized Request	AP received unrecognized request
721	No LS Responses	No LS responses
725	SCG received Passive Request	SCG received passive request
727	SCG sent Controller Information report	SCG sent controller information report
728	SCG received Management Request	SCG received management request
729	SCG sent AP Info by Venue Report	SCG sent AP info by venue report
730	SCG sent Query Venues Report	SCG sent query venues report
731	SCG sent Associated Client Report	SCG sent associated client report
732	SCG forwarded Calibration Request to AP	SCG forwarded calibration request to AP
733	SCG forwarded Footfall Request to AP	SCG forwarded footfall request to AP
734	SCG received Unrecognized Request	SCG received unrecognized request
833	SSH Tunnel Switched	SSH tunnel switched

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

Alarm and Event Management

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 21 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 39
- Event Attributes on page 40
- Generation of Alarm and Event on page 40

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 43 and Events Types on page 103 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 6 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 6 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 103.

AP Authentication Alarms

Following are the alarms related to AP authentication.

- RADIUS server unreachable on page 44
- LDAP server unreachable on page 45
- AD server unreachable on page 45
- WeChat ESP authentication server unreachable on page 45
- WeChat ESP authentication server unresolvable on page 46
- WeChat ESP DNAT server unreachable on page 46
- WeChat ESP DNAT server unresolvable on page 47

RADIUS server unreachable

TABLE 7 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 8 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 9 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 10 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 10 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 11 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 12 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 12 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 13 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 142.

AP Communication Alarms

Following are the alarms related to access point communications.

- AP rejected on page 47
- AP configuration update failed on page 48
- AP swap model mismatched on page 48
- AP pre-provision model mismatched on page 49
- AP firmware update failed on page 49
- AP WLAN oversubscribed on page 50

AP rejected

TABLE 14 AP rejected alarm

Alarm	AP rejected
Alarm Type	apStatusRejected

TABLE 14 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 15 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 16 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 16 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 17 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 18 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 19 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 50
- LS authentication failure on page 51
- AP failed to connect to LS on page 51

No LS responses

TABLE 20 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 21 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 22 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 113.

AP State Change Alarms

Following are the alarms related to access point state changes.

- AP cable modem interface down on page 53
- AP DHCP service failure on page 53
- AP NAT failure on page 54
- AP DHCP/NAT DWPD Ethernet port configuration override on page 54
- SZ DHCP/NAT DWPD Ethernet port configuration override on page 55
- SIM removal on page 55

AP rebooted by system

TABLE 23 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 24 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 25 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 26 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 122.

AP DHCP service failure

TABLE 27 AP DHCP service failure alarm

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

TABLE 27 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 28 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 29 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 30 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 51.

SIM removal

TABLE 31 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.

- RADIUS fails to authenticate with AD NPS server on page 59
- Fails to establish TLS tunnel with AD/LDAP on page 60

Authentication server not reachable

TABLE 32 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 33 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 34 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 35 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 36 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 37 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 38 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 39 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 148.

Fails to establish TLS tunnel with AD/LDAP

TABLE 40 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 148.

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 60

GtpManager (DP) disconnected

TABLE 41 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 41 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 157 event 1201.

NOTE
Refer to Control and Data Plane Interface Events on page 157.

Cluster Alarms

Following are alarms related to cluster:

- New node failed to join on page 62
- Node removal failed on page 62
- Node out of service on page 63
- Cluster in maintenance state on page 63
- Cluster backup failed on page 63
- Cluster restore failed on page 64
- Cluster upgrade failed on page 64
- Cluster application stopped on page 65
- Node bond interface down on page 65
- Node physical interface down on page 66
- Cluster node rebooted on page 66
- Cluster node shut down on page 67
- Disk usage exceed threshold on page 67
- Cluster out of service on page 68
- Cluster upload AP firmware failed on page 68
- Cluster add AP firmware failed on page 68
- Unsync NTP time on page 69
- Cluster upload KSP file failed on page 69
- Configuration backup failed on page 69
- Configuration restore failed on page 70
- AP certificate updated on page 70
- Upgrade SS table failed on page 71
- Over switch max capacity on page 71

New node failed to join

TABLE 42 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 43 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 44 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 45 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 46 Cluster backup failed alarm

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

TABLE 46 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 47 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 48 Cluster upgrade failed alarm

Alarm	Cluster upgrade failed
Alarm Type	upgradeClusterFailed
Alarm Code	807

TABLE 48 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 49 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 50 Node bond interface down alarm

Alarm	Node bond interface down
Alarm Type	nodeBondInterfaceDown

TABLE 50 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 51 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 52 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 52 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 53 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 54 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 55 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 56 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 57 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 57 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 58 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 59 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 60 Configuration backup failed alarm

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

TABLE 60 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 61 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 62 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 173.

Upgrade SS table failed

TABLE 63 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.

> **NOTE**
> Refer to Cluster Alarms on page 61.

Over switch max capacity

TABLE 64 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 72
- AP configuration generation failed on page 72
- End-of-life AP model detected on page 72
- VLAN configuration mismatch on non DHCP/NAT WLAN on page 73
- VLAN configuration mismatch on DHCP/NAT WLAN on page 73

Zone configuration preparation failed

TABLE 65 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 66 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 67 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,T 300"

TABLE 67 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

VLAN configuration mismatch on non DHCP/NAT WLAN

TABLE 68 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 69 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 69 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 195.

Data Plane Alarms

Following are the alarms related to data plane.

- Data plane configuration update failed on page 74
- Data plane disconnected on page 75
- Data plane physical interface down on page 75
- Data plane process restarted on page 75
- Data plane license is not enough on page 76
- Data plane upgrade failed on page 76

Data plane configuration update failed

TABLE 70 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 71 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 72 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 73 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 73 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 74 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 75 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 75 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 198.

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

TABLE 76 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 77 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 77 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 78 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 to

IPMI Alarms

NOTE
This section is not applicable for vSZ-E.

Following are the alarms related to IPMIs.

- ipmiThempBB on page 78
- ipmiThempP on page 79
- ipmiFan on page 79
- ipmiFanStatus on page 80

ipmiThempBB

TABLE 79 ipmiThempBB alarm

Alarm	ipmiThempBB
Alarm Type	ipmiThempBB
Alarm Code	902

TABLE 79 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 80 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 81 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 81 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 82 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 216.

Licensing Interface Alarms

The following are the alarms related to licensing:

- License going to expire on page 80
- Insufficient license capacity on page 81
- Data plane DHCP IP license insufficient on page 81
- Data plane NAT session license insufficient on page 82
- Insufficient license capacity on page 82

License going to expire

TABLE 83 License going to expire alarm

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

TABLE 83 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 84 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 219.

Data plane DHCP IP license insufficient

TABLE 85 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 85 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 86 Data pane 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 219.

Insufficient license capacity

TABLE 87 Insufficient license capacity alarm

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

SCI Alarms

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

Connect to SCI failure

TABLE 88 Connect to SCI failure alarm

Alarm	Connect to SCI failure
Alarm Type	connectToSciFailure
Alarm Code	4003
Severity	Major
Aggregation Policy	From the event code xxx 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 xxx.
Displayed on the web interface	Try to connect to SCI with all SCI profiles but failure.
Description	This alarm occurs when the controller tries connecting to SCI with its profiles but fails.
Recommended Actions	

SCI has been disabled

TABLE 89 SCI has been disabled alarm

Alarm	SCI has been disabled
Alarm Type	disabledSciDueToUpgrade
Alarm Code	4004
Severity	Warning
Aggregation Policy	From the event code xxx 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 xxx.
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 90 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 xxx an alarm is raised for every event. A single event triggers a single alarm.

TABLE 90 SCI and FTP have been disabled alarm (continued)

Alarm	SCI and FTP have been disabled
Auto Clearance	The alarm is auto cleared with the event code xxx.
Displayed on the web interface	SCI and FTP have been disabled. It is recommended to enable SCI instead of FTP
Description	This event occurs when the SCI and FTP are disabled.
Recommended Actions	

> **NOTE**
> Refer to SCI Events on page 224.

System Alarms

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

Following are the alarms with the system log severity:

- No LS responses on page 84
- LS authentication failure on page 85
- {produce.short.name} failed to connect to LS on page 85
- Syslog server unreachable on page 85
- CSV export FTP maximum retry on page 86
- CSV export disk threshold exceeded on page 86
- CSV export disk max capacity reached on page 87
- Process restart on page 87
- Service unavailable on page 87
- Keepalive failure on page 88
- Resource unavailable on page 88
- The last one data plane is disconnected zone affinity profile on page 89
- Unconfirmed program detection on page 89

No LS responses

TABLE 91 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}]

TABLE 91 No LS responses alarm (continued)

Alarm	No LS responses
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 92 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 93 {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 94 Syslog server unreachable alarm

Alarm	Syslog server unreachable
Alarm Type	syslogServerUnreachable

TABLE 94 Syslog server unreachable alarm (continued)

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

CSV export FTP maximum retry

TABLE 95 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 96 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 97 CSV export disk max capacity reached alarm

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

Process restart

TABLE 98 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 99 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"

TABLE 99 Service unavailable alarm (continued)

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

Keepalive failure

TABLE 100 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 101 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 102 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 226.

Unconfirmed program detection

TABLE 103 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 on page 90
- Fan failure on page 90
- Module insertion on page 91
- Module removal on page 91
- Temperature above threshold warning on page 91
- Stack member unit failure on page 92

- [PoE power allocation failure](#) on page 92
- [DHCP_Snooping: DHCP offer dropped message](#) on page 92
- [Port put into error disable state](#) on page 93
- [Switch offline](#) on page 93
- [Switch duplicated](#) on page 93
- [Reject certificate signing request](#) on page 94
- [Pending certificate signing request](#) on page 94
- [Switch CPU major threshold exceed](#) on page 94
- [Switch CPU critical threshold exceed](#) on page 95
- [Switch memory major threshold exceed](#) on page 95
- [Switch memory critical threshold exceed](#) on page 95
- [Switch custom major threshold exceed](#) on page 96
- [Switch custom critical threshold exceed](#) on page 96

Power supply failure

TABLE 104 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 105 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 106 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 107 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 108 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 109 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 110 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 111 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 112 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 113 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 114 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 115 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 116 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 117 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 118 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 119 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 120 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 120 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 121 Switch custom major threshold exceed alarm

Alarm	Switch custom major threshold exceed
Alarm Type	hitMajorSwitchCombined
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 122 Switch custom critical threshold exceed alarm

Alarm	Switch custom critical threshold exceed
Alarm Type	hitCriticalSwitchCombined
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:

- CPU threshold exceeded on page 97
- Memory threshold exceeded on page 97
- Disk usage threshold exceeded on page 98
- The drop of client count threshold exceeded on page 98
- License threshold exceeded on page 98
- HDD health degradation on page 99

- Rate limit for TOR surpassed on page 99
- The number of users exceeded its limit on page 100
- The number of devices exceeded its limit on page 100
- Over AP maximum capacity on page 101

CPU threshold exceeded

TABLE 123 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 124 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 124 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 125 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 126 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 127 License threshold exceeded alarm

Alarm	License threshold exceeded
Alarm Type	licenseThresholdExceeded

TABLE 127 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 128 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 129 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 129 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 130 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 131 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 to

Over AP maximum capacity

TABLE 132 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 on page 101
- AP is disconnected from secure gateway on page 101
- AP secure gateway association failure on page 102

AP softGRE gateway not reachable

TABLE 133 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 134 AP is disconnected from secure gateway alarm

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

TABLE 134 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 135 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

Events Types

Accounting Events

Following are the events related to accounting.

- Accounting server not reachable on page 103
- AP accounting response while invalid config on page 104
- AP account message drop while no accounting start message on page 104
- Unauthorized COA/DM message dropped on page 105

Accounting server not reachable

TABLE 136 Accounting server not reachable event

Event	Accounting server not reachable
Event Type	accSrvrNotReachable
Event Code	1602
Severity	Major
Attribute	"mvnoId"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "accSrvrIp"="30.30.30.30" "SZMgmtIp"="2.2.2.2"
Displayed on the web interface	Accounting Server [{accSrvrIp}] not reachable from Radius Proxy [{radProxyIp}] on {produce.short.name} [{SZMgmtIp}].

TABLE 136 Accounting server not reachable event (continued)

Event	Accounting server not reachable
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 137 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 138 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 139 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 43.

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 105	AP managed on page 106	AP rejected on page 106
AP firmware updated on page 106	AP firmware update failed on page 107	Updating AP firmware on page 107
Updating AP configuration on page 107	AP configuration updated on page 108	AP configuration update failed on page 108
AP pre-provision model mismatched on page 108	AP swap model mismatched on page 109	AP WLAN oversubscribed on page 109
AP illegal to change country code on page 109	AP configuration get failed on page 110	Rogue AP on page 110
SSID-spoofing rogue AP on page 110	Mac-spoofing rogue AP on page 110	Same-network rogue AP on page 111
Ad-hoc network device on page 111	Ad-hoc network device on page 111	Rogue AP disappeared on page 111
Classified Rogue AP on page 112	AP image signing failed on page 112	Jamming attack on page 112

AP discovery succeeded

TABLE 140 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"

TABLE 140 AP discovery succeeded event (continued)

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

AP managed

TABLE 141 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 142 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 143 AP firmware updated event

Event	AP firmware updated
Event Type	apFirmwareUpdated
Event Code	106
Severity	Informational
Attribute	"apMac"="xxx.xxx.xxx.xxx" , "configID"="23456781234", "toVersion"="3.2.0.0.539", "fromVersion"="3.2.0.0.x"
Displayed on the web interface	AP [{apName&&apMac}] updated its firmware from [{fromVersion}] to [{toVersion}].

TABLE 143 AP firmware updated event (continued)

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

AP firmware update failed

TABLE 144 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 145 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 146 Updating AP configuration event

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

AP configuration updated

TABLE 147 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 148 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 149 AP pre-provision model mismatched event

Event	AP pre-provision model mismatched
Event Type	apModelDiffWithPreProvConfig
Event Code	112
Severity	Major
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "wsgIP"="xxx.xxx.xxx.xxx", "configModel"="xxx.xxx.xxx.xxx" "model"="R700"
Displayed on the web interface	AP [{apName&&apMac}] model [{model}] is different from per-provision configuration model [configModel]
Description	This event occurs when the AP model differs from the configuration model.

AP swap model mismatched

TABLE 150 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 151 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 152 AP illegal to change country code event

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

AP configuration get failed

TABLE 153 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 154 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"="xxxxxxxxx", "channel"="xx"
Displayed on the web interface	Rogue AP[{rogueMac}] with SSID[{ssid}] is detected by [{apName&&apMac}] on channel[{channel}]
Description	This event occurs when the AP detects a rogue AP.

SSID-spoofing rogue AP

TABLE 155 SSID-spoofing rogue AP event

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

Mac-spoofing rogue AP

TABLE 156 Mac-spoofing rogue AP event

Event	Mac-spoofing rogue AP
Event Type	mac-spoofingRogueAPDetected

TABLE 156 Mac-spoofing rogue AP event (continued)

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

Same-network rogue AP

TABLE 157 Same-network rogue AP event

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

Ad-hoc network device

TABLE 158 Ad-hoc network device event

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

Rogue AP disappeared

TABLE 159 Rogue AP disappeared event

Event	Rogue AP disappeared
Event Type	maliciousRogueAPTimeout
Event Code	185

TABLE 159 Rogue AP disappeared event (continued)

Event	Rogue AP disappeared
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 160 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 161 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

Jamming attack

TABLE 162 Jamming attack event

Event	Jamming attack
Event Type	jammingDetected
Event Code	189

TABLE 162 Jamming attack event (continued)

Event	Jamming attack
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.

AP LBS Events

Following are the events related to AP Location Based Service.

No LS responses

TABLE 163 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 164 LS authentication failure event

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

TABLE 164 LS authentication failure event (continued)

Event	LS authentication failure
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 165 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 166 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 167 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"=""

TABLE 167 AP started location service event (continued)

Event	AP started location service
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 168 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 169 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 170 AP received passive footfall request event

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

AP received unrecognized request

TABLE 171 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 50.

AP Mesh Events

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

EMAP downlink connected to MAP

TABLE 172 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 173 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 174 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 175 EMAP uplink disconnected from MAP event

Event	EMAP uplink disconnected from MAP
Event Type	emapUlinkDisconnectWithMap
Event Code	408
Severity	Informational
Attribute	"emapMac"="xx:xx:xx:xx:xx:xx", "mapMac="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	eMAP [{apName&&apMac}] uplink disconnected from MAP [{mapName&&mapMac}]
Description	This event occurs when the EMAP uplink disconnects from MAP.

MAP disconnected

TABLE 176 MAP disconnected event

Event	MAP disconnected
Event Type	mapDisconnected
Event Code	411
Severity	Informational

TABLE 176 MAP disconnected event (continued)

Event	MAP disconnected
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 177 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 178 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 179 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 180 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 181 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 182 MAP uplink disconnected from EMAP event

Event	MAP uplink disconnected from EMAP
Event Type	mapUlinkDisconnectToeMap
Event Code	418
Severity	Informational
Attribute	"mapMac"="xx:xx:xx:xx:xx:xx", "emapMac"="xx:xx:xx:xx:xx:xx"
Displayed on the web interface	MAP [{apName&&apMac}] disconnected from eMAP [{emapName&&emapMac}]
Description	This event occurs when the MAP disconnects from EMAP.

MAP uplink connected to RAP

TABLE 183 MAP uplink connected to RAP event

Event	MAP uplink connected to RAP
Event Type	mapUlinkConnectToRap

TABLE 183 MAP uplink connected to RAP event (continued)

Event	MAP uplink connected to RAP
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 184 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 185 Mesh state updated to MAP event

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

Mesh state updated to MAP no channel

TABLE 186 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 187 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 188 Mesh state update to RAP no channel event

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

MAP downlink connected to MAP

TABLE 189 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 190 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 191 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 country code updated on page 125	AP channel updated because dynamic frequency selection (DFS) detected a radar on page 125	AP change control plane on page 126
AP connected on page 126	AP deleted on page 126	AP heartbeat lost on page 127
AP tagged as critical on page 127	AP cable modem interface down on page 127	AP brownout on page 128
AP cable modem power-cycled by user on page 128	AP smart monitor turn off WLAN on page 128	AP client load balancing limit reached on page 128
AP client load balancing limit recovered on page 129	AP WLAN state changed on page 129	AP capacity reached on page 129
AP capacity recovered on page 130	AP cable modem interface up on page 130	AP cable modem soft-rebooted by user on page 130
AP cable modem set to factory default by user on page 131	AP health high latency flag on page 131	AP health low capacity flag on page 131
AP health high connection failure flag on page 132	AP health high client count flag on page 132	AP health high latency clear on page 132
AP health low capacity clear on page 133	AP health high connection failure clear on page 133	AP health high client count clear on page 133
Primary DHCP AP is down on page 134	Primary DHCP AP is up on page 134	Secondary DHCP AP is down on page 134
Secondary DHCP AP is up on page 135	Primary or secondary DHCP AP detects 90% of the configured total IPs on page 135	Both primary and secondary DHCP server APs are down on page 135
AP NAT gateway IP failover detected for particular VLAN pool on page 136	AP NAT gateway IP fall back detected for particular VLAN pool on page 136	NAT VLAN capacity affected detected by NAT gateway AP at zone due to three (3) consecutive NAT gateway AP IPs are down for particular VLAN pool on page 136
NAT VLAN capacity restored detected by NAT gateway AP due to (at least) one out of the three (3) consecutive NAT gateway AP IP were down is now up on page 137	AP NAT failure detected by SZ due to three (3) consecutive NAT gateway APs are down on page 137	AP health high airtime utilization flag on page 138
AP health high airtime utilization clear on page 138	AP cluster failover on page 138	AP cluster rehome on page 139
Backhaul switched to primary on page 139	Backhaul switched to secondary on page 139	LTE network connectivity lost on page 140
Ethernet network connectivity lost on page 140	LTE DHCP timeout on page 140	Ethernet link down on page 140
Ethernet link up on page 141	SIM switch on page 141	Remote host blacklisted on page 141
SIM removal on page 142	LTE network registration status on page 142	LTE connection status on page 142

AP rebooted by user

TABLE 192 AP rebooted by user event

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

AP rebooted by system

TABLE 193 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 194 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 195 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 196 AP reset to factory default event

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

TABLE 196 AP reset to factory default event (continued)

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

AP channel updated

TABLE 197 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 198 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 199 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

TABLE 199 AP channel updated because dynamic frequency selection (DFS) detected a radar event (continued)

Event	AP channel updated because dynamic frequency selection (DFS) detected a radar
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 200 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 201 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 202 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"

TABLE 202 AP deleted event (continued)

Event	AP deleted
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 203 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 204 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 205 AP cable modem interface down event

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

AP brownout

TABLE 206 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 207 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 208 AP smart monitor turn off WLAN event

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

AP client load balancing limit reached

TABLE 209 AP client load balancing limit reached event

Event	AP client load balancing limit reached
Event Type	apCLBlimitReached
Event Code	320
Severity	Warning

TABLE 209 AP client load balancing limit reached event (continued)

Event	AP client load balancing limit reached
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 210 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 211 AP WLAN state changed event

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

AP capacity reached

TABLE 212 AP capacity reached event

Event	AP capacity reached
Event Type	apCapacityReached

TABLE 212 AP capacity reached event (continued)

Event	AP capacity reached
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 213 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 214 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 215 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"

TABLE 215 AP cable modem soft-rebooted by user event (continued)

Event	AP cable modem soft-rebooted by user
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 216 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 217 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 218 AP health low capacity flag event

Event	AP health low capacity flag
Event Type	apHealthCapacityFlag
Event Code	329
Severity	Warning
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current 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}].

TABLE 218 AP health low capacity flag event (continued)

Event	AP health low capacity flag
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 219 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 220 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 221 AP health high latency clear event

Event	AP health high latency clear
Event Type	apHealthLatencyClear
Event Code	332
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "current 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}].

TABLE 221 AP health high latency clear event (continued)

Event	AP health high latency clear
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 222 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 223 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 224 AP health high client count clear event

Event	AP health high client count clear
Event Type	apHealthClientCountClear
Event Code	335
Severity	Informational
Attribute	"apName"="xxxxx", "apMac"="xx:xx:xx:xx:xx:xx", "currentValue"="xxxxx", configuredThreshold"="xxxxx",
Displayed on the web interface	AP [{apName&&apMac}] cleared client count health [{currentValue}], which is no longer past the threshold [{configuredThreshold}].

TABLE 224 AP health high client count clear event (continued)

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

Primary DHCP AP is down

TABLE 225 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 226 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 227 Secondary DHCP AP is down event

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

Secondary DHCP AP is up

TABLE 228 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 229 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 230 Both primary and secondary DHCP server APs are down event

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

AP NAT gateway IP failover detected for particular VLAN pool

TABLE 231 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 232 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 233 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}].

TABLE 233 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 (continued)

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
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 234 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 235 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 236 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 237 AP health high airtime utilization clear event

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

AP cluster failover

TABLE 238 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 239 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 51.

Backhaul switched to primary

TABLE 240 Backhaul switched to primary event

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

Backhaul switched to secondary

TABLE 241 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 242 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 243 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 244 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 245 Ethernet link down event

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

TABLE 245 Ethernet link down event (continued)

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

Ethernet link up

TABLE 246 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 247 SIM switch event

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

Remote host blacklisted

TABLE 248 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 249 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 250 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 251 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 252 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 253 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 254 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 255 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 256 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 257 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","zoneNa me"="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 258 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-8484-829192 75ddc3","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 259 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-8484-829192 75ddc3","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 260 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 261 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 262 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 263 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 264 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 265 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.

AP USB Events

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

-
-

AP USB software package downloaded

TABLE 266 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 267 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.

-
-
-
-
-
-
-
-

- RADIUS fails to authenticate with AD NPS server on page 152
- Successfully established the TLS tunnel with AD/LDAP on page 152
- Fails to establish TLS tunnel with AD/LDAP on page 152

Authentication server not reachable

TABLE 268 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 269 Authentication failed over to secondary event

Event	Authentication failed over to secondary
Event Type	authFailedOverToSecondary
Event Code	1651
Severity	Major
Attribute	"mvnoId"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "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 270 Authentication fallback to primary event

Event	Authentication fallback to primary
Event Type	authFallbackToPrimary
Event Code	1652
Severity	Major
Attribute	"mvnoId"=12 "ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "realm"= "wlan.mnc080.mcc405.3gppnetwork.org" "radProxyIp"="7.7.7.7" "primary"="20.20.20.20" "secondary"="30.30.30.30" "SZMgmtIp"="2.2.2.2"

TABLE 270 Authentication fallback to primary event (continued)

Event	Authentication fallback to primary
Displayed on the web interface	Radius Server Fallback to Primary [{primary}] from Secondary [{secondary}] on Radius Proxy [{radProxyIp}] on {produce.short.name} [{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 271 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 272 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 273 Bind fails with AD/LDAP event

Event	Bind fails with AD/LDAP
Event Type	racADLDAPBindFail
Event Code	1753
Severity	Major

TABLE 273 Bind fails with AD/LDAP event (continued)

Event	Bind fails with AD/LDAP
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 274 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 275 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 276 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 55.

Successfully established the TLS tunnel with AD/LDAP

TABLE 277 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 278 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.

TABLE 278 Fails to establish TLS tunnel with AD/LDAP event (continued)

Event	Fails to establish TLS tunnel with AD/LDAP
Auto Clearance	This event triggers the alarm 1762, which is auto cleared by the event code 1761.

NOTE

Refer to

Authorization Events

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

DM received from AAA

TABLE 279 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 280 DM NACK sent to AAA event

Event	DM NACK sent to AAA
Event Type	dmNackSntAAA
Event Code	1642

TABLE 280 DM NACK sent to AAA event (continued)

Event	DM NACK sent to AAA
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 281 DM sent to NAS event

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

DM NACK received from NAS

TABLE 282 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 283 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 284 CoA NACK sent to AAA event

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

CoA sent NAS

TABLE 285 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 286 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 287 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 288 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 on page 157
- GtpManager (DP) disconnected on page 157
- Session updated at DP on page 158
- Session update at DP failed on page 158
- Session deleted at DP on page 158
- Session delete at DP failed on page 159
- C2d configuration failed on page 159

DP connected

TABLE 289 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 290 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 291 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 292 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 293 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"

TABLE 293 Session deleted at DP event (continued)

Event	Session deleted at DP
Displayed on the web interface	TTG/PDG session for UE with IMSI [{ueImsi}] and MSISDN [{ueMsisdn}] has been deleted from Data plane [{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 294 Session delete at DP failed event

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

C2d configuration failed

TABLE 295 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 60.

Client Events

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

- Client authentication failed on page 161

Client authentication failed

TABLE 296 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 297 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 298 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 299 Client disconnected event

Event	Client disconnected
Event Type	clientDisconnect

TABLE 299 Client disconnected event (continued)

Event	Client disconnected
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 300 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 301 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 302 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 303 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 304 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 305 Client logged out event

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

Client roaming disconnected

TABLE 306 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 307 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",

TABLE 307 Client blocked event (continued)

Event	Client blocked
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 308 Client grace period event

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

Onboarding registration succeeded

TABLE 309 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 310 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",

TABLE 310 Onboarding registration failed event (continued)

Event	On boarding registration failed
	"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 311 Remediation succeeded event

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

Remediation failed

TABLE 312 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 313 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"="",

TABLE 313 Force DHCP disconnected event (continued)

Event	Force DHCP disconnected
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 314 WDS device joined event

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

WDS device left

TABLE 315 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 316 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"

TABLE 316 Client is blocked because of barring UE rule event (continued)

Event	Client is blocked because of barring UE rule
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 317 Client is unblocked by barring UE rule event

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

Start CALEA mirroring client

TABLE 318 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 319 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}].

TABLE 319 Stop CALEA mirroring client event (continued)

Event	Stop CALEA mirroring client
Description	This event occurs when CALEA stops mirroring the client image.

Wired client joined

TABLE 320 Wired client joined event

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

Wired client failed to join

TABLE 321 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 322 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"

TABLE 322 Wired client disconnected event (continued)

Event	Wired client disconnected
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 323 Wired client authorization successfully event

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

Wired client session expired

TABLE 324 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 325 Application identified event

Event	Application identified
Event Type	application of user is identified
Event Code	8001
Severity	Informational

TABLE 325 Application identified event (continued)

Event	Application identified
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 326 Application denied event

Event	Application denied
Event Type	application of user is denied
Event Code	8002
Severity	Informational
Attribute	
Displayed on the web interface	APP[{APP}] denied from AP[{apMac}] for client [{STA_MAC}] with source[{SRC_IP}:{SRC_PORT}] destination[{DST_IP}:{DST_PORT}] Proto[{PROTO}]
Description	This event occurs when the application of the user is denied.

URL filtering server unreachable

TABLE 327 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 328 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 329 Packet spoofing detected event

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

Packet spoofing detected

TABLE 330 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 331 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 332 Packet spoofing detected event

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

Cluster Events

Following are the events related to clusters.

Cluster created successfully

TABLE 333 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 334 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 335 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 336 Node removal completed event

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

Node removal failed

TABLE 337 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 338 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 339 Cluster in maintenance state event

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

Cluster back in service

TABLE 340 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 341 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 342 Cluster backup failed event

Event	Cluster backup failed
Event Type	backupClusterFailed
Event Code	810

TABLE 342 Cluster backup failed event (continued)

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

Cluster restore completed

TABLE 343 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 344 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 345 Cluster node upgrade completed event

Event	Cluster node upgrade completed
Event Type	upgradeClusterNodeSuccess
Event Code	813
Severity	Informational

TABLE 345 Cluster node upgrade completed event (continued)

Event	Cluster node upgrade completed
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 346 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 347 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 348 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

TABLE 348 Cluster application stopped event (continued)

Event	Cluster application 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 349 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 350 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 351 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 352 Cluster leader changed event

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

Node bond interface down

TABLE 353 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 354 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 355 Node IP address changed event

Event	Node IP address changed
Event Type	nodeIPChanged
Event Code	823

TABLE 355 Node IP address changed event (continued)

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

Node physical interface down

TABLE 356 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 357 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 358 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",

TABLE 358 Cluster node rebooted event (continued)

Event	Cluster node rebooted
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 359 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 360 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 361 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 362 Cluster upload completed event

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

Cluster upload failed

TABLE 363 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 364 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 365 Cluster remove node started event

Event	Cluster remove node started
Event Type	removeNodeStarted
Event Code	834

TABLE 365 Cluster remove node started event (continued)

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

Node back in service

TABLE 366 Node back in service event

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

Resync NTP time

TABLE 367 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 368 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 369 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 370 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 371 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 372 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 373 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 374 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 375 Cluster upload AP firmware completed event

Event	Cluster upload AP firmware completed
Event Type	clusterUploadAPFirmwareSuccess

TABLE 375 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 376 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 377 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 378 Cluster add AP firmware completed event

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

TABLE 378 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 379 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 380 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 381 Unsync NTP Time event

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

TABLE 381 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 382 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 383 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 384 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 385 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 386 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 387 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 388 Configuration restore succeeded event

Event	Configuration restore succeeded
Event Type	clusterCfgRestoreSuccess
Event Code	863

TABLE 388 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 389 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 390 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 391 AP Certificate Updated event

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

TABLE 391 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 392 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 393 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 394 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 395 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 396 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 397 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 398 Management service ready event

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

TABLE 398 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 399 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 400 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 401 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 61.

Configuration Events

Following are events related to configuration.

Configuration updated

TABLE 402 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 403 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 403 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 404 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 405 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 406 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 406 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 407 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 408 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 409 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 409 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 410 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

Data Plane Events

Following are the events related to data plane.

Data plane discovered on page 199	Data plane discovery failed on page 199	Data plane configuration updated on page 199
Data plane configuration update failed on page 200	Data plane heartbeat lost on page 200	Data plane IP address updated on page 201
Data plane updated to a new control plane on page 201	Data plane status update failed on page 201	Data plane statistics update failed on page 202
Data plane connected on page 202	Data plane disconnected on page 202	Data plane physical interface down on page 203
Data plane physical interface up on page 203	Data plane packet pool is under low water mark on page 203	Data plane packet pool is under critical low water mark on page 204
Data plane packet pool is above high water mark on page 204	Data plane core dead on page 204	Data plane process restarted on page 204
Data plane discovery succeeded on page 205	Data plane managed on page 205	Data plane deleted on page 206

Data plane license is not enough on page 206	Data plane upgrade started on page 206	Data plane upgrading on page 206
Data plane upgrade succeeded on page 207	Data plane upgrade failed on page 207	Data plane of data center side successfully connects to the CALEA server on page 207
Data plane of data center side fails to connect to the CALEA server on page 208	Data plane successfully connects to the other data plane on page 208	Data plane fails to connect to the other data plane on page 209
Data plane disconnects to the other data plane on page 209	Start CALEA mirroring client in data plane on page 209	Data plane DHCP IP pool usage rate is 100 percent on page 210
Data plane DHCP IP pool usage rate is 80 percent on page 210	Data plane NAT session capacity usage rate is 80 percent on page 211	Data plane NAT session capacity usage rate is 100 percent on page 211
Data plane DHCP IP capacity usage rate is 80 percent on page 212	Data plane DHCP IP capacity usage rate is 100 percent on page 212	dpIpmiThempBB on page 212
dpIpmiThempP on page 213	dpIpmiFan on page 213	dpIpmiREThempBB on page 214
dpIpmiREThempP on page 214	dpIpmiREFan on page 214	Data plane backup success on page 215
Data plane backup failed on page 215	Data plane restore success on page 215	Data plane restore failed on page 216

Data plane discovered

TABLE 411 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 412 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 413 Data plane configuration updated event

Event	Data plane configuration updated
Event Type	dpConfUpdated

TABLE 413 Data plane configuration updated event (continued)

Event	Data plane configuration updated
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 414 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 415 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 416 Data plane heartbeat lost event

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

TABLE 416 Data plane heartbeat lost event (continued)

Event	Data plane heartbeat lost
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 417 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 418 Data plane updated to a new control plane event

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

Data plane status update failed

TABLE 419 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}].

TABLE 419 Data plane status update failed event (continued)

Event	Data plane status update failed
Description	This event occurs when the data plane fails to update its status on the controller.

Data plane statistics update failed

TABLE 420 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 421 Data plane connected event

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

Data plane disconnected

TABLE 422 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 423 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 424 Data plane physical interface up event

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

Data plane packet pool is under low water mark

TABLE 425 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 426 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 427 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 428 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 429 Data plane process restarted event

Event	Data plane process restarted
Event Type	dpProcessRestart
Event Code	520

TABLE 429 Data plane process restarted event (continued)

Event	Data plane process restarted
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 430 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 431 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 432 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 433 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 434 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 435 Data plane upgrading event

Event	Data plane upgrading
Event Type	dpUpgrading
Event Code	551
Severity	Informational

TABLE 435 Data plane upgrading event (continued)

Event	Data plane upgrading
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 436 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 437 Data plane upgrade failed event

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

> **NOTE**
> Refer to Data Plane Alarms on page 74.

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

> **NOTE**
> Events 1257 to 1267 are not applicable to SCG.

TABLE 438 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 SCG.

TABLE 439 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 SCG.

TABLE 440 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 SCG.

TABLE 441 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.

> **NOTE**
> Events 1257 to 1267 are not applicable to SCG.

Data plane disconnects to the other data plane

> **NOTE**
> Events 1257 to 1267 are not applicable to SCG.

TABLE 442 Data plane disconnects to the other data plane event

Event	Data plane disconnects to the other data plane
Event Type	dpP2PTunnelDisconnected
Event Code	1262
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "dpIP"="xx.xx.xx.xx", "targetDpKey"="xx:xx:xx:xx:xx:xx","targetDpIp"="xxx.xxx.xxx.xxx"
Displayed on the web interface	Data Plane[{dpName&&dpKey}] disconnects to the other Data Plane[{targetDpKey&&targetDpIp}]
Description	This event occurs when the data plane disconnects from another data plane.

Start CALEA mirroring client in data plane

> **NOTE**
> Events 1257 to 1267 are not applicable to SCG.

TABLE 443 Start CALEA mirroring client in data plane event

Event	Start CALEA mirroring client in data plane
Event Type	dpStartMirroringClient
Event Code	1263

TABLE 443 Start CALEA mirroring client in data plane event (continued)

Event	Start CALEA mirroring client in data plane
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 SCG.

TABLE 444 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 445 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 446 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 447 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 448 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 449 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 450 Data plane DHCP IP capacity usage rate is 100 percent event

Event	Data plane DHCP IP capacity usage rate is 100 percent
Event Type	dpDhcpIpCapacityUsageRate100
Event Code	1286
Severity	Major
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "totalLicenseCnt"="1234567890", "consumedLicenseCnt"="1234567890", "availableLicenseCnt"="1234567890"
Displayed on the web interface	Data Plane[{dpKey}] DHCP IP Capacity usage rate is 100 percent. (total [{totalLicenseCnt}], consumed [{consumedLicenseCnt}], available [{availableLicenseCnt}])
Description	This event occurs when the data plane NAT session capacity usage rate is 100%.

NOTE
Refer to Data Plane Alarms on page 74.

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 451 dpIpmiThempBB event

Event	dpIpmiThempBB
Event Type	dpIpmiThempBB

TABLE 451 dpIpmiThempBB event (continued)

Event	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 452 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}].
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 453 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 454 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 455 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 456 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"

TABLE 456 dpIpmiREFan event (continued)

Event	dpIpmiREFan
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 backup success

TABLE 457 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"
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 458 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 459 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.

TABLE 459 Data plane restore success event (continued)

Event	Data plane restore success
Description	This event occurs when Data plane restore is successful.

Data plane restore failed

TABLE 460 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.

IPMI Events

> **NOTE**
> This section is not applicable for vSZ-E.

Following are the events related to IPMIs.

- ipmiThempBB on page 216
- ipmiThempP on page 217
- ipmiFan on page 217
- ipmiFanStatus on page 217
- ipmiREThempBB on page 218
- ipmiREThempP on page 218
- ipmiREFan on page 218
- ipmiREFanStatus on page 219

ipmiThempBB

TABLE 461 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}]

TABLE 461 ipmiThempBB event (continued)

Event	ipmiThempBB
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 462 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 463 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 464 ipmiFanStatus event

Event	ipmiFanStatus
Event Type	ipmiFanStatus
Event Code	912
Severity	Major
Attribute	"id"="x", "status"="xxxxx", "nodeMac"="xx:xx:xx:xx:xx:xx"

TABLE 464 ipmiFanStatus event (continued)

Event	ipmiFanStatus
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 465 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 466 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 467 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}].

TABLE 467 ipmiREFan event (continued)

Event	ipmiREFan
Description	This event occurs when the system fan module comes back to the normal status.

ipmiREFanStatus

TABLE 468 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 78.

Licensing Interface Events

Following are the events related to licensing.

License sync succeeded

TABLE 469 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 470 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 471 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 472 License import failed event

Event	License import failed
Event Type	licenseImportFail

TABLE 472 License import failed event (continued)

Event	License import failed
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 473 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 474 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 475 Insufficient license capacity event

Event	Insufficient license capacity
Event Type	apConnectionTerminatedDueToInsufficientLicense
Event Code	1256
Severity	Major
Attribute	"licenseType"=" xxx"
Displayed on the web interface	Insufficient [{licenseType}] license is detected and it will cause existing AP connections to terminate.

TABLE 475 Insufficient license capacity event (continued)

Event	Insufficient license capacity
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 476 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 477 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 478 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 479 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 480 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 481 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 80.

Insufficient license capacity

TABLE 482 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 483 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 484 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 485 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 486 SCI has been disabled event

Event	SCI has been disabled
Event Type	disabledSciDueToUpgrade
Event Code	4004

TABLE 486 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 487 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 82.

Session Events

Following event is related to user equipment TTG session.

- Delete all sessions on page 226

Delete all sessions

TABLE 488 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 489 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 490 LS authentication failure event

Event	LS authentication failure
Event Type	scgLBSAuthFailed
Event Code	722
Severity	Major

TABLE 490 LS authentication failure event (continued)

Event	LS authentication failure
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 491 {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 492 {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 493 {produce.short.name} received passive request event

Event	{produce.short.name} received passive request
Event Type	scgLBSStartLocationService
Event Code	725
Severity	Informational
Attribute	"nodeMac"="xx:xx:xx:xx:xx:xx:", "type"="", "venue"="", "SZMgmtIp"="", "band"=""

TABLE 493 {produce.short.name} received passive request event (continued)

Event	{produce.short.name} received passive request
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 494 {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 495 {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 496 {produce.short.name} sent AP info by venue report event

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

{produce.short.name} sent query venues report

TABLE 497 {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 498 {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 499 {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 500 {produce.short.name} forwarded footfall request to AP event

Event	{produce.short.name} forwarded footfall request to AP
Event Type	scgLBSFwdPassiveFFReq

TABLE 500 {produce.short.name} forwarded footfall request to AP event (continued)

Event	{produce.short.name} forwarded footfall request to AP
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 501 {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 502 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 503 Syslog server unreachable event

Event	Syslog server unreachable
Event Type	syslogServerUnreachable
Event Code	751
Severity	Major

TABLE 503 Syslog server unreachable event (continued)

Event	Syslog server unreachable
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 504 Syslog server switched event

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

Generate AP config for plane load rebalance succeeded

TABLE 505 Generate AP config for plane load rebalance succeeded event

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

Generate AP config for plane load rebalance failed

TABLE 506 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.

TABLE 506 Generate AP config for plane load rebalance failed event (continued)

Event	Generate AP config for plane load rebalance 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 507 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 508 FTP transfer error event

Event	FTP transfer error
Event Type	ftpTransferError
Event Code	971
Severity	Warning
Attribute	"ip"="xxx.xxx.xxx.xxx", "portID"="xxxx", "reason"="xxxxx"
Displayed on the web interface	File [{reason}] transferred to FTP server [{ip}:{portID}] unsuccessfully
Description	This event occurs when the file transfer to the FTP server fails.

File upload

TABLE 509 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 510 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 511 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 512 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 513 SMS sent failed event

Event	SMS sent failed
Event Type	smsSendFailed

TABLE 513 SMS sent failed event (continued)

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

Process restart

TABLE 514 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 515 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 516 Keepalive failure event

Event	Keepalive failure
Event Type	keepAliveFailure
Event Code	1003
Severity	Major

TABLE 516 Keepalive failure event (continued)

Event	Keepalive failure
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 517 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 SCG.

TABLE 518 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 519 CALEA UE Matched event

Event	CALEA UE Matched
Event Type	dpCaleaUeInterimMatched
Event Code	1268

TABLE 519 CALEA UE Matched event (continued)

Event	CALEA UE Matched
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 520 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 521 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 522 ZD AP rejected event

Event	ZD AP rejected
Event Type	zdAPRejected
Event Code	2003

TABLE 522 ZD AP rejected event (continued)

Event	ZD AP rejected
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 523 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 524 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 525 Database error event

Event	Database error
Event Type	recoverCassandraError
Event Code	3011
Severity	Informational
Attribute	"nodeName"="xxx","reason"="recovery reason"

TABLE 525 Database error event (continued)

Event	Database error
Displayed on the web interface	Recover database error on node [{nodeName}], reason : [].
Description	This event occurs when the internal errors on the database are fixed.

Password expiration

TABLE 526 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 527 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 528 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 account is idle for a period of time.

Disable inactive admins

TABLE 529 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 530 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 Data Plane Alarms on page 74.

Unconfirmed program detection

TABLE 531 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 532 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 533 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 534 Switch warning message event

Event	Switch warning message
Event Type	SwitchWarningMessage
Event Code	20003

TABLE 534 Switch warning message event (continued)

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

Switch CPU warning threshold exceed

TABLE 535 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 536 Switch CPU major threshold exceed event

Event	Switch CPU warning threshold exceed
Event Type	majorCpuThresholdExceed
Event Code	22011
Severity	Major
Attribute	"switchSerialNumber"="x", cpuUsage="x%" (Warning Threshold – Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[CPU Usage - {switchSerialNumber}] CPU major threshold {cpuUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when CPU usage of the Switch crosses the major threshold.

Switch CPU critical threshold exceed

TABLE 537 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}

TABLE 537 Switch CPU critical threshold exceed event (continued)

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

Switch memory warning threshold exceed

TABLE 538 Switch memory warning threshold exceed event

Event	Switch memory warning threshold exceed
Event Type	warningCpuThresholdExceed
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 539 Switch memory major threshold exceed event

Event	Switch memory major threshold exceed
Event Type	majorMemoryThresholdExceed
Event Code	22021
Severity	Major
Attribute	"switchSerialNumber"="x", memoryUsage="x%" (Warning Threshold – Critical Threshold),switchName = "x", switchMac = "xx:xx:xx:xx:xx:xx"
Displayed on the web interface	[Memory Usage - {switchSerialNumber}] Memory major threshold {memoryUsage} exceeded on Switch {switchName&switchMac}
Description	This event occurs when memory usage of the Switch crosses the major threshold.

Switch memory critical threshold exceed

TABLE 540 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}

TABLE 540 Switch memory critical threshold exceed event (continued)

Event	Switch memory critical threshold exceed
Description	This event occurs when memory usage of the Switch crosses the critical threshold of 100%.

Switch custom warning threshold exceed

TABLE 541 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 542 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 543 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 544 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 545 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 546 Accept certificate signing request event

Event	Accept certificate signing request
Event Type	acceptCertificateSigningRequest
Event Code	22002
Severity	Informational
Attribute	switchSerialNumber = "x"
Displayed on the web interface	[SCEP - {switchSerialNumber}] Accept Certificate Signing Request.
Description	This event occurs when there is a SCEP Accept Certificate Signing Request.

Reject certificate signing request

TABLE 547 Reject certificate signing request event

Event	Reject certificate signing request
Event Type	rejectCertificateSigningRequest
Event Code	22003
Severity	Major

TABLE 547 Reject certificate signing request event (continued)

Event	Reject certificate signing request
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 548 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 on page 247
- Memory threshold exceeded on page 247
- Disk usage threshold exceeded on page 247
- CPU threshold back to normal on page 248
- Memory threshold back to normal on page 248
- Disk threshold back to normal on page 248
- The drop of client count threshold exceeded on page 248
- License threshold exceeded on page 249
- HDD health degradation on page 249
- Rate limit threshold surpassed on page 249
- Rate limit threshold restored on page 250
- Rate limit for TOR surpassed on page 250
- The number of users exceed its limit on page 251
- The number of devices exceeded its limit on page 251
- Over AP maximum capacity on page 251

CPU threshold exceeded

TABLE 549 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 550 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 551 Disk usage threshold exceeded event

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

CPU threshold back to normal

TABLE 552 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 553 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 554 Disk threshold back to normal event

Event	Disk threshold back to normal
Event Type	diskUsageThresholdBackToNormal
Event Code	955
Severity	Informational
Attribute	"nodeName"="xxx","nodeMac"="xx:xx:xx:xx:xx:xx", "perc"="XX"
Displayed on the web interface	Disk threshold [{perc}%] got back to normal on control plane [{nodeName}-C].
Description	This event occurs when the disk usage comes back to normal.

The drop of client count threshold exceeded

TABLE 555 The drop of client count threshold exceeded event

Event	The drop of client count threshold exceeded
Event Type	clientCountDropThresholdExceeded
Event Code	956
Severity	Warning

TABLE 555 The drop of client count threshold exceeded event (continued)

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

License threshold exceeded

TABLE 556 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 557 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 558 Rate limit threshold surpassed event

Event	Rate limit threshold surpassed
Event Type	rateLimitThresholdSurpassed
Event Code	1300
Severity	Major

TABLE 558 Rate limit threshold surpassed event (continued)

Event	Rate limit threshold surpassed
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SZMgmtIp"="2.2.2.2" "aaaSrvIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "MOR"=1000 "THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold surpassed for AAA Server [{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 559 Rate limit threshold restored event

Event	Rate limit threshold restored
Event Type	rateLimitThresholdRestored
Event Code	1301
Severity	Informational
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SZMgmtIp"="2.2.2.2" "aaaSrvIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "MOR"=1000 "THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Threshold restored for AAA Server [{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 560 Rate limit for TOR surpassed event

Event	Rate limit for TOR surpassed
Event Type	rateLimitTORSurpassed
Event Code	1302
Severity	Critical
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SZMgmtIp"="2.2.2.2" "aaaSrvIp"="1.1.1.1" "AAAServerType"="Auth/Acct" "MOR"=1000 "THRESHOLD"="500" "TOR"="501"
Displayed on the web interface	Maximum Outstanding Requests (MOR) surpassed for AAA Server [{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

TABLE 560 Rate limit for TOR surpassed event (continued)

Event	Rate limit for TOR surpassed
	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 561 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 562 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 96.

Over AP maximum capacity

TABLE 563 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.

TABLE 563 Over AP maximum capacity event (continued)

Event	Over AP maximum 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 564 Data plane accepted a tunnel request event

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

Data plane rejected a tunnel request

NOTE

This event is not applicable for vSZ-E.

TABLE 565 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 566 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 567 AP created a tunnel event

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

AP tunnel disconnected

NOTE
This event is not applicable for vSZ-E.

TABLE 568 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 569 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 570 AP SoftGRE tunnel fails over secondary to primary event

Event	AP SoftGRE tunnel fails over secondary to primary
Event Type	apSoftGRETunnelFailoverStoP
Event Code	612
Severity	Warning
Attribute	"apMac"="xx:xx:xx:xx:xx:xx", "primaryGRE"="xxx.xxx.xxx.xxx", "secondaryGRE"="xxxx"
Displayed on the web interface	AP [{apName&&apMac}] fails over from secondaryGRE[{secondaryGRE}] to primaryGRE[{primaryGRE}].
Description	This event occurs when AP moves from a secondary to a primary GRE.

AP SoftGRE gateway reachable

TABLE 571 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 572 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 573 Data plane set up a tunnel event

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

AP secure gateway association success

TABLE 574 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 575 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 576 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 101.

Tunnel Events - Data Plane

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

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

- DP sGRE GW unreachable on page 257
- DP sGRE keep alive timeout on page 257
- DP sGRE GW inactive on page 258
- DP DHCPRelay no response on page 258
- DP DHCPRelay failover on page 258
- DP sGRE new tunnel on page 258
- DP sGRE keepalive recovery on page 259
- DP DHCPRelay response recovery on page 259
- DP sGRE GW reachable on page 259
- DP sGRE GW active on page 260

DP sGRE GW unreachable

TABLE 577 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 578 DP sGRE keep alive timeout event

Event	DP sGRE keep alive timeout
Event Type	dpSgreKeepAliveTimeout
Event Code	616
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x
Displayed on the web interface	Data plane [{dpName&&dpKey}] detected KeepAlive packet to Core Gateway [{GatewayIP}] is lost due to timeout
Description	This event occurs when the data plane detects that a keep alive packet to the core network gateway is lost due to a timeout.

DP sGRE GW inactive

TABLE 579 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 580 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 581 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 582 DP sGRE new tunnel event

Event	DP sGRE new tunnel
Event Type	dpSgreNewTunnel

TABLE 582 DP sGRE new tunnel event (continued)

Event	DP sGRE new tunnel
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 583 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 584 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 585 DP sGRE GW reachable event

Event	DP sGRE GW reachable
Event Type	dpSgreGWReachable
Event Code	624
Severity	Informational
Attribute	"dpKey"="xx:xx:xx:xx:xx:xx", "gatewayIP"="x.x.x.x"

TABLE 585 DP sGRE GW reachable event (continued)

Event	DP sGRE GW reachable
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 586 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