USER GUIDE

Ruckus LTE AP Alarms and Events Guide Release SC 03.00.00.00XX

Part Number: 800-72541-001
Publication Date: January 2020

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Preface

Document Conventions

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

TABLE 1 Text Conventions

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

Notes, Cautions, and Safety Warnings

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

NOTE

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

ATTENTION

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

CAUTION

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

DANGER

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

Command Syntax Conventions

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

Convention	Description
bold text	Identifies command names, keywords, and command options.

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

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

Ruckus Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting Ruckus Customer Services and Support

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

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

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

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

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

About This Document

Purpose of the Document

This document provides information about various alarms and events that Ruckus LTE AP generates.

Intended Audience

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

Abbreviations

The following table describes the abbreviations used in the document.

TABLE 2 Abbreviations

Abbreviation	Description
AP	Access Point
CA	Carrier Aggregation or Certificate Authority (part of a PKI)
CBRS	Citizen Broadband Radio Service
CMP	Certificate Management Protocol
CPI	Certified Professional Installer
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPD	Digital Pre-Distortion
EARFCN	E-UTRAN absolute radio frequency channel number
EPC	Evolved Packet Core
FTP	File Transfer Protocol
GPS	Global Positioning System
HeMS	Home eNodeB Management System
HO	Handover
HTTPS	HyperText Transport Protocol Secure
KPI	Key Performance Indicator
LO	Local Oscillator
LTE	Long Term Evolution

TABLE 2 Abbreviations (continued)

Abbreviation	Description
MME	Mobility Management Entity
MQTT	Message Queuing Telemetry Transport
NHN	Neutral Host Network
NTP	Network Time Protocol
OAM	Operation and Management
OCSP	Online Certificate Status Protocol
PCI	Physical [layer] Cell Identifier
PLMN	Public Land Mobile Network
PM	Performance Management
PoE	Power over Ethernet
SAS	Spectrum Access System
SCTP	Stream Control Transmission Protocol

Introduction to Ruckus LTE AP Alarms

Ruckus LTE AP Alarms Overview

Alarms are unexpected events indicating a condition that typically requires corrective action. Unexpected events are distinct incidents that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Ruckus LTE AP alarms are in response to one or more related events. Only certain events generate alarms.

Alarms have a severity (Critical, Major, Minor, Warning, and Information). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or is cleared manually).

Following is the list of Ruckus LTE AP alarms described in this document:

Naming Convention for Alarms

The following naming convention is used to describe the alarms.

Field Name	Field Description			
Alarm Identifier	Alarm identifier.			
Description	Alarm as displayed on Cloud. <Specific problem>:<Additional Text>:<Additional Information>			
Details				
Additional Information	Information displayed on Cloud.			
Specific Problem	Specific problem responsible for the event.			
Perceived Severity	Indicates the severity of an alarm sent to HeMS.			
Action to clear alarm	Provides the action required to clear an alarm.			
Entered Event	**Exit Event**	**Probable Cause**	**System Actions**	**Additional Text**
<number> Event at which an alarm is raised.	Event at which an alarm is cleared.	Probable cause of the event.	Action taken by the system in case an alarm is raised.	Text displayed on Cloud.

NOTE

<number> indicates the text in the Additional Information field mapped to the respective Entered event.

Cell Id <i> where i can be 1 or 2 in case of CA mode and 1 in case of non-CA mode.

Classification of Alarms Severity

The alarms can be classified based on severity as follows:

Severity	Description
Critical	A critical alarm is raised when LTE AP is not in an operable state.
Major	A major alarm is raised when LTE AP can operate but some functionality is not occurring. For example, cell transmission not taking place.
Minor	A minor alarm is raised when LTE AP can operate but certain functionality is not working efficiently.
Warning	It is a warning to be considered within a time period.
Information	It is an information about LTE AP.

Ruckus LTE AP Alarms

Ruckus LTE AP Alarms in Release SC 3.0

The following section provides detailed information about alarms.

Hardware Failure Alarm

Alarm Identifier	100			
Description	Missing RF configurations:<Additional text>:<Additional Information>			
Details				
Additional Information	1. Alarm triggered when Tx Local Oscillator goes out of sync.Carrier ID = <id> 2. Alarm triggered when Rx Local Oscillator goes out of sync.Carrier ID = <id> 3. Alarm triggered when Tx Power exceeds maximum expected value.Carrier ID = <id> 4. Alarm triggered when Tx Power is outside the expected range.Carrier ID = <id> 5. Alarm triggered when selected configuration is not supported by a topology.Carrier ID = <id> 6. Alarm triggered when configuration specified is not supported by calibration data.Carrier ID = <id>			
Specific Problem	Missing RF configurations.			
Perceived Severity	Critical			
Action to clear alarm	LTE AP to be reset to factory defaults.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
1. Tx or Rx LO out of sync	Tx LO is in sync.	Tx LO out of sync.	Cell transmission is disabled.	txLOSyncLoss
2. Rx LO out of sync	Rx LO is in sync	Rx LO out of sync.		rxLOSyncLoss
3. Excessive Tx Power	Tx Power should be in range.	Excessive Tx Power		txPowerExceededMax
4. Tx Power out of expected range	Tx Power in expected range.	Tx Power out of expected range		txPowerOutOfBounds
5. Invalid configuration (major)	Valid configuration is required.	Invalid configuration (major)		invalidConfiguration
6. Configuration not supported by calibration data	Valid configuration is required.	Configuration not supported by calibration data.		calibrationRequired

Temperature Critical Alarm

Alarm Identifier	101
Description	RSC temperature critically high:temperatureCritical:A Carrier's path temperature has exceeded a critical threshold. Carrier ID = <id>.
Details	
Additional Information	A Carrier's path temperature has exceeded a critical threshold. Carrier ID = <id>.
Specific Problem	RSC temperature critically high.
Perceived Severity	Critical

Action to clear alarm	1. Switch off LTE AP and reboot it. 2. LTE AP is operational after 10 minutes.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when temperature exceeds maximum critical threshold defined for normal LTE AP operation.	LTE AP temperature within Normal Range alarm is sent when LTE AP temperature returns to normal operating range.	LTE AP temperature exceeds maximum critical threshold.	LTE radio is disabled.	temperatureCritical.

Temperature Warning Alarm

Alarm Identifier	102			
Description	RSC temperature too high:temperatureWarning:A Carriers's path temperature has exceeded a warning threshold. Carrier ID = <id>			
Details				
Additional Information	A Carriers's path temperature has exceeded a warning threshold. Carrier ID = <id>			
Specific Problem	RSC temperature too high.			
Perceived Severity	Warning			
Action to clear alarm	1. Switch off LTE AP and reboot it. 2. Switch on LTE AP after 10 minutes.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional text**
Alarm is triggered when the temperature for one of the carrier's paths has exceeded a warning threshold.	LTE AP temperature within Normal Range alarm is sent when LTE AP temperature returns to normal operating range.	LTE AP temperature is higher than expected.	A warning alarm is raised.	temperatureWarning.

LTE Radio OpState Disabled Alarm

Alarm Identifier	105			
Description	LTE Radio OpState is disabled:AP Service is disabled. S1 connection is terminated until AP Service shall be enabled.:LTE Radio OP State is disabled.			
Details				
Additional Information	LTE Radio OP State is disabled.			
Specific Problem	LTE Radio OpState is disabled.			
Perceived Severity	Critical			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Loss of sync	Sync is restored.	LTE operational state is disabled.	No action is required.	AP Service is disabled. S1 connection is terminated until AP Service shall be enabled.
Loss of EPC connectivity	EPC connectivity is reestablished.			
Loss of SAS connectivity (Transmit Expiry time)	SAS connectivity is restored.			

Loss of Sync Sources Alarm

Alarm Identifier	108

Description	Sync Lost: All Sync sources lost: Alarm is triggered when all sync sources are lost.			
Details				
Additional Information	Alarm is triggered when all sync sources are lost.			
Specific Problem	Sync Lost			
Perceived Severity	Major			
Action to clear alarm	LTE AP reboots after expiry of holdOverTimer expiry. The value of holdoverTimer varies depending upon configured syncsource.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when clock reports from all active sync sources are missing or invalid.	LTE AP is expected to reboot after holdOverTimer expiry. The value of holdOverTimer varies depending upon configured syncsource.	Loss of synchronization.	LTE AP is expected to reboot after half an hour of sync loss based on configuration.	All sync sources lost.

HoldOver Timeout Alarm

Alarm Identifier	109			
Description	Sync holdover expired: Holdover timeout: Alarm is triggered when holdover timeout occurs.			
Details				
Additional Information	Alarm is triggered when holdover timeout occurs.			
Specific Problem	Sync holdover expired.			
Perceived Severity	Major			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when LTE AP is unable to achieve sync till holdover expiry time occurs.	Sync Acquired alarm is sent when the time base re-acquires synchronization to an external source.	Loss of synchronization.	LTE AP reboots.	Holdover timeout.

Dead Peer Detection Alarm

Alarm Identifier	111			
Description	EPC SeGW connection lost <Additional Text><Additional Information>			
Details				
Additional Information	1. Link down for a peer with which EPC IPSec tunnel is established. 2. Sent when Ipsec procedure is failed for all the secGw EPC servers.			
Specific Problem	EPC SeGW connection lost.			
Perceived Severity	Critical			
Action to clear alarm	• EPC SeGW reachability might have been lost/link is down. Check for EPC SeGW reachability. • If EPC SeGW is reachable, then check for IPSec-related service running on EPC SeGW.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
1. Alarm is triggered when EPC IPSec tunnel peer link is down.	EPC SeGW Connection Established alarm is sent when Ruckus LTE AP has (re)-established an IPSec tunnel to at least one of the EPC's SeGW(s).	Link down for a peer with which EPC tunnel is established.	LTE AP retries IPSec tunnel re-establishment until reboot.	DPD detected EPC,<url>.IPSec proc failed for EPC.

2. Alarm is triggered when EPC IPSec tunnel peer link is down.	EPC SeGW Connection Established alarm is sent when Ruckus LTE AP has (re)-established an IPSec tunnel to at least one of the EPC's SeGW(s).	Link down for a peer with which EPC tunnel is established.	LTE AP retries IPSec tunnel re-establishment until reboot.	IPSEC proc failed for EPC.

SCTP Association Failure Alarm

Alarm Identifier	112			
Description	RRC SCTP Association Failure - MME IP Address = <IP Address>, RRC/SCTP association failure alarm.			
Details				
Additional Information	RRC/SCTP association failure alarm.			
Specific Problem	RRC SCTP Association Failure			
Perceived Severity	Critical			
Action to clear alarm	Check network configuration and correct it in case network configurations are incorrect.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when S1AP Connection fails or is torn down with MME.	S1AP Connection Established alarm is set when Ruckus LTE has (re-)established an S1AP connection.	Connection Establishment error.	Cell transmission is disabled.	MME IP Address = <IP>

File Upload Failure Alarm

Alarm Identifier	115			
Description	File upload/streaming failure - <Additional Text>, Failed to upload KPIs to File Server/MQTT broker.			
Details				
Additional Information	Failed to upload KPIs to File Server/ MQTT broker.			
Specific Problem	File upload/streaming failure.			
Perceived Severity	Minor			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when LTE AP is in overload condition and fails to send the PM xml file TR-069 agent.	Alarm will clear after the next upload hour if server is reachable.	File error.	No action is required.	CONFIG_FILE Upload to ftp server Failure
Alarm is triggered whe LTE AP fails to upload log files to FTP server.	Alarm will clear after the next upload hour if server is reachable.	File error	No action is required.	LOG_FILE Upload to ftp server Failure

Software Activation Failure Alarm

Alarm Identifier	117
Description	Firmware image download failure - <Additional Text>, Software Activation/Download failure
Details	
Additional Information	Software Activation/Download failure.
Specific Problem	Firmware image download failure.
Perceived Severity	Minor

Action to clear alarm	1. Check for correct package with correct checksum. 2. Check if correct FTP credentials are provided in Upgrade request or check FTP server. 3. Some system commands may be failing on Ruckus LTE AP. So, reboot the LTE AP in that case. 4. Free some space in /mnt/flash. 5. Download correct package as per board type.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
1. Software download failure reported due to Checksum failure.	Software download is triggered again.	Software download failure.	No action is required.	Checksum failure.
2. Download failure				Download failure.
3. Internal error				Internal error.
4. Unable to untar the image file				Unable to untar package.
5. Package Name incompatible				Package Name incompatible.
6. Software compatibility failed				1. Downgrade not possible without tz.mbn image. 2. Downgrade not possible from current software version. 3. Upgrade not possible without tz.mbn image.

Configuration Image Download Failure Alarm

Alarm Identifier	119			
Description	Configuration image download failure: Download Failure: SwMgr failed to download the configuration image			
Details				
Additional Information	SwMgr failed to download the configuration image.			
Specific Problem	Configuration image download failure.			
Perceived Severity	Minor			
Action to clear alarm	Correct FTP credentials provided in Upgrade request or check FTP server.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional text**
Alarm is triggered when Software Manager fails to download configuration image.	Another Configuration Image Download request.	Configuration image fails to download.	No action is required.	Download Failure

File Persistence Error Alarm

Alarm Identifier	120
Description	File persistence error: No vendor config file present: File is no longer present or has been corrupted.

Details				
Additional Information	File is no longer present or has been corrupted.			
Specific Problem	File persistence error.			
Perceived Severity	Warning			
Action to clear alarm	Check if vendor log file instance requested for upload exists or not on Ruckus LTE AP.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when RPC is uploaded for a configuration file which does not exist or for crash logs which do not exist.	Next RPC upload request.	File is no longer present or has been corrupted.	No action is required.	No vendor config file present.

Server Authentication Failure Alarm

Alarm Identifier	122
Description	Server authentication failure - <Additional Text>, <Additional Info>.
Details	
Additional Information	1. Sent when Ruckus LTE AP is unable to resolve FQDN of initial server. 2. Sent when Ruckus LTE AP is unable to ping to initial server. 3. Sent when Ruckus LTE AP is unable to resolve FQDN of serving server. 4. Sent when Ruckus LTE AP is unable to ping to serving server. 5. Sent when Ruckus LTE AP is unable to resolve FQDN of HeMS Security Gateway 1. 6. Sent when Ruckus LTE AP is unable to ping to HeMS Security Gateway 1. 7. Sent when IPSec tunnel creation procedure failed for HeMS Security Gateway 1. 8. Sent when Ruckus LTE AP is unable to resolve FQDN of Security Gateway 2. 9. Sent when Ruckus LTE AP is unable to ping to HeMS Security Gateway 2. 10. Sent when IPSec tunnel creation procedure failed for HeMS Security Gateway 2. 11. Sent when Ruckus LTE AP is unable to resolve FQDN of Security Gateway 3. 12. Sent when Ruckus LTE AP is unable to ping to HeMS Security Gateway 3. 13. Sent when IPSec tunnel creation procedure failed for HeMS Security Gateway 3. 14. Sent when Ruckus LTE AP is unable to resolve FQDN of EPC Security Gateway 1. 15. Sent when Ruckus LTE AP is unable to ping to EPC Security Gateway 1. 16. Sent when IPSec tunnel creation procedure failed for EPC Security Gateway 1. 17. Sent when Ruckus LTE AP is unable to resolve FQDN of EPC Security Gateway 2. 18. Sent when Ruckus LTE AP is unable to ping to EPC Security Gateway 2. 19. Sent when IPSec tunnel creation procedure failed for EPC Security Gateway 2. 20. Sent when Ruckus LTE AP is unable to resolve FQDN of EPC Security Gateway 3. 21. Sent when IPSec tunnel creation procedure failed for EPC Security Gateway 3.
Specific Problem	Server authentication failure.
Perceived Severity	Major

Action to clear alarm	1. • Check if DNS server for iHeMS is configured and is reachable. • If reachable, check if DNS is configured to resolve the iHeMS FQDN. 2. iHems reachability has been lost. Check for iHeMS reachability. 3. • Check if DNS server for iHeMS is configured and is reachable. • If reachable, check if DNS is configured to resolve the iHeMS FQDN. 4. ACS reachability has been lost. Check for ACS reachability. 5. • Check if DNS server for HeMS SecGw1 is configured and is reachable. • If reachable, check if DNS is configured to resolve the HeMS SecGw1 FQDN. 6. HeMS SecGw1 reachability has been lost or link is down. Check for SecGw1 reachability. 7. • HeMS SecGw1 reachability might have been lost or link is down. Check for SecGw1 reachability. • If gateway is reachable, then check for IPSec-related service is running on SecGw1. 8. • Check if DNS server for HeMS SecGw2 is configured and is reachable. • If reachable, check if DNS is configured to resolve the HeMS SecGw2 FQDN. 9. HeMS SecGw2 reachability has been lost or link is down. Check for SecGw2 reachability. 10. • HeMS SecGw2 reachability might have been lost or link is down. Check for SecGw2 reachability. • If gateway is reachable then check for IPSEC related service running on HeMS SecGw2. 11. • Check if DNS server for HeMS Security Gateway3 is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of HeMS SecGw3. 12. HeMS SecGw3 reachability has been lost or link is down. Check for SecGw3 reachability. 13. • HeMS SecGw3 reachability might have been lost or link is down. Check for SecGw3 reachability • If gateway is reachable, then check for IPSec-related service running on HeMS SecGw3. 14. • Check if DNS server for EPC Security Gateway1 is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of EPC SecGw1. 15. EPC SecGw1 reachability has been lost. Check for EPC SecGw1 reachability. 16. • EPC SecGw1 reachability might have been lost or link is down. Check for SecGw1 reachability. • If gateway is reachable, then check for IPSec-related service running on EPC SecGw1. 17. • Check if DNS server for EPC Security Gateway2 is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of EPC SecGw2. 18. EPC SecGw2 reachability has been lost or link is down. Check for EPC SecGw2 reachability. 19. • EPC SecGw2 reachability might have been lost or link is down. Check for SecGw2 reachability. • If gateway is reachable, then check for IPSec-related service running on EPC SecGw2. 20. • Check if DNS server for EPC Security Gateway3 is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of EPC SecGw3. 21. EPC SecGw3 reachability has been lost or link is down. Check for EPC SecGw3 reachability.

Entered Event	Exit Event	Probable Cause	System Action	Additional Text
1. IhemsFqdnResolutionFailure	When LTE AP resolves FQDN of initial server.	iHeMS FQDN could not be resolved.	LTE AP retries to resolve FQDN of initial server until reboot.	iHeMS FQDN resolution failure,<url>
2. IhemsDiscoveryFailure	When iHeMS becomes reachable.	iHeMS Reachability failure.	LTE AP retries to check reachability of initial server until reboot.	iHeMS discovery failure,<url>
3. ShmsFqdnResolutionFailure	When LTE AP resolves FQDN for sHeMS.	sHeMS FQDN could not be resolved.	LTE AP retries to resolve FQDN of serving server until reboot.	sHeMS FQDN resolution failure,InternetGatewayDevice. ManagementServer.URL,<url>.

4. ShemsDiscoveryFailure	When sHeMS becomes reachable.	sHeMS reachability failure.	LTE AP retries to check reachability of serving server until reboot.	sHeMS discovery failure,InternetGatewayDevice. ManagementServer.URL,<url>
5. HemsSecurityGateway1FqdnResolutionFailure	When LTE AP resolves FQDN of HeMS Security Gateway 1.	HeMS Security Gateway 1 FQDN cannot be resolved.	LTE AP retries to resolve HeMS Security Gateway 1 FQDN until reboot.	Security HeMS Gateway 1 FQDN resolution,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1,<url>
6. HemsSecurityGateway1NotReachable	When LTE AP pings HeMS Security Gateway 1.	HeMS Security Gateway 1 reachability failure.	LTE AP retries to check reachability until reboot.	Security HeMS Gateway 1 not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1,<url>
7. IpsecProcedureFailedForHemsSecurityGateway1	When IPSec tunnel creation is successful for HeMS Security Gateway 1.	IPSec tunnel creation procedure fails for HeMS Security Gateway 1.	Recovery until reboot.	HEMS gateway 1 IPSEC proc failed,InternetGatewayDevice. S ervices.FAPService. {i}.FAPControl.LTE.Gateway.SecGWServer1,<url>
8. HemsSecurityGateway2FqdnResolutionFailure	When LTE AP resolves FQDN of HeMS Security Gateway 1.	Security Gateway 2 FQDN cannot be resolved.	Retries to resolve HeMS GAteway 2 FQDN until reboot.	HeMS Gateway 2 FQDN resolution failure,InternetGatewayDevice .X _001392_FAPMgmtSecGW.SecGWServer2,<url>.
9. HemsSecurityGateway2NotReachable	When LTE AP resolves FQDN of HeMS Security Gateway 2.	HeMS Security Gateway 2 reachability failure.	Retries to check reachability until reboot.	HeMS Gateway 2 not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer2,<url>
10. IpsecProcedureFailedForHemsSecurityGateway2	When tunnel creation procedure is successful for HeMS Security Gateway 2.	IPSec tunnel creation procedure fail for HeMS Security Gateway 2.	LTE AP retries until reachable.	HeMS Gateway 2 IPSec proc failed,InternetGatewayDevice. Services.FAPService. {i}.FAPControl.LTE.Gateway.SecGWServer2,<url>
11. HemsSecurityGateway3FqdnResolution Failure	LTE AP resolves FQDN of HeMS Security Gateway 3.	Security Gateway 3 FQDN cannot be resolved.	LTE AP retries resolution of serving server until reboot.	HeMS Gateway 3 FQDN resolution failure,InternetGatewayDevice .X _001392_FAPMgmtSecGW.SecGWServer3,<url>
12. HemsSecurityGateway3NotReachable	When LTE AP resolves FQDN of HeMS Security Gateway 3.	HeMS Security Gateway 3 reachability failure.	LTE AP retries to check reachability until reboot.	HeMS Gateway 3 not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer3,<url>.
13. IpsecProcedureFailedForHemsSecurityGateway3	When tunnel is created successfully.	IPSec tunnel creation procedure fail for HeMS Security Gateway 3.	LTE AP retries three times until recovery timer expires, then goes for retries again until reboot timer expires*.	HeMS Gateway 3 IPSec proc failed,InternetGatewayDevice. Services.FAPService. {i}.FAPControl.LTE.Gateway.SecGWServer3,<url>.
14. EPCSecurityGateway1FqdnResolution Failure	When LTE AP resolves FQDN successfully.	Security Gateway 1 FQDN cannot be resolved.	LTE AP retries for reachability until reboot.	EPC Gateway 1 FQDN resolution failure,InternetGatewayDevice .Services.FAPService. {i}.FAPControl.LTE.Gateway.SecGWServer1,<url>

15. EPCSecurityGateway1NotReachable	When LTE AP pings EPC Security Gateway 1 successfully.	EPC Security Gateway 1 reachability failure.	LTE AP retries to check reachability until reboot.	EPC Gateway 1 not reachable,nternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1,<url>.
16. IpsecProcedureFailedForEPCSecurityGateway1	When IPSec tunnel for EPC is created successfully.	IPSec tunnel creation procedure fails for EPC Security Gateway 1.	LTE AP retries until reboot timer expires*.	EPC Gateway 1 IPSec proc failed,InternetGatewayDevice.S ervices.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer1,<url>.
17. EPCSecurityGateway2FqdnResolution Failure	When LTE AP resolves FQDN successfully.	EPC Security Gateway 2 FQDN cannot be resolved.	LTE AP retries for reachability until reboot.	EPC Gateway 2 FQDN resolution failure,InternetGatewayDevice.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer2,<url>
18. EPCSecurityGateway2NotReachable	When LTE AP pings EPC Security Gateway 2 successfully.	EPC Security Gateway 2 reachability failure.	LTE AP retries to check reachability until reboot.	EPC Gateway 2 not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer2,<url>.
19. IpsecProcedureFailedForEPCSecurityGateway2	When IPSec tunnel for EPC is created successfully.	IPSec tunnel creation procedure fails for EPC Security Gateway 2.	LTE AP retries until reboot timer expires*.	EPC Gateway 2 IPSec proc failed,InternetGatewayDevice.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer2,<url>.
20. EPCSecurityGateway3FqdnResolutionFailure	When LTE AP resolves FQDN successfully.	EPC Security Gateway 3 FQDN cannot be resolved.	LTE AP retries for reachability until reboot.	EPC Gateway 3 FQDN resolution failure,InternetGatewayDevice.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer3,<url>
21. EPCSecurityGateway3NotReachable	When LTE AP pings EPC Security Gateway 3 successfully.	EPC Security Gateway 3 reachability failure.	LTE AP retries to check reachability until reboot.	EPC Gateway 3 IPSec proc failed,InternetGatewayDevice.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer3,<url>.

NOTE

*LTE AP reboots after reboot timer expiration.

Server Certificate Revoked Alarm

Alarm Identifier	123
Description	Server certificate revoked: <Additional text>, <Additional Info>
Details	

Additional Information	1. Sent when HeMS SecGw1 Certificate is no longer valid. 2. Sent when HeMS SecGw1 CA Certificate is no longer valid. 3. Sent when HeMS SecGw2 Certificate is no longer valid. 4. Sent when HeMS SecGw2 CA Certificate is no longer valid. 5. Sent when HeMS SecGw3 Certificate is no longer valid. 6. Sent when HeMS SecGw3 CA Certificate is no longer valid 7. Sent when EPC SecGw1 Certificate is no longer valid. 8. Sent when EPC SecGw1 CA Certificate is no longer valid. 9. Sent when EPC SecGw2 Certificate is no longer valid. 10. Sent when EPC SecGw2 CA Certificate is no longer valid. 11. Sent when EPC SecGw3 Certificate is no longer valid. 12. Sent when EPC SecGw3 CA Certificate is no longer valid. 13. Sent when iHeMS certificate is revoked. 14. Sent when CA certificate of iHeMS is revoked 15. Sent when Ruckus LTE AP certificate is revoked. 16. Sent when CA certificate of Ruckus LTE AP is revoked.			
Specific Problem	Server certificate revoked.			
Perceived Severity	Major			
Action to clear alarm	Replace the revoked certificate with valid/correct certificate.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional text**
1. HEMSSecGw1CertificateRevoked	No exit event.	HeMS Security Gateway 1 certificate is revoked.	Security module halts until reboot timer expires*.	HeMS gateway 1 Certificate revoked.
2. HEMSSecGw1CACertificateRevoked	No exit event.	OCSP server cannot validate HeMS Security Gateway 1 CA certificate.	When Security Gateway 1 Certificate is fetched correctly, then the alarm is cleared.	HeMS gateway 1 CA Certificate revoked.
3. HEMSSecGw2CertificateRevoked	No exit event.	HeMS Security Gateway 2 certificate is revoked.	Security module halts until reboot timer expires*.	HeMS gateway 2 Certificate revoked.
4. HEMSSecGw2CACertificateRevoked	No exit event.	OCSP server cannot validate HeMS Security Gateway 2 CA certificate.	Security module halts until reboot timer expires*.	HeMS gateway 2 CA Certificate revoked.
5. HEMSSecGw3CertificateRevoked	No exit event.	HeMS Security Gateway 3 certificate is revoked.	Security module halts until reboot timer expires*.	HeMS gateway 3 Certificate revoked.
6. HEMSSecGw3CACertificateRevoked	No exit event.	OCSP server cannot validate HeMS Security Gateway 3 CA certificate.	Security module halts until reboot timer expires*.	HeMS gateway 3 CA Certificate revoked.
7. EPCSecGw1CertificateRevoked	No exit event.	EPC Security Gateway 1 certificate is revoked.	Security module halts until reboot timer expires*.	EPC gateway 1 Certificate revoked.
8. EPCSecGw1CACertificateRevoked	No exit event.	OCSP server cannot validate EPC Security Gateway 1 CA certificate.	Security module halts until reboot timer expires*.	EPC gateway 1 CA Certificate revoked.
9. EPCSecGw2CertificateRevoked	No exit event.	EPC Security Gateway 2 certificate is revoked.	Security module halts until reboot timer expires*.	EPC gateway 2 Certificate revoked.

10. EPCSecGw2CACertificateRevoked	No exit event.	OCSP server cannot validate EPC Security Gateway 2 CA certificate.	OCSP server cannot validate EPC Security Gateway 2 CA certificate.	EPC gateway 2 CA Certificate revoked.
11. EPCSecGw3CertificateRevoked	No exit event.	EPC Security Gateway 3 certificate is revoked.	Security module halts until reboot timer expires*.	EPC gateway 3 Certificate revoked.
12. EPCSecGw3CACertificateRevoked	No exit event.	OCSP server cannot validate EPC Security Gateway 3 CA certificate.	Security module halts until reboot timer expires*.	EPC gateway 3 CA Certificate revoked.
13. IhemsOcspCertificateRevoked	No exit event.	iHeMS certificate is revoked.	Security module halts until reboot timer expires*.	iHeMS Certificate revoked.
14. IhemsCAcertificateRevoked	No exit event.	iHeMS CA certificate is revoked.	Security module halts until reboot timer expires*.	iHeMS CA Certificate revoked.
15. RscOcspCertificateRevoked	No exit event.	Ruckus LTE AP OCSP certificate is revoked.	Security module halts until reboot timer expires*.	Ruckus LTE AP Certificate revoked.
16. RscCAcertificateRevoked	No exit event.	Ruckus LTE AP CA certificate is revoked.	Security module halts until reboot timer expires*.	Ruckus LTE AP CA Certificate revoked.

NOTE

*LTE AP reboots after reboot timer expiration.

Server Revocation Check Failure Alarm

Alarm Identifier	124			
Description	Server revocation check failure - <Additional Text>, <Additional Info>			
Details				
Additional Information	1. Sent when OCSP/CRL procedure failed for EPCSecurityGateway2. 2. Sent when OCSP/CRL procedure failed for EPCSecurityGateway3. 3. Sent when iHeMS OCSP/CRL procedure failed. 4. Sent when Ruckus LTE AP OCSP/CRL procedure failed.			
Specific Problem	Server revocation check failure.			
Perceived Severity	Major			
Action to clear alarm	1. • EPC SecGw2 OCSP server is not reachable or link is down. Check for reachability of EPC SecGw2 OCSP server. • EPC SecGw2 OCSP server is not responding. Check if OCSP service is running and is configured to successfully check the status of EPC secGw2 certificate. 2. • EPC SecGw3 OCSP server is not reachable or link is down. Check for reachability of EPC SecGw3 OCSP server. • EPC SecGw3 OCSP server is not responding. Check if OCSP service is running and is configured to successfully check the status of EPC secGw3 certificate. 3. • iHems OCSP server is not reachable or link is down. Check for reachability of iHems OCSP server. • iHems OCSP server is not responding. Check OCSP service is running and is configured to successfully check the status of iHems certificate.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**

1. EPCSecGw2OCSPProcedureFailed	When OCSP procedure gets successful.	Server revocation check failure.	LTE AP retries OCSP procedure until reboot timer expires*.	EPC gateway 2 OCSP/CRL procfailed, InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer2,<url>
2. EPCSecGw3OCSPProcedureFailed	When OCSP procedure gets passed for EPC Security Gateway 3 successfully.	EPC Security Gateway 3 OCSP procedure failure.		EPC gateway 3 OCSP/CRL proc failed, InternetGatewayDevice.Services.FAPService.3.FAPControl.LTE.Gateway.SecGWServer1,<url>
3. IhemsOcspProcFailed	When iHeMS OCSP procedure gets successful.	iHeMS OCSP procedure failure.		iHeMS OCSP/CRL proc failed.
4. RscOcspProcFailed	When LTE AP OCSP procedure is completed successfully.	Ruckus LTE AP OCSP procedure failure.		OCSP/CRL failed for SAS <url>.

NOTE

*LTE AP reboots after reboot timer expiration.

OCSP Server not Reachable Alarm

Alarm Identifier	125
Description	OCSP/CRL Server not reachable: <Additonal text>, <Additional Info>
Details	
Additional Information	1. Sent when Ruckus LTE AP is unable to resolve FQDN of HeMS SecGw1 OCSP/CRL server 2. Sent when Ruckus LTE AP is unable to ping HeMS SecGw1 OCSP/CRL server. 3. Sent when Ruckus LTE AP is unable to resolve fqdn of HeMS SecGw2 OCSP/CRL server. 4. Sent when Ruckus LTE AP is unable to ping HeMS SecGw2 OCSP/CRL server. 5. Sent when Ruckus LTE AP is unable to resolve FQDN of HeMS SecGw3 OCSP/CRL server. 6. sent when Ruckus LTE AP is unable to ping HEMS SecGw3 OCSP/CRL server. 7. Sent when Ruckus LTE AP is unable to resolve fqdn of EPC SecGw1 OCSP/CRL server. 8. Sent when Ruckus LTE AP is unable to ping EPC SecGw1 OCSP/CRL server. 9. Sent when Ruckus LTE AP is unable to ping EPC SecGw2 OCSP/CRL server. 10. Sent when Ruckus LTE AP is unable to resolve fqdn of EPC SecGw3 OCSP/CRL server. 11. Sent when Ruckus LTE AP is unable to ping EPC SecGw3 OCSP/CRL server.
Specific Problem	OCSP/CRL Server not reachable.
Perceived Severity	Major

Action to clear alarm	1. • Check if DNS server for HeMS Security Gateway1 OCSP Server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of HeMS SecGw1 OCSP server. 2. HeMS SecGw1 OCSP server reachability has been lost / link is down. Check for HeMS SecGw1 OCSP server reachability. 3. • Check if DNS server for HeMS Security gateway2 OCSP Server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of HeMS SecGw2 OCSP server. 4. HeMS SecGw2 OCSP server reachability has been lost or link is down. Check for HeMS SecGw1 OCSP server reachability. 5. • Check if DNS server for HeMS Security Gateway3 OCSP Server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of HeMS SecGw3 OCSP Server. 6. HeMS SecGw3 OCSP server reachability has been lost / link is down. Check for HEMS SecGw3 OCSP server reachability. 7. • Check if DNS server for EPC Security Gateway1 OCSP Server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of EPC SecGw1 OCSP Server. 8. EPC SecGw1 OCSP server reachability has been lost or link is down. Check for EPC SecGw1 OCSP server reachability 9. EPC SecGw2 OCSP server reachability has been lost / link is down. Check for EPC SecGw2 OCSP server reachability. 10. • Check if DNS server for EPC Security gateway3 OCSP Server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of EPC SecGw3 OCSP Server. 11. EPC SecGw3 OCSP server reachability has been lost or link is down. Check for EPC SecGw3 OCSP server reachability.

Entered Event	Exit Event	Probable Cause	System Action	Additional Text
1. HEMSSecGw1OCSPserverFqdnResolutionFailure	When LTE AP is able to resolve FQDN successfully.	HEMS Security Gateway 1 OCSP server FQDN cannot be resolved.	LTE AP retries to resolve FQDN until reboot timer expires*.	HeMS gateway 1 OCSP/CRL server fqdn resolution failure,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1,<url>
2. HEMSSecGw1OCSPserverNotReachable	When LTE AP is able to ping the HeMS Security Gateway 1 OCSP server.	HEMS Security Gateway 1 OCSP server reachability failure.	LTE AP retries for reachability of Security Gateway 2 until reboot timer expires*.	HeMS gateway 1 OCSP/CRL server not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1,<url>
3. HEMSSecGw2OCSPserverFqdnResolutionFailure	When LTE AP is able to resolve FQDN of the HeMS Security Gateway 2 OCSP server.	HeMS Security Gateway 2 OCSP server FQDN cannot be resolved.	LTE AP retries FQDN resolution until reboot timer expires*.	HeMS gateway 2 OCSP/CRL server fqdn resolution failure,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer2,<url>
4. HEMSSecGw2OCSPserverNotReachable	When LTE AP is able to ping HeMS Security Gateway 2 OCSP server successfully.	HEMS Security Gateway 2 OCSP server reachability failure.	LTE AP retries reachability of the HeMS Security Gateway 2 OCSP server until reboot timer expires*.	HeMS gateway 2 OCSP/CRL server not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer2,<url>
5. HEMSSecGw3OCSPserverFqdnResolutionFailure	When LTE AP is able to resolve FQDN of the HeMS Security Gateway 3 OCSP server.	HeMS Security Gateway 3 OCSP server FQDN cannot be resolved.	LTE AP retries to check reachability until reboot timer expires*.	HeMS gateway 3 OCSP/CRL server fqdn resolution failure,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer3,<url>
6. HEMSSecGw3OCSPserverNotReachable	When LTE AP is able to ping the HeMS Security Gateway 3 OCSP server.	HeMS Security Gateway 3 OCSP server reachability failure.	LTE AP retries reachability of the HeMS Security Gateway 3 OCSP server until reboot timer expires*.	HEMS gateway 3 OCSP/CRL server not reachable,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer3,<url>

7. EPCSecGw1OCSPserverFqdnResolutionFailure	When LTE AP is able to resolve FQDN of the EPC Security Gateway 1 OCSP server.	HEMS Security Gateway 3 OCSP server FQDN cannot be resolved.	LTE AP retries to resolve FQDN until reboot timer expires*.	EPC gateway 1 OCSP/CRL server fqdn resolution failure,InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer1,<url>
8. EPCSecGw1OCSPserverNotReachable	When LTE AP is able to ping the EPC Security Gateway 1 OCSP server successfully.	EPC Security Gateway 1 OCSP server reachability failure.	LTE AP retries to check reachability until reboot timer expires*.	EPC gateway 1 OCSP/CRL server server not reachable,InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer2,<url>
9. EPCSecGw2OCSPserverNotReachable	When LTE AP is able to ping the EPC Security Gateway 2 OCSP server successfully.	EPC Security Gateway 21 OCSP server reachability failure.	LTE AP retries to check reachability until reboot timer expires*.	EPC gateway 2 OCSP/CRL server not reachable,InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer1,<url>
10. EPCSecGw3OCSPserverFqdnResolutionFailure	When LTE AP is able to resolve FQDN of the EPC Security Gateway 3 OCSP server successfully.	EPC Security Gateway 3 OCSP server FQDN cannot be resolved.	LTE AP retries FQDN resolution until reboot timer expires*.	EPC gateway 3 OCSP/CRL server fqdn resolution failure,InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer3,<url>
11. EPCSecGw3OCSPserverNotReachable	When LTE AP is able to ping the EPC Security Gateway 3 OCSP server successfully.	EPC Security Gateway 3 OCSP server reachability failure.	LTE AP retries reachability of the Security Gateway 3 OCSP server until reboot timer expires*.	EPC gateway 3 OCSP/CRL server not reachable,InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer2,<url>

NOTE

*LTE AP reboots after reboot timer expiration.

Server Root CA Certificate Missing or Expired Alarm

Alarm Identifier	126
Description	Server Root CA Certificate Missing or Expired: <Additional text>, <Additional Info>
Details	
Additional Information	1. Sent when CA certificate of iHeMS is expired. 2. Sent when CA certificate of iHeMS is missing. 3. Sent when Manufacturer Certificate is expired. 4. Sent when Manufacturer Certificate is missing. 5. Sent when Manufacturer certificate is invalid. 6. Sent when Operator Certificate is expired. 7. Sent when Operator certificate is invalid. 8. Sent when CA certificate of CBRS PKI is missing. 9. Sent when CA certificate of NHN PKI is missing.
Specific Problem	Server Root CA Certificate Missing or Expired.
Perceived Severity	Critical
Action to clear alarm	Replace the missing certificate with a valid one.

Entered Event	Exit Event	Probable Cause	System Action	Additional Text
1. ExpiredCAcertificate	No exit event.	Expired iHeMS CA certificate.	Security module halts until reboot timer expires*.	iHeMS CA Certificate revoked.
2. MissingCAcertificate		Missing iHeMS CA certificate.		iHeMS CA Certificate revoked.
3. ExpiredManufacturerCertificate		Expired Manufacturer certificate.		Manufacturer Certificate is expired.
4. MissingManufacturerCertificate		Missing iHeMS CA certificate.		Manufacturer Certificate missing.
5. InvalidManufacturercertificate		Invalid Manufacturer certificate.		Invalid Manufacturer Certificate.
6. ExpiredOperatorCertificate		Expired Operator certificate.		Operator Certificate is expired.
7. InvalidOperatorcertificate		Invalid Operator certificate.		Invalid Operator Certificate.
8. MissingCAcertificatePkiNhn		Missing NHN PKI CA certificate.		CBRS PKI CA Certificate missing.
9. MissingCAcertificatePkiCbrs		Missing CBRS PKI CA certificate.		NHN PKI CA Certificate missing.

NOTE

*LTE AP reboots after reboot timer expiration.

NTP TOD Sync Failure Alarm

Alarm Identifier	127			
Description	NTP Sync cannot be established - ntpd synchronization is not achieved, NTP synchronization is not achieved.			
Details				
Additional Information	NTP synchronization is not achieved.			
Specific Problem	NTP Sync cannot be established.			
Perceived Severity	Minor			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when NTP_SYNC_FAILURE due to NTP server FQDN resolution failure or IP reachability failure.	Sync is achieved from any Sync Source.	FQDN resolution failure or network reachability issue to NTP server.	No action is required.	ntpd synchronization is not achieved.

RA/CA not reachable Alarm

Alarm Identifier	128
Description	<Specific Problem>, <Additional Text>, <Additional Info>
Details	
Additional Information	1. Sent when Ruckus LTE AP is unable to ping to CMP Server for NHN PKI. 2. Sent when Ruckus LTE AP is unable to resolve fqdn of CMP Server for NHN PKI. 3. Sent when Ruckus LTE AP is unable to ping to CMP Server for CBRS PKI. 4. Sent whenRuckus LTE AP is unable to ping to CMP Server for CBRS PKI.
Specific Problem	1. NHN PKI RA/CA FQDN resolution failure 2. NHN PKI RA/CA not reachable 3. CBRS PKI RA/CA FQDN resolution failure 4. CBRS PKI RA/CA not reachable

Perceived Severity	Major			
Action to clear alarm	1. • Check if DNS server for NHN PKI CMP server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of CMP Server for NHN PKI. 2. CMP Server reachability has been lost / link is down. Check for NHN PKI CMP Server reachability. 3. • Check if DNS server for CBRS PKI CMP Server is configured and is reachable. • If reachable, check if DNS is configured to resolve the FQDN of CMP Server for CBRS PKI. 4. CMP Server reachability is lost or link is down. Check for CBRS PKI CMP Server reachability.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional text**
1. CMPServerFqdnResolutionFailurePkiNhn	When LTE AP is able to resolve FQDN of CMP server for NHN PKI successfully.	NHN PKI CMP server FQDN resolution failure.	LTE AP retries to resolve FQDN until reboot timer expires*.	CMP server fqdn failure for NHN PKI,InternetGatewayDevice.Security.X_001392_PKI.2.CMPServerURL,<url>
2. CMPServerNotReachablePkiNhn	When LTE AP is able to ping to CMP server for NHN PKI successfully.	NHN PKI CMP server reachability failure.	LTE AP retries to check reachability of CMP server until reboot timer expires*.	CMP server not reachable for NHN PKI,InternetGatewayDevice.Security.X_001392_PKI.2.CMPServerURL,<url>.
3. CMPServerFqdnResolutionFailurePkiCbrs	LTE AP is able to resolve FQDN of CMP server for CBRS PKI successfully.	CBRS PKI CMP server FQDN resolution failure.	LTE AP retries to resolve FQDN for CBRS PKI until reboot timer expires*.	CMP server fqdn failure for CBRS PKI,InternetGatewayDevice.Security.X_001392_PKI.3.CMPServerURL,<url>
4. CMPServerNotReachablePkiCbrs	When LTE AP is able to ping the CMP server for CBRS PKI successfully.	CBRS PKI CMP server reachability failure.	LTE AP retries for reachability until reboot timer expires*.	CMP server not reachable for CBRS PKI,InternetGatewayDevice.Security.X_001392_PKI.3.CMPServerURL,<url>.

NOTE

*LTE AP reboots after reboot timer expiration.

Ruckus LTE AP Disconnected from Management Cloud SeGW

Alarm Identifier	129			
Description	RSC disconnected from management cloud SecGW - <Additional text>, <Additional Info>			
Details				
Additional Information	1. Link down for a peer with which HeMS IPSec tunnel is established. 2. Sent when IPSec procedure is failed for all the HEMS SeGW servers.			
Specific Problem	RSC disconnected from management cloud SecGW.			
Perceived Severity	Critical			
Action to clear alarm	1. • HeMS SecGw reachability might have been lost or link with SecGw has been down. Check for SecGw reachability. • If HeMS Security gateway is reachable then check for IPSec-related service running on Hems SecGw. 2. • HeMS SecGw reachability might have been lost or link with SecGw has been down. Check for SecGw reachability. • If HeMS Security gateway is reachable then check for IPSec-related service running on Hems SecGw.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
1. HEMSDpdDetected	IPSec tunnel creation is successful for HeMS Security Gateway 1.	IPSec tunnel creation procedure fail for HeMS Security Gateway 1.	Recovery until reboot.	DPD detected HEMS,<url>

2. IpsecProcedureFailedForHemsSecurityGateway1	When peer recovers from link down.	Link down for a peer with which HeMS tunnel is established.	LTE AP retries for tunnel re-establishment until reboot.	Security HeMS Gateway 1 IPSec proc failed,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1,<url>.

Enrolment Failure Alarm

Alarm Identifier	130			
Description	<Specific Problem>, <Additional text>, <Additional Information>			
Details				
Additional Information	1. Sent when CMP server is Not responding for NHN PKI. 2. Sent when CMP procedure failed for CBRS PKI. 3. Sent when CMP server is Not responding for CBRS PKI. 4. Sent when CMP procedure failed for NHN PKI.			
Specific Problem	1. NHN PKI RA/CA not responding. 2. Enrolment failure for CBRS PKI. 3. CBRS PKI RA/CA not responding. 4. Enrolment failure for NHN PKI.			
Perceived Severity	Major			
Action to clear alarm	1. Check for CMP procedure service running on CMP Server and configured properly. 2. • Check for CMP procedure related service running on CMP Server. • If CMP service is running, check if server is configured correctly to issue certificate in CMP procedure. 3. Check for CMP procedure service running on CMP Server and configured properly. 4. • Check for CMP procedure related service running on CMP Server. • If CMP service is running, check if server is configured correctly to issue certificate in CMP procedure.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
1. CMPServerNotRespondingPkiNhn	When CMP server is responding for NHN PKI successfully.	No response from CMP server for NHN PKI.	LTE AP retries for connection with CMP server until reboot timer expires*.	CMP server not responding for NHN PKI,InternetGatewayDevice.Security.X_001392_PKI.2.CMPServerURL,<url>
2. CMPProcedureFailedPkiNhnway1	When CMP procedure gets successful for NHN PKI.	CMP procedure failed for NHN PKI.	LTE AP retries for procedure complete until reboot timer expires*.	CMP proc failed for CBRS PKI,InternetGatewayDevice.Security.X_001392_PKI.3.CMPServerURL,<url>
3. CMPServerNotRespondingPkiCbrs	When CMP server is responding for CBRS PKI successfully.	No response from CMP server for CBRS PKI.	LTE AP retries for connection with CMP server until reboot timer expires*.	CMP server not responding for CBRS PKI,InternetGatewayDevice.Security.X_001392_PKI.3.CMPServerURL,<url>
4. CMPProcedureFailedPkiCbrs	When CMP procedure get success for CBRS PKI.	CMP procedure failed for CBRS PKI.	LTE AP retries for procedure complete until reboot timer expires*.	CMP proc failed for NHN PKI,InternetGatewayDevice.Security.X_001392_PKI.2.CMPServerURL,<url>

NOTE

*LTE AP reboots after reboot timer expiration.

CBSD Registration Error Alarm

Alarm Identifier	133			
Description	CBSD Registration error - <Additional Text>, SAS-CBSD Procedure Failure.			
Details				
Additional Information	SAS-CBSD Procedure Failure.			
Specific Problem	CBSD Registration error.			
Perceived Severity	Critical			
Action to clear alarm	• Check configuration. • Check additional text. • If required, switch off LTE AP and then switch it on after 10 minutes.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when Registration Procedure fails with SAS, due to an error received from SAS or SAS was not reachable.	Successful registration with SAS.	Configuration or Customization error.	Retry if SAS was not reachable, else wait for user action.	Category Error
				Certificate Error in Registration resp
				SAS Registration Failure error: errorcode
				Failure due to INVALID Registration required data
				Protocol Version not Compatible

CBSD Grant Error Alarm

Alarm Identifier	134			
Description	CBSD Grant Error - <Additional Text>, SAS-CBSD Procedure Failure.			
Details				
Additional Information	SAS-CBSD Procedure Failure.			
Specific Problem	CBSD Grant Error.			
Perceived Severity	Minor			
Action to clear alarm	• Check additional text. • If required, switch off LTE AP and switch on after 10 minutes.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Grant Procedure fails with SAS due to error received from SAS due to incorrect parameters (cbsdId).	Successful acquiring of grant from SAS.	Configuration or Customization error.	Attempt re-registration procedure.	Certificate Error in Grant resp.
Grant Procedure fails with SAS due to requested channel not available.			Attempt grant on different channel/issue spectrum inquiry.	Empty channel received in Spectrum Inquiry response.
SAS was not reachable.			Retry if SAS was not reachable.	SAS Grant Unsuccessfull errorCode.
Protocol version is not compatible.			Attempt with re-registration procedure.	Protocol version not compatible.

CBSD Grant Suspended Alarm

Alarm Identifier	135			
Description	CBSD Grant Suspended, <Additional Text>, SAS-CBSD Procedure Failure.			
Details				
Additional Information	SAS-CBSD Procedure Failure.			
Specific Problem	CBSD Grant Suspended.			
Perceived Severity	Major			
Action to clear alarm	• Check additional text. • If required, switch off LTE AP and switch on after 10 minutes.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when Grant Suspension/ Termination or error received from SAS in Heartbeat procedure.	When SAS-mode is set to direct and SAS changes the Grant state back to transmitting.	Configuration or Customization error.	Attempt re-registration procedure or grant on different channel/ issue spectrum inquiry.	Grant suspended due to Transmit timer expiry.
				Grant revoked due to 500 failure Code in Heartbeat Response from SAS.
				Grant suspended due to transmit timer Expiry.

SAS Certificate Expired Alarm

Alarm Identifier	136		
Description	SAS certificate expired: Certificate Outdated.		
Details			
Additional Information	Certificate outdated.		
Specific Problem	SAS certificate expired.		
Perceived Severity	Critical		
Action to clear alarm	Check SAS account configuration.		
Entered Event	**Exit Event**	**Probable Cause**	**System Action**
Alarm is triggered when Handshake procedure fails with SAS due to certificate expiry.	Successful handshake with SAS.	Configuration or Customization error.	Retry procedure with SAS.

SAS Certificate Invalid Alarm

Alarm Identifier	137		
Description	SAS certificate invalid: Security procedure failure with SAS.		
Details			
Additional Information	Security procedure failure with SAS.		
Specific Problem	SAS certificate invalid.		
Perceived Severity	Critical		
Action to clear alarm	Check SAS account configuration.		
Entered Event	**Exit Event**	**Probable Cause**	**System Action**

Alarm is triggered when an invalid certificate (curl code 60) is installed on LTE AP.	After enrolling with correct PKI.	Configuration image failed to download.	Retry

SAS not Reachable Alarm

Alarm Identifier	138			
Description	SAS is not reachable: <Additional Text>, Connectivity issue with SAS.			
Details				
Additional Information	Connectivity issue with SAS.			
Specific Problem	SAS is not reachable.			
Perceived Severity	Major			
Action to clear alarm	Check SAS account configuration.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
SAS could not be connected.	Successful connection with SAS.	Configuration or customization error.	Retry to connect to SAS.	SAS Not Reachable: Curl Code 45 Received.
FQDN resolution failure for SAS URL.				FQDN Resolution Failed for SAS URL.
When wrong SAS URL is received.				Wrong SAS URL Received.

CBSD Installation Error Alarm

Alarm Identifier	139			
Description	CBSD installation error: CONFIGURATION(SAS MODE) Details Not Available: Invalid-Incomplete configuration provided.			
Details				
Additional Information	Invalid-Incomplete configuration provided.			
Specific Problem	CBSD installation error.			
Perceived Severity	Major			
Action to clear alarm	Check SAS account configuration.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when some mandatory configuration is missing or not valid for LTE AP to perform registration.	Successful registration with SAS.	Configuration or customization error.	No action is required.	CONFIGURATION(SAS MODE) Details Not Available.
				EEPROM data is invalid.
				CBSD SAS ACCOUNT(URL) Details Not Available.
				CONFIGURATION (spectrumToRequest) Not Available.
				Invalid/Missing CBSD Location.

Conclusive CBSD Location Change Detection Alarm

Alarm Identifier	141
Description	CBSD location modified without CPI:CBSD Location Change Detected.
Details	

Additional Information	CBSD Location Change Detected.		
Specific Problem	CBSD location is modified without CPI.		
Perceived Severity	Critical		
Action to clear alarm	Switch off LTE AP and switch it on.		
Entered Event	**Exit Event**	**Probable Cause**	**System Action**
Alarm is triggered when conclusive Location change is detected due to movement of LTE AP.	RegistrationEnable flag toggled.	Configuration or customization error.	Report the alarm.

Probable CBSD Location Change Detection Alarm

Alarm Identifier	142			
Description	CBSD location might be modified without CPI: <Additional Text>: Probable CBSD Location Changed.			
Details				
Additional Information	Probable CBSD Location Changed.			
Specific Problem	LTE AP location is modified without CPI.			
Perceived Severity	Major			
Action to clear alarm	Switch off LTE AP and switch it on.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Alarm is triggered when conclusive Location change is detected due to movement of LTE AP.	RegistrationEnable flag toggled.	Configuration or customization error.	No action is required.	Location Change Detection:GPS/AGPS distance.
				Location Change Detection:CDP/LLDP.
				Location Change Detection:GEO IP

LTE AP Blacklisted

Alarm Identifier	143			
Description	CBSD has been blacklisted by SAS:RSC Blacklisted by SAS.			
Details				
Additional Information	RSC Blacklisted by SAS.			
Specific Problem	LTE AP is blacklisted by SAS.			
Perceived Severity	Major			
Action to clear alarm	Registration Enable toggle.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Response code 101(BLACKLISTED) received from SAS.	Registration Enable toggle followed by successful registration with SAS again.	This responseCode is returned if LTE AP is under a SAS or FCC enforcement action and is barred from CBRS operation. In general, LTE AP should not try to re-register until actions external to this specification are taken.	No system action until operator intervention.	CBSD has been blacklisted by SAS.

LTE OAM Configuration Failure

Alarm Identifier	701			
Description	Critical Configuration Failure - Cell Configuration Failure For Cellid:<i>:Cell configuration failed - OAM configuration failure alarm.			
Details				
Additional Information	OAM configuration failure alarm.			
Specific Problem	Critical configuration failure.			
Perceived Severity	Critical			
Action to clear alarm	Fix OAM configuration accordingly. The operator needs to clear this alarm manually.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Error in OAM configuration.	User intervention is required.	Software error.	Fix the configuration sent to LTE AP. The operator needs to clear this alarm manually. No alarm will be raised for subsequent configuration error unless LTE AP is restarted.	Critical Configuration Failure - Cell Configuration Failure For Cellid: <i>:Cell configuration failed.

NOTE

For <i>, refer the **Naming Convention for Alarms** section.

PCI Confusion Detected

Alarm Identifier	705			
Description	eNodeB detected pci confusion: pciConfusionDetected with PhyCellId=<PCI creating confusion> ,CellIdentity_1=<Cell Id of the first cell creating confusion> ,PLMNID_1=<PLMN Id of the first cell> ,CellIdentity_2=<Cell Id of the second cell creating confusion> ,PLMNID_2=<PLMN Id of the second cell>: Received pci confusion indication from lte			
Details				
Additional Information	Received pci confusion indication from lte.			
Specific Problem	eNodeB detected pci confusion			
Perceived Severity	Major			
Action to clear alarm	Auto clear (currently not supported). Currently, alarm clears on reboot.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
On detecting two neighbors with same PCI and EARFCN in its Neighbor Relation Table.	When PCI re-selection happens.	Received PCI confusion indication from LTE.	Send eNBConfigurationUpdate towards all connected neighbors with neighbor cell's CGI info.	pciConfusionDetected with PhyCellId=<PCI creating confusion> ,CellIdentity_1=<Cell Id of the first cell creating confusion> ,PLMNID_1=<PLMN Id of the first cell> ,CellIdentity_2=<Cell Id of the second cell creating confusion> ,PLMNID_2=<PLMN Id of the second cell>

Colliding PCI Selected

Alarm Identifier	706
Description	No free PCI to use in the provisioned list: Colliding PCI selected;CellConfigIdx:<i>: PCI selection failure alarm, and the cell will continue to operate with a colliding PCI

Details				
Additional Information	PCI selection failure alarm, and the cell will continue to operate with a colliding PCI.			
Specific Problem	No free PCI to use in the provisioned list.			
Perceived Severity	Major			
Action to clear alarm	Re-provision PCI pool with non-colliding PCIs.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
When PCI collision occurs on any cell and colliding PCI is selected for transmission due to scarcity of free PCIs in pool.	On re-configuring PCI pool with non-colliding PCIs.	No free PCI to use in the provisioned list.	Raise PCI selection failure alarm and continue to operate with a colliding PCI.	Colliding PCI selected;CellConfigIdx:<i>

NOTE

For <i>, refer the **Naming Convention for Alarms** section.

IP Allocation Failure

Alarm Identifier	810			
Description	DHCP not provide any lease to RSC: <Additional text>: Sent when RSC fails to acquire IP from DHCP server.			
Details				
Additional Information	Sent when RSC fails to acquire IP from DHCP server.			
Specific Problem	DHCP not provide any lease to RSC.			
Perceived Severity	Major			
Action to clear alarm	Network/DHCP configuration issue needs to be resolved to clear the alarm.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
IP allocation failed on EPC Interface.	LTE AP reboot is required.	IP allocation failed on interface.	LTE AP will reboot on reboot timer expiry.	Failed to allocate IP from DHCP server on EPC interface.
IP allocation failed on PTP Interface.	LTE AP reboot is required.			Failed to allocate IP from DHCP server on PTP interface.
IP allocation failed on MGMT Interface.	LTE AP reboot is required.			Failed to allocate IP from DHCP server on MGMT interface.

NOTE

Default time is 12 minutes.

GPS Lost Alarm

Alarm Identifier	901			
Description	GPS Session could not be established or maintained - Location source is missing or lost, Alarm is triggered when GPS session could not be maintained.			
Details				
Additional Information	Alarm is triggered when GPS session could not be maintained.			
Specific Problem	GPS session could not be established or maintained.			
Perceived Severity	Critical			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**

When a GPS session could not be maintained.	When a GPS session is recovered.	Location source is missing or lost.	No action is required.	Location source is missing or lost.

Disk Usage Exceed Threshold

Alarm Identifier	902			
Description	CPU usage of krait exceeds minor threshold. Default is 85%: FLASH ALARM: Flash usage goes above minor threshold.			
Details				
Additional Information	Flash usage goes above minor threshold.			
Specific Problem	CPU usage of krait exceeds minor threshold. Default is 85%			
Perceived Severity	Warning			
Action to clear alarm	When the disk usage is below minor threshold, the alarm will be cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Disk usage of krait exceeds minor threshold. (Default threshold 85%)	When disk usage is below minor threshold.	Disk usage is above minor threshold.	Raises a warning.	FLASH ALARM

Disk Full

Alarm Identifier	903			
Description	Flash usage exceeds major threshold. Default is 95%: FLASH ALARM: Flash usage goes above major threshold			
Details				
Additional Information	Flash usage goes above major threshold.			
Specific Problem	Flash usage exceeds major threshold. Default is 95%.			
Perceived Severity	Major			
Action to clear alarm	When the disk usage is below major threshold, the alarm is cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Disk usage is above major threshold (Default threshold 95%).	When the disk usage is below major threshold, the alarm is cleared.	Disk usage exceeds major threshold.	Raises an alarm.	FLASH ALARM

Memory Usage Exceed Threshold

Alarm Identifier	904			
Description	RAM usage of krait exceeds minor threshold. Default is 90%: MEMORY ALARM: Memory usage on krait goes above minor threshold.			
Details				
Additional Information	Memory usage on krait goes above minor threshold.			
Specific Problem	RAM usage of krait exceeds minor threshold. Default is 90%.			
Perceived Severity	Warning			
Action to clear alarm	When the memory usage is below minor threshold, the alarm is cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Memory usage on krait is above minor threshold. (Default threshold 90%)	When the memory usage is below minor threshold.	Memory usage of krait exceeds minor threshold.	Raises a warning.	MEMORY ALARM

Memory Full

Alarm Identifier	905			
Description	RAM usage of krait exceeds major threshold. Default is 95%: MEMORY ALARM: Memory usage on krait goes above major threshold.			
Details				
Additional Information	Memory usage on krait goes above major threshold.			
Specific Problem	RAM usage of krait exceeds major threshold. Default is 95%.			
Perceived Severity	Major			
Action to clear alarm	When memory usage is below major threshold, this alarm is cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Memory usage on krait is above major threshold. (Default threshold 95%)	When memory usage is below major threshold.	Memory usage of krait exceeds major threshold.	Raises an alarm.	MEMORY ALARM

CPU Usage Exceed Threshold

Alarm Identifier	906			
Description	CPU usage of krait exceeds minor threshold. Default is 85%: CPU ALARM: CPU usage on krait application processor goes above minor threshold.			
Details				
Additional Information	CPU usage on krait application processor goes above minor threshold.			
Specific Problem	CPU usage of krait exceeds minor threshold. Default is 85%.			
Perceived Severity	Warning			
Action to clear alarm	When CPU usage is below minor threshold, the alarm is cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
CPU usage of krait exceeds minor threshold. (Default threshold 85%)	When CPU usage goes below minor threshold.	CPU usage of krait exceeds minor threshold.	Raises a warning.	CPU ALARM

CPU Overload

Alarm Identifier	907			
Description	CPU usage of krait exceeds major threshold. Default is 95%: CPU ALARM: CPU usage on krait application processor goes above major threshold.			
Details				
Additional Information	CPU usage on krait application processor goes above major threshold.			
Specific Problem	CPU usage of krait exceeds major threshold. Default is 95%.			
Perceived Severity	Major			
Action to clear alarm	When CPU usage is below minor threshold, the alarm is cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
CPU usage on krait application processor goes above major threshold.	When CPU usage is below minor threshold.	Out of CPU cycles.	Raises an alarm.	CPU ALARM

Ethernet Link Down

Alarm Identifier	908			
Description	Ethernet cable unplugged: ETHERNET LINK STATE ALARM: Ethernet link layer goes down event is received from Ethernet device driver available with PFM_BSP.			
Details				
Additional Information	Ethernet link layer goes down event is received from Ethernet device driver available with PFM_BSP.			
Specific Problem	Ethernet cable unplugged.			
Perceived Severity	Major			
Action to clear alarm	When port is enabled on LAN.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Ethernet cable disconnected.	Ethernet cable connected.	Link failure.	None	ETHERNET LINK STATE ALARM

Operating Voltage Exceed Threshold

Alarm Identifier	909			
Description	Operating voltage exceeds threshold: VOLTAGE ALARM: voltage measurement from PMIC is not within threshold value of the operating voltage of the board.			
Details				
Additional Information	Voltage measurement from PMIC is not within threshold value of the operating voltage of the board.			
Specific Problem	Operating voltage exceeds threshold.			
Perceived Severity	Major			
Action to clear alarm	When voltage measurement reaches within threshold value of operating voltage of the board, the alarm is cleared.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
Voltage measurement from PMIC is not within threshold value of the operating voltage of the board.	When voltage measurement reaches within threshold value of operating voltage of the board.	Operating voltage exceeds threshold.	Raises an alarm.	VOLTAGE ALARM

Backhaul Capacity Degraded

Alarm Identifier	910			
Description	Backhaul Capacity Degraded: ETHERNET LINK SPEED ALARM: Ethernet speed falls below the specified threshold.			
Details				
Additional Information	Ethernet speed falls below the specified threshold.			
Specific Problem	Backhaul Capacity Degraded.			
Perceived Severity	Warning			
Action to clear alarm	When Ethernet speed is at par or above the specified threshold.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
When Ethernet speed falls below the specified threshold.	When Ethernet speed is at par or above the specified threshold.	LAN connectivity.	None	ETHERNET LINK SPEED ALARM

LTE AP Startup Failure

Alarm Identifier	912			
Description	System startup Failure due to failure in submodule: <Additional text>; Failure occurring during system startup.			
Details				
Additional Information	Failure occurring during system startup.			
Specific Problem	System startup Failure due to failure in submodule.			
Perceived Severity	Major			
Action to clear alarm	LTE AP reboots.			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
When PTP, NL, GPS synchronization is not achieved.	When PTP, NL, GPS synchronization is achieved.	Server is not reachable.	Raises a critical alarm. LTE AP restart procedure will be triggered.	Synchronization is not achieved.
LTE AP not able to receive IP from DHCP server.	LTE AP receives routable IP from DHCP server.	IP allocation failed on interface.	LTE AP will reboot after 10-15 minutes.	CELL SETUP FAILURE - IP ALLOC TIMER EXPIRED.

Max Secure X2 Connected

Alarm Identifier	913			
Description	Maximum number of secure x2 connections created: 16 secure x2 connections already established: maximum limit for number of secure x2 connections reached.			
Details				
Additional Information	Maximum limit for number of secure x2 connections reached.			
Specific Problem	Maximum number of secure x2 connections created.			
Perceived Severity	Major			
Action to clear alarm	None			
Entered Event	**Exit Event**	**Probable Cause**	**System Action**	**Additional Text**
More than 16 X2 connection have been initiated.	None	Maximum number of secure x2 connections created.	None	16 secure x2 connections already established.

PoE Power Negotiation Failure

Alarm Identifier	914		
Description	Switch not providing adequate power - LLDP Power Negotiation failed with switch.		
Details			
Additional Information	LLDP Power Negotiation failed with switch.		
Specific Problem	Switch not providing adequate power.		
Perceived Severity	Major		
Action to clear alarm	When desired PoE power level is negotiated, the alarm is cleared.		
Entered Event	**Exit Event**	**Probable Cause**	**System Action**
LLDP Power Negotiation fails with switch.	When desired PoE power level is negotiated.	Switch is not providing adequate power.	Raises an alarm.

Ruckus LTE AP Information Events

LTE AP Information Events

The following section provides information about the Information events for Ruckus LTE AP Release SC 3.0.

LTE AP Authentication Successful

Alarm Identifier	501
Description	Event is triggered when Ruckus LTE AP is authenticated with SAS successfully. No certificate is issued during the process.
Default Severity	Information
Entered Event	Event is triggered when Ruckus LTE AP is authenticated with SAS successfully.
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	Successful authentication with SAS.
Specific Problem	LTE AP event

LTE AP Registration Successful

Alarm Identifier	502
Description	Event is triggered when LTE AP is registered with SAS successfully.
Default Severity	Information
Entered Event	Event is triggered when LTE AP is registered with SAS successfully.
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	Successful registration with SAS.
Specific Problem	LTE AP event

LTE AP Grant Successful

Alarm Identifier	503
Description	Event is triggered when LTE AP receives a Grant successfully .
Default Severity	Information
Entered Event	Event is triggered when LTE AP receives a Grant successfully .
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	LTE AP receives a grant successfully.
Specific Problem	LTE AP event

LTE AP Operational Parameter Change

Alarm Identifier	505
Description	Event is triggered when LTE AP receives a Heartbeat response from SAS requesting a change of operating parameters.
Default Severity	Information
Entered Event	Event is triggered when LTE AP receives a Heartbeat response from SAS requesting a change of operating parameters.
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	LTE AP receives a Heartbeat successfully.
Specific Problem	LTE AP event

LTE AP Grant Relinquished

Alarm Identifier	507
Description	Event is triggered when LTE AP relinquishes Grant successfully.
Default Severity	Information
Entered Event	Event is triggered when LTE AP relinquishes Grant successfully.
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	LTE AP relinquishes a Grant successfully.
Specific Problem	LTE AP event

LTE AP Deregistered

Alarm Identifier	508
Description	Event is triggered when LTE AP deregisters with SAS successfully.
Default Severity	Information
Entered Event	Event is triggered when LTE AP deregisters with SAS.
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	LTE AP deregisters successfully.
Specific Problem	LTE AP event

LTE AP successfully downloaded software

Alarm Identifier	918
Description	Software download procedure successful
Default Severity	Information
Entered Event	Event is triggered when software download procedure is successful
Managed Objects	SOM
Event Type	Processing Info event
Probable Cause	Software download successful

Specific Problem	LTE AP event

LTE AP Reboot Reasons

Ruckus LTE AP Reboot Categories and Causes

The following sections provide information on reboot causes under different categories.

Reboot due to LTE AP internal fault

- SEC_CERT_REVOKED
- ROLLBACK
- TX_LO_SYNC_LOSS
- TX_POWER_EXCEED_MAX
- INTERNAL_FAILURE
- SYSTEM_CRASH
- POWER_CYCLE
- RF_CRITICAL_ALARM_RAISED
- SYNCHRONIZATION_NOT_ACHIEVED
- SHEMS_UNREACHABLE
- HOLDOVER_EXPIRY
- PHASE_LOCK_RECOVERY_FAILURE
- DISCONNECT_REBOOT_TIMER_EXPIRED
- EARFCN_MISMATCH
- RF_POWER_MISMATCH

Reboot due to LTE AP sub-system implementation requirement

Data Model

- CRITICAL_CONFIGURATION_RECV ()

Board Management

- CPU_USAGE_MAX_THRESHOLD_REACHED
- MEMORY_USAGE_MAX_THRESHOLD_REACHED

IP Management

- DHCP_LEASE_EXPIRED_FOR_ENTERPRISE_IP

TFCS

- SYNC_SOURCE_CHANGE_FROM_VCTXO

PTP

- PTP_MASTER_RECOVERY

Security

- CERT_KEY_UPDATED
- EPC_TUNNEL_RECOVERY_FAILURE

LTE Stack

- LTE_STACK_IP_CHANGED
- BW_MODIFIED
- MME_IP_CHANGED

Software Download

- SW_DOWNLOAD_REQ_RCVD

Reboot due to SW upgrade

- SOFTWARE_UPGRADE
- SOFTWARE_ACTIVATION
- SOFTWARE_FAILED

Reboot triggered due to Remote user action

- REBOOT_FROM_HEMS
- FACTORY_RESET
- RESTART_FROM_RESET_BUTTON

Reboot triggered due to Local user action

- RESTART_FROM_CLI
- FACTORY_RESET
- RESTART_FROM_RESET_BUTTON

Reboot triggered due to recovery from an external error

- HEMS_TUNNEL_RECOVERY_FAILURE
- HEMS_AND_EPC_VIRTUAL_IP_SAME

COMMSCOPE®
RUCKUS®

Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com