

RUCKUS LTE AP Management User Guide, 20.03

Supporting Release 2020.03 LTE

Copyright, Trademark and Proprietary Rights Information

© 2020 CommScope, Inc. 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 CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope 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, 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, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED 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.....	9
Document Conventions.....	9
Notes, Cautions, and Safety Warnings.....	9
Command Syntax Conventions.....	9
Document Feedback.....	10
RUCKUS Product Documentation Resources.....	10
Online Training Resources.....	10
Contacting RUCKUS Customer Services and Support.....	11
What Support Do I Need?.....	11
Open a Case.....	11
Self-Service Resources.....	11
About This Guide.....	13
About This Document.....	13
What's New in This Document.....	13
Getting Started.....	15
LTE AP Management Overview.....	15
How LTE AP Management Works.....	15
Supported Web Browsers.....	16
Signing Up for Ruckus LTE AP Management	16
Logging in to the Ruckus LTE AP Management Portal.....	17
Navigating the Ruckus LTE AP Management Web Interface.....	17
Getting to Know the Dashboard.....	21
Color-coding of Numbers for Venues, APs, and Clients.....	24
Updating Your Profile.....	25
Changing Your Password.....	25
Resetting Your Password.....	26
Logging Out of the Ruckus LTE AP Management Portal.....	26
Supported AP Models.....	26
Working with Venues.....	27
Venues Overview.....	27
Adding a Venue.....	27
Editing LTE Settings for a Venue.....	29
Adding Macro EARFCN	34
Editing Macro EARFCN.....	37
Configuring SAS Account for a Venue.....	40
Configuring Software Build Version of the AP Model for a Venue	41
Viewing Existing Venues.....	41
Viewing Venue Information.....	42
Viewing Clients Connected to a Venue.....	42
Viewing APs Assigned to a Venue.....	42
Working with Floor Plans.....	43
Viewing Networks Configured for a Venue.....	47
Viewing Events That Have Occurred in a Venue.....	48
Customizing the LTE Setting for a Venue.....	49
Customizing the Wireless Radio Settings.....	50

Editing a Venue.....	51
Deleting a Venue.....	51
Managing Network Devices: APs.....	53
AP Overview.....	53
Adding an AP.....	53
AP Statuses.....	54
Adding ECGI Records.....	54
Adding Certified Professional Installer Details.....	56
Certifying an LTE AP.....	57
Viewing LTE APs.....	59
Viewing ECGI Records.....	60
Viewing CPI Details.....	61
Viewing Wi-Fi APs.....	62
Exporting AP Screen Details.....	63
Filtering APs.....	63
Searching for APs Based on AP Name, MAC Address, IP Address, Model, and Tags.....	63
Displaying APs That Are in Specific Status.....	64
Displaying a Specific AP Model.....	64
Displaying APs Associated With a Specific Tag.....	64
Viewing AP Details.....	64
Viewing Wi-Fi Clients Associated with an AP.....	65
Viewing Networks Configured on an AP.....	67
Viewing Events That Have Occurred on the AP.....	67
Viewing AP Properties.....	68
Editing an LTE AP.....	70
Editing ECGI Records.....	72
Editing Certified Professional Installer Details.....	73
Configuring Bonjour Services (Wi-Fi Only).....	74
Creating or Editing a Bonjour Service.....	75
Enabling or Disabling a Bonjour Service.....	75
Viewing Existing Bonjour Services.....	76
Deleting a Bonjour Service.....	76
Downloading the AP Logs.....	77
Turning AP LEDs ON/OFF.....	78
Blink AP LEDs.....	81
Rebooting an AP.....	82
Resetting an AP to Factory Defaults.....	83
Disabling or Enabling AP Service.....	83
Deleting an AP from Ruckus LTE AP Management.....	84
Managing Wi-Fi Networks.....	87
LTE Networks in Ruckus LTE AP Management.....	87
LTE Network	87
Creating an LTE Network.....	87
Viewing LTE Network (EPC) details.....	92
Editing an LTE Network.....	95
Deleting a Network.....	95
Wi-Fi Networks in Ruckus LTE AP Management.....	96
Creating Networks Overview.....	96
Viewing LTE Clients.....	143

Viewing Associated LTE Clients.....	143
Filtering Associated Clients.....	143
Displaying Clients That Belong to a Particular Venue.....	143
Displaying Clients That Are Associated with a Particular AP.....	143
Managing Wi-Fi Clients and Guests.....	145
Viewing Associated Clients.....	145
Filtering Associated Clients.....	146
Viewing Client Details.....	146
Managing Guests.....	151
Creating a Guest Pass.....	151
Viewing Guest Passes.....	152
Viewing Guest User Details.....	153
Disabling a Guest User.....	156
Generating a New Guest User Password.....	156
Deleting a Guest User.....	157
Monitoring Events.....	159
Event Monitoring Overview.....	159
Event Severity Levels.....	159
Event Types.....	159
Event List.....	160
Viewing Events.....	162
Exporting Events to a CSV File.....	163
Viewing Analytics.....	165
Analytics Overview.....	165
Available LTE Analytics Report.....	165
Statistics Supported in LTE AP.....	165
KPIs Supported in LTE AP.....	167
Accessing LTE KPIs.....	170
Plots.....	171
Available Analytics Reports.....	172
Client Traffic.....	172
Unique Clients.....	172
Number of Sessions.....	172
Session Inventory.....	173
Session Duration.....	173
AP Traffic.....	174
Viewing and Filtering Wi-Fi Analytics Data.....	174
Performing Administrative Tasks.....	177
Performing Administrative Tasks.....	177
Viewing Your Account Details.....	177
Viewing Administrators.....	178
Understanding Administrator Roles.....	179
Adding an Administrator.....	179
Editing or Deleting an Administrator.....	180
Inviting a Ruckus Partner to Manage Your Account.....	180
Configuring Notification Settings.....	181
Adding an Email Address for System Notifications.....	181
Editing, or Deleting an Email Address for System Notifications.....	182

Adding an SMS Address.....	182
Editing or Deleting a Mobile Number.....	182
Using the Support Options on the Web Interface.....	183
Recovery Network Passphrase.....	183
Allow Access to Ruckus Support.....	183
Viewing Your License Information.....	183
Adding a SAS Account.....	184
Editing a SAS Account.....	186
Viewing Your SAS Account.....	188
Deleting a SAS Account.....	189
Enabling or Disabling Access Restriction	191
Sending Feedback.....	191
Reporting an Issue.....	192
Troubleshooting Basic Issues.....	195
Login Issues.....	195
AP Is Unable to Connect to Ruckus LTE AP Management.....	195
Firewall Ports to Open for Ruckus LTE AP Management.....	195
Troubleshooting LTE Issues.....	196
Initial Setup Issues.....	196
Venue Status Check using Alarms.....	198
Collecting LTE AP Logs via LTE AP Management.....	200
Debugging Performance Issues.....	202
AP States in LTE AP Management.....	204
Ruckus LTE Alarms.....	207
Temperature Critical Alarm.....	208
Temperature Warning Alarm.....	208
LTE Radio OpState Disabled Alarm.....	209
RSC at max capacity.....	209
Loss of Sync Sources Alarm.....	209
HoldOver Timeout Alarm.....	210
Dead Peer Detection Alarm.....	210
SCTP Association Failure Alarm.....	211
File Upload Failure Alarm.....	211
Software Activation Failure Alarm.....	211
Configuration Image Download Failure Alarm.....	212
Server Authentication Failure Alarm.....	213
Server Certificate Revoked Alarm.....	216
Server Revocation Check Failure Alarm.....	218
Server Root CA Certificate Missing or Expired Alarm.....	219
OCSP Server not Reachable Alarm.....	220
NTP TOD Sync Failure Alarm.....	222
RA/CA not reachable Alarm.....	223
Ruckus LTE AP Disconnected from Management Cloud SeGW.....	224
Enrolment Failure Alarm.....	224
CBSD Registration Error Alarm.....	225
CBSD Grant Error Alarm.....	226
CBSD Grant Suspended Alarm.....	226
SAS Certificate Expired Alarm.....	227
SAS Certificate Invalid Alarm.....	227

SAS not Reachable Alarm.....	227
CBSD Installation Error Alarm.....	228
Conclusive CBSD Location Change Detection Alarm.....	228
Probable CBSD Location Change Detection Alarm.....	229
RSC Startup Failure Alarm.....	229
tx LO Sync Loss Alarm.....	229
rx LO Sync Loss Alarm.....	230
txPowerExceededMax Alarm.....	230
txPowerOutOfBounds Alarm.....	230
rxDiversity Alarm.....	231
GPS Lost Alarm.....	231
LTE SecGW Alarms.....	232
LTE Controller Alarms.....	232
Configuration Failure Alarm.....	232
Synchronization Error Alarm.....	232
Configuration Pending Alarm.....	233
TDD Configuration Failure Alarm.....	233
LTE RSM Alarms	233
Configuration Failure Alarm.....	233

Preface

- Document Conventions..... 9
- Command Syntax Conventions..... 9
- Document Feedback..... 10
- RUCKUS Product Documentation Resources..... 10
- Online Training Resources..... 10
- Contacting RUCKUS Customer Services and Support..... 11

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	<code>device(config)# interface ethernet 1/1/6</code>
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 .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> 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.

Preface

Document Feedback

Convention	Description
<i>italic text</i>	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, <i>member</i> [<i>member</i> ...].
\	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 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

- [About This Document](#)..... 13
- [What's New in This Document](#)..... 13

About This Document

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

What's New in This Document

TABLE 2 Summary of Enhancements in RUCKUS LTE AP Management Release 2020.03

Features	Description	Location
Macro-eNB	Added an option to select the Cell Type as Home-eNB (default) or Macro-eNB . This feature is available for the Q950-US02.	Adding ECGI Records on page 54 and Editing an LTE AP on page 70.

Getting Started

- LTE AP Management Overview..... 15
- How LTE AP Management Works..... 15
- Supported Web Browsers..... 16
- Signing Up for Ruckus LTE AP Management 16
- Logging in to the Ruckus LTE AP Management Portal..... 17
- Navigating the Ruckus LTE AP Management Web Interface..... 17
- Getting to Know the Dashboard..... 21
- Updating Your Profile..... 25
- Changing Your Password..... 25
- Resetting Your Password..... 26
- Logging Out of the Ruckus LTE AP Management Portal..... 26
- Supported AP Models..... 26

LTE AP Management Overview

LTE AP Management enables you to configure and manage Ruckus LTE APs and their services.

NOTE

Only demo level support for WI-FI AP management is available in this release.

Before you begin using the LTE AP Management, you must have the following items:

- At least one supported Ruckus LTE AP with one valid LTE license
- Internet connection

How LTE AP Management Works

You can power on the Ruckus LTE APs using an AC adapter (included in the box) or a PoE+ switch/injector. Plug an RJ-45 cable with reliable Internet connectivity into the AP. For more information on installation and setup, refer to the *Quick Setup Guide* included in the AP box and also available on Ruckus' support portal.

LTE APs are designed to seek an IP address from an external DHCP server on the LAN where the AP is plugged in. Manual IP configuration is not available for LTE APs.

After obtaining an IP address successfully, an LTE AP sends connection requests to the following services:

1. Ruckus LTE AP Management (EMS)
2. Network—Evolved Packet Core (EPC)
3. Spectrum Allocation Service (SAS)
4. Timing Source (Alternate timing source equipment, GPS or another AP with Timing information—Timing Master AP)

NOTE

IP connectivity to EMS, EPC, SAS and the timing source (PTP timing phase and frequency lock) is a must for an AP to provide LTE service. A disruption to any of these connections may lead to an LTE AP service outage.

Getting Started

Supported Web Browsers

You can configure an AP to complete the following actions:

- Obtain its timing information from the GPS satellites and then assume the role of a Master PTP source for other APs in the network.
- Assume a PTP slave role and obtain its timing information from another AP that is the designated Master (that is reachable by IP address) for that venue.

In the current release, each venue can have up to a maximum of 6 APs configured as the Timing Master source. The network configuration allows up to 32 APs to obtain their timing information (timing slaves) per Master AP. There can also be multiple APs with timing source set as GPS satellites.

For an AP to obtain timing via a GPS signal connection and/or function as a master timing source, place the AP such that it has direct line-of-sight with open sky or as close to the outside facing windows or doors as possible. Certain glass types prevent GPS synchronization despite line-of-sight. Use an external GPS source in such situations. Passive GPS antenna support only for Q710 & Q410 via the sma connector available. Q910 is an outdoor model and it does not have an external antenna connector.

After the timing information is obtained and the LTE AP is connected to EPC Network via S1 connection and has a valid grant from SAS to transmit LTE signal, it provides LTE service to all clients that are using valid SIM cards for this LTE network.

Supported Web Browsers

The Ruckus LTE AP Management Service portal is accessible using a web browser. Before signing up for the Ruckus LTE AP Management Service or logging in to the web interface to manage your networks, make sure that you are using a supported browser.

The following table lists the web browsers that the LTE AP Management Service supports.

TABLE 3 Supported Web Browsers

Browser	Release
Google Chrome	57.0.2987.110 and later
Apple Safari	10.0.3 (12602.4.8) and later
Mozilla Firefox	52.0 and later

Signing Up for Ruckus LTE AP Management

Access to the portal is enabled when at least one license is activated for LTE.

When you purchase Ruckus LTE APs, you have a choice of either purchasing LTE AP management licenses (CLD-RKSC-*) or Private LTE Network services (CLD-NTWK-*), 1-for-1. Each AP requires one license of either type of license to operate.

After the purchase is complete, an email confirming the purchase along with a license activation code is sent to the email provided during the purchase process. Use the same email address to activate the licenses which will prompt you to create a Support account with us (if one is not available already) and use this account to log into:

<https://lte-cloud.ruckuswireless.com>

NOTE

Make sure that the email address provided during the license purchase, is the same exact email used during the license activation/support portal access. Mismatch in emails will stall you from activating licenses.

Logging in to the Ruckus LTE AP Management Portal

The Ruckus LTE AP Management web-based portal is the primary interface to the LTE AP Management. To manage your APs and service settings, you must first log in to the portal.

To log in to the Ruckus Cloud for LTE, follow these steps.

1. Log on to the Ruckus USA-based Cloud portal: <https://lte-cloud.ruckuswireless.com>.

The Ruckus LTE AP Management login page appears. You can access your Ruckus Cloud for LTE and the LTE AP licenses hosted on this portal.

NOTE

To manage Wi-Fi APs, go to <https://cloud.ruckuswireless.com>.

2. In the login box, enter your Ruckus support account email address and password.
3. Click **Log In**.

The page refreshes, and then the Dashboard appears in your web browser.

Navigating the Ruckus LTE AP Management Web Interface

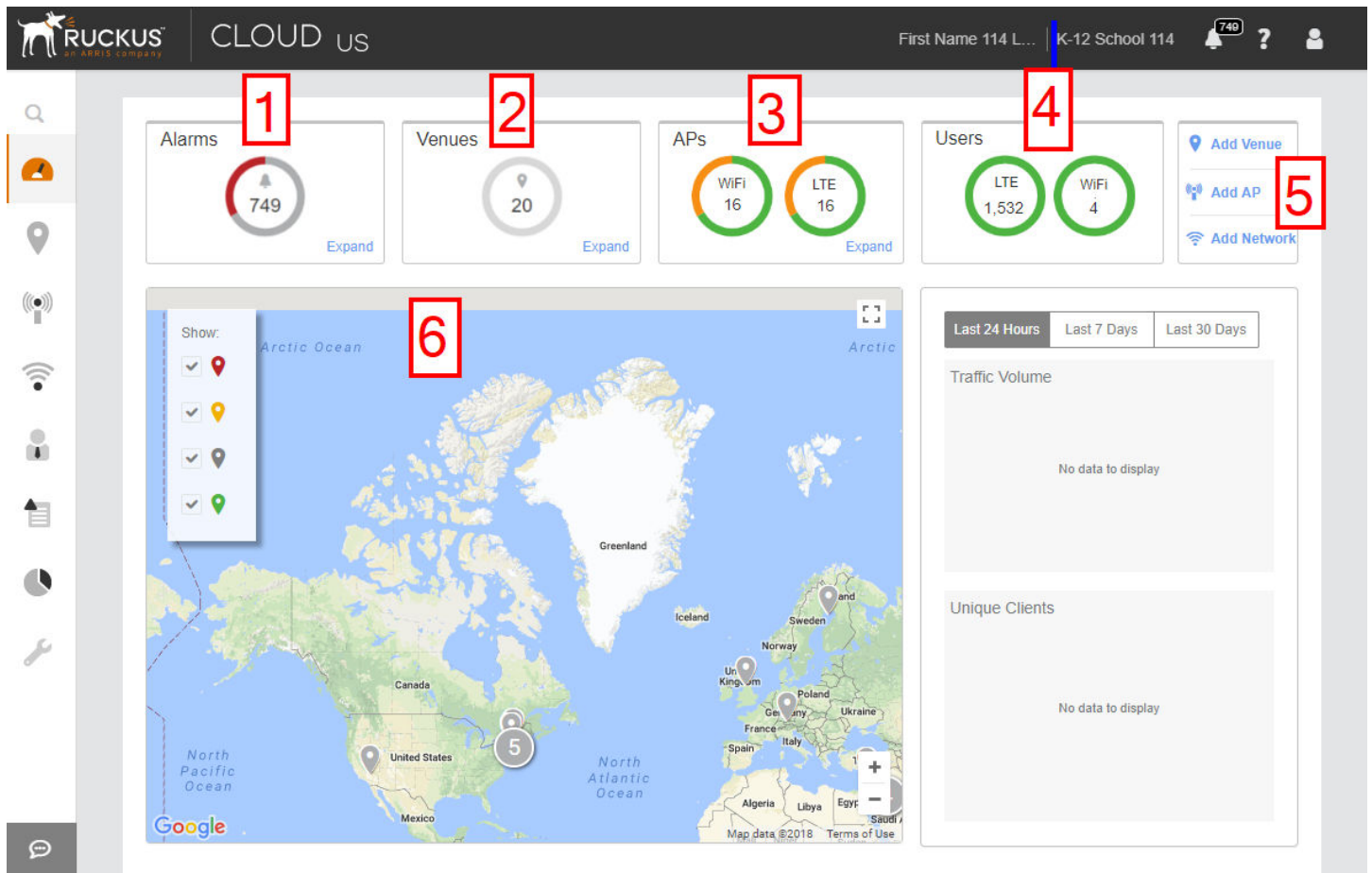
The Ruckus LTE AP Management web interface is a graphical interface for managing your access points, venues, and wireless networks.

After you sign up for a LTE AP Management account, you can access the LTE AP Management web interface from any device (for example, a desktop, laptop, or smart phone) that is connected to the Internet.

Getting Started

Navigating the Ruckus LTE AP Management Web Interface



FIGURE 1 Dashboard: A snapshot of your networks



NOTE

The top banner displays "US" when you are logged in to the US-based LTE AP Management.

TABLE 4 Dashboard elements

Number	Box Name	Description
1	Alarms	<p>Displays the number of uncleared alarms that are generated on your Ruckus LTE networks. When no alarms are generated, the message <code>No Active Alarms</code> appears when you click Alarms. To view details of the uncleared alarms Expand. The following information pertaining to active alarms is displayed.</p> <ul style="list-style-type: none"> • Start Time: Displays when the alarm occurred in the date (MM/DD/YYYY) and time (00:00 hours) format. When you mouse-over, it displays how many days ago the alarm occurred. The latest alarm appears on the top of the column. Click the header to sort this column. • Severity: Displays the severity of the alarms with the severity icons as show in the following image. <p>FIGURE 2 Alarm icons</p>  <p>Click the header of the column to sort it by the alarm type.</p> <ul style="list-style-type: none"> • Description: Displays the alarm ID and the description of the errors or conditions. Click the header of the column to sort it by date. • Source: Displays the source AP. Click the AP name to go to the Overview page and view all the alarms for the AP. The active alarms on the Access Point> Overview page appear as shown the following image. <p>FIGURE 3 Active Alarms</p>  <ul style="list-style-type: none"> – Green indicates that everything is operating normally. – Red indicates that some issues have been found. Click the double-down caret icon at the end of the status message to learn more about the issues. – Yellow indicates that the wireless network service is degraded. Click the double-down caret icon at the end of the status message to learn more about the issue or issues causing the degradation. <ul style="list-style-type: none"> • Identifier: Displays the MAC address of the AP. • To clear an alarm from the summary table, click the Clear Alarm check box. • Click Export to CSV to export information pertaining to all the active alarms to a CSV file. • Click Clear All to clear all active alarms. <p>Alternatively, click the bell icon on the top-right corner to view alarm details. A resizable pop-up window appears displaying the alarm details. Click the bottom-left corner of the Alarms window to resize it.</p>
2	Venues	<p>Displays the number of venues that have been configured in your LTE AP Management account.</p> <ul style="list-style-type: none"> • To view a summary of the venues, including their locations, number of networks, number of APs, and number of active wireless clients, click Expand in the bottom-right corner of the Venues box. • To view or edit the settings of a venue, click the venue name in the summary table. • To view the Venues page, click Venues.

Getting Started

Navigating the Ruckus LTE AP Management Web Interface

TABLE 4 Dashboard elements (continued)




Number	Box Name	Description
3	APs	<p>Displays the number of LTE and Wi-Fi APs in separate widgets (circle marks) that have been added to the LTE AP Management account. If there are no Wi-Fi and LTE APs, the values are displayed as "0", circled in gray. If there are APs, the respective values are circled in green.</p> <ul style="list-style-type: none"> To view a summary of the APs, including their names, statuses, models, IP addresses, serial numbers, MAC addresses, venues in which they are deployed, mesh roles, number of active clients, click Expand in the bottom-right corner of the APs box. To view the APs page with LTE as the default tab, click APs. To view the APs page with the WiFi tab as the default, click WiFi.
4	Clients	<p>Displays the number of LTE and Wi-Fi clients that are currently connected to managed APs, inside a widget (circle mark). If there are no Wi-Fi and LTE clients, the value is displayed as "0", circled in gray. If there are users, the respective values are circled in green.</p> <p>Clicking the Clients link displays the Users page with LTE as the default tab and the LTE user details are displayed. If one of the previous conditions exist, the Wi-Fi widget is displayed along side the LTE widget. To view the Users page with the WiFi tab as the default, click WiFi.</p> <p>In the grid that displays the client details, primary sorting is based on the number of clients in a venue and secondary sorting is based on the number clients in an AP. The venue with the highest number of clients appears in the top most row and proceeds in descending order. Clicking the row displays the relevant venue or AP.</p> <p>NOTE Unlike WiFi, the LTE tab displays only the number of currently connected clients, per venue.</p>
5	Essential shortcuts	<p>Displays shortcuts for the following basic tasks:</p> <ul style="list-style-type: none"> Add Venue: Click to open the screen for adding a venue, and then follow the instructions in Adding a Venue on page 27. Add AP: Click to open the screen for adding an AP, and then follow the instructions in Adding an AP on page 53. Add Network: Click to open the screen for adding a network, and then follow the instructions in Creating an LTE Network on page 87.
6	Map	Displays venue location markers within the Google map.

The following table describes the web interface elements of the Ruckus LTE AP Management.

TABLE 5 Web interface Elements

Name	Description
Search box	Enter a keyword or phrase to search for matches in venues, APs, and networks.
Navigation pane	<p>Use the navigation pane to navigate through the main pages of the portal, which include:</p> <ul style="list-style-type: none"> Dashboard Venues APs Networks Users Events Analytics Administration
Content area	When you click an item on the navigation pane, the related information (tables, lists, configuration options and so on) appear in the content area.
User information	Displays your first and last name as recorded in your Ruckus account profile.

TABLE 5 Web ilterface Elements (continued)

Name	Description
 (the Alarm indicator)	Click to view the alarms that have occurred on the controller and managed APs. If a number appears above the icon, it indicates the number of new alarms that have occurred.
 (Help)	Click to view a submenu that contains links to the online help <ul style="list-style-type: none"> • Documentation: Click to view the complete online help. • How-To videos: Click to view training videos on YouTube. • Help for this page: Click this link to view context-sensitive help. • Contact support: Click this link to go to Ruckus support contact page, if you have a problem or want to ask a question. • Open a case: Click this link to open a case. • My open cases: Click this link to view your open cases and their status. • Privacy:Click this link to view the Ruckus Cloud privacy policy. • About Ruckus Cloud: Click this link to view the running version of Ruckus Cloud software.
 (Account)	Click to view links for managing your account. <ul style="list-style-type: none"> • Updating Your Profile on page 25: Click to edit the format of the date and event details level that are configured for your account. • Changing Your Password on page 25: Click to edit your Ruckus profile password. • Logging Out of the Ruckus LTE AP Management Portal on page 26: Click to log out of the web interface.

Getting to Know the Dashboard

The Dashboard is the first page that appears after you log in to the Ruckus LTE AP Management portal. The Dashboard displays both LTE and WiFi alarms, venues, APs, and users.

NOTE



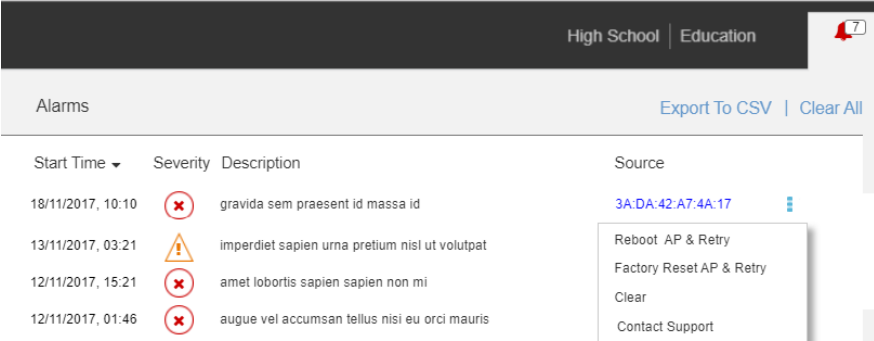
LTE AP support is available only on the US-based LTE AP Management version. This is different from the US-based Ruckus Cloud Wi-Fi.

Getting Started

Getting to Know the Dashboard

The Wi-Fi clients widgets (circle marks) appears on the **Dashboard** only when there is a Wi-Fi configuration and/or a Wi-Fi license purchased.

TABLE 6 Dashboard Elements

Number	Box Name	Description
1	Alarms	<p>Displays the number of uncleared alarms that are generated on your Ruckus LTE networks. When no alarms are generated, the message <code>No Active Alarms</code> appears when you click Alarms. To view details of the uncleared alarms Expand. The following information pertaining to active alarms is displayed.</p> <ul style="list-style-type: none"> • Start Time: Displays when the alarm occurred in the date (MM/DD/YYYY) and time (00:00 hours) format. When you mouse-over, it displays how many days ago the alarm occurred. The latest alarm appears on the top of the column. Click the header to sort this column. • Severity: Displays the severity of the alarms with the severity icons as shown in the following image. <p>FIGURE 4 Alarm Icons</p>  <ul style="list-style-type: none"> • Click the header of the column to sort it by the alarm type. • Description: Displays the alarm ID and the description of the errors or conditions. Click the header of the column to sort it by date. • Source: Displays the source AP if you have a valid license. Click the AP name to go to the Overview page and view all the alarms for the AP. The active alarms on the Access Point-> Overview page appear as shown the following image. <p>FIGURE 5 Active Alarms</p>  <ul style="list-style-type: none"> – Green indicates that everything is operating normally. – Red indicates that some issues have been found. Click the double-down caret icon at the end of the status message to learn more about the issues. – Yellow indicates that the wireless network service is degraded. Click the double-down caret icon at the end of the status message to learn more about the issue or issues causing the degradation. <ul style="list-style-type: none"> • Identifier: Displays the MAC address of the AP. • To clear an alarm from the summary table, click the Clear Alarm check box. • Click Export to CSV to export information pertaining to all the active alarms to a .csv file. • Click Clear All to clear all active alarms. <p>For the alarms pertaining to failed tasks display action overflow menu (three vertical dots) icon.</p> <p>FIGURE 6 Alarms with Actions Menu</p> 

When clicked on the action menu, the following options are displayed.

TABLE 6 Dashboard Elements (continued)

Number	Box Name	Description
2	Venues	<p>Displays the number of venues that have been configured in your LTE AP Management account.</p> <ul style="list-style-type: none"> To view a summary of the venues, including their locations, number of networks, number of APs, and number of active wireless clients, click Expand in the bottom-right corner of the Venues box. To view or edit the settings of a venue, click the venue name in the summary table. To view the Venues page, click Venues.
3	APs	<p>Displays the number of LTE and Wi-Fi APs in separate widgets (circle marks) that have been added to the LTE AP Management account. If there are no Wi-Fi and LTE APs, the values are displayed as "0", circled in gray. If there are APs, the respective values are circled in green.</p> <ul style="list-style-type: none"> To view a summary of the APs, including their names, statuses, models, IP addresses, serial numbers, MAC addresses, venues in which they are deployed, mesh roles, number of active clients, click Expand in the bottom-right corner of the APs box. To view the APs page with LTE as the default tab, click APs. To view the APs page with the WiFi tab as the default, click WiFi.
4	Clients	<p>Displays the number of LTE and Wi-Fi clients that are currently connected to managed APs, inside a widget (circle mark). If there are no Wi-Fi and LTE clients, the value is displayed as "0", circled in gray. If there are users, the respective values are circled in green.</p> <p>Clicking the Clients link displays the Users page with LTE as the default tab and the LTE user details are displayed. If one of the previous conditions exist, the WiFi widget is displayed along side the LTE widget. To view the Users page with the WiFi tab as the default, click WiFi.</p> <p>In the grid that displays the client details, primary sorting is based on the number of clients in a venue and secondary sorting is based on the number clients in an AP. The venue with the highest number of clients appears in the top most row and proceeds in descending order. Clicking the row displays the relevant venue or AP.</p> <p>NOTE Unlike WiFi, the LTE tab displays only the number of currently connected clients, per venue.</p>
5	Essential shortcuts	<p>Displays shortcuts for the following basic tasks:</p> <ul style="list-style-type: none"> Add Venue: Click to open the screen for adding a venue, and then follow the instructions in Adding a Venue on page 27. Add AP: Click to open the screen for adding an AP, and then follow the instructions in Adding an AP on page 53. Add Network: Click to open the screen for adding a network, and then follow the instructions in Creating an LTE Network on page 87.
6	Map	Displays venue location markers within the Google map.

NOTE

References to the name of an object managed by the Ruckus LTE AP Management portal (Venue, AP, Network, Client) display in blue to represent a link to the detail page of the object. For example, the MAC address under the Alarms on the Dashboard links to the AP details page.

Color-coding of Numbers for Venues, APs, and Clients

The segmented color lines around the numbers of venues, APs and clients indicate the statuses of the venues and APs.

- Green: Operating normally
- Red: Requires attention
- Grey: Remains in setup mode

Updating Your Profile

Update your profile if you need to change your time zone or event detail level.

NOTE

You cannot edit your name, email address, and role on the Ruckus LTE AP Management Service portal. To edit your name and email address, edit your profile on the Ruckus Wireless Support website.

Follow these steps to update your profile.

1. On the miscellaneous bar (located in the upper-right corner of the web interface), click  .

A submenu appears.

NOTE


You cannot change your name, email address, and role here.

2. Click **My Profile**.
The **My Profile** screen appears.
3. Edit any of the following profile settings:
 - **Date Format**: Select a desired date format.
 - **Event Details Level**: Select the level of detail that you want the LTE AP Management Service to display for events on the **Events** page.
4. Click **Save**.

You have completed updating your profile.

Changing Your Password

To change your Ruckus LTE AP Management Service password, edit your Ruckus Cloud profile.

1. On the miscellaneous bar (located in the upper-right corner of the web interface), click  .

A submenu appears.

2. Click **Change password**.
The **Editing Your Profile** page on the Ruckus Cloud Support website appears.
3. In **Password**, type in your new password.
4. In **Confirm Password**, retype the password you entered in the previous step.

The page refreshes as your Ruckus Cloud profile password is updated. When the password is updated successfully, the following message appears:

Your profile was successfully updated.

You have completed updating your Ruckus LTE AP Management Service password.

Resetting Your Password

If you forget password, you can reset it from the Ruckus LTE AP Management Service portal log in page.


1. Log on to <https://lte-cloud.ruckuswireless.com>.
The sign-in page appears.
2. Click the `Forgot password?` link below the sign-in form.
The **Resetting Your Password** page on the Ruckus Wireless Support website appears.
3. In **Email**, enter the email address that you used to sign up for an LTE AP Management Service tenant account.
4. Click **Reset Password**.
5. Check your email inbox for a message from Ruckus Wireless Support that explains how to reset your password.
6. Follow the instructions in the email message.

You have completed resetting your password.

Logging Out of the Ruckus LTE AP Management Portal

When the Ruckus LTE AP Management portal does not detect any activity from you within 30 minutes, it will automatically log you out. You can also manually log out of the portal.

Follow these steps to log out of the LTE AP Management portal.

1. In the upper-right corner of the page, click  .
2. Click **Log out**.

The page refreshes, and then the log on form appears, which indicates that you have successfully logged off.

Supported AP Models

Ruckus LTE AP Management supports the following APs:

- Q710-US02
- Q910-US02
- Q410-US01
- Q950-US02

NOTE

Older SKUs Q710-US00 and Q910-US00 are also supported.

This platform is designed for Ruckus LTE AP Management. Wi-Fi AP support is demo level only.

Working with Venues

- Venues Overview..... 27
- Adding a Venue..... 27
- Editing LTE Settings for a Venue..... 29
- Adding Macro EARFCN 34
- Editing Macro EARFCN..... 37
- Configuring SAS Account for a Venue..... 40
- Configuring Software Build Version of the AP Model for a Venue 41
- Viewing Existing Venues..... 41
- Viewing Venue Information..... 42
- Editing a Venue..... 51
- Deleting a Venue..... 51

Venues Overview

Venues are the primary resource managed by LTE AP Management. A venue represents a physical space where an access point (AP) is deployed. Venues can vary in size from a small room to a large multi-floor building.

While each venue may have multiple APs, each AP can belong to only one venue.

Adding a Venue

You must add a venue before you can connect your APs to the AP Management Service to provision the LTE service. By default, a sample venue named My Venue exists. If you want to assign your APs to a venue other than the default, you can add a new venue.

Follow these steps to add a venue.

1. On the Dashboard, click **Venues**.
The **Venues** page appears.

Working with Venues

Adding a Venue

2. In the upper-right corner of the page, click **Add Venue**.

The **Create New Venue** dialog box appears.

Create New Venue ? X

* Venue name:

Description:

* Address: *Make sure to include a city and country in the address*

Cupertino, California, US

Apple Park visitor Center

Cupertino

Stevens Creek Blvd

Google

Map data ©2020 Terms of Use Report a map error

☉ Pacific Daylight Time [UTC -07:00]

Address Notes:

Venue LTE Settings

LTE DHCP Allocation: IPv4 IPv6 ?

Go to floor plans to add a floor plan Cancel Create

3. In the **Venue name** field (required), type a name for the venue that you are creating.
4. In the **Description** field, type a brief description of the venue.
5. In the **Address** field (required), type the address where the venue is located.
You can enter either a full or partial address. For example, if you type 350 W Java Dr, Google displays the location that matches the address. Select the correct address.
6. In **Address Notes**, add notes or comments about this venue. For example, you can add the floor number or suite number.
7. Under the **Venue LTE Settings** section, select either **IPv4** or **IPv6** for **LTE DHCP Allocation** .
A venue can work with either with IPv4 or IPv6 DHCP allocation. After the venue is created, the DHCP allocation cannot be changed.

- (Optional) Select the **Go to floor plan to add a floor plan** check box to create a floor plan.
- Click **Create**.

The message `Creating venue...` appears as the AP Management Service creates the venue in your account. The **Add New Floor Plan** dialog box appears. Make sure that the **Go to floor plan to add a floor plan** check box is selected.

- Enter a name for the floor plan in the **Floor Plan Name** text field.
- Enter the floor number or click the Up or Down arrow and select the floor **floor number** text field. The "0" (zero) represents a ground floor.
- Click the **Upload** button to upload a floor plan image.
- To calibrate the floor plan to a map, select the **Next, calibrate the floor plan to a map** check box and click the **Add** button. The system displays `Creating floor plan..` and then the `Uploading image...` Next, the **Floor Plan Calibration** dialog box prompts you to calibrate the floor plan image to a map.

NOTE

Calibrating the floor plan allows you to properly geo-position the APs which is mandatory for AP-SAS interaction. To perform calibration, click and position the two pins on corresponding features on the floor plan and on the map.

- After the calibration, click the **Save** button.

System displays `Updating floorplan...` The newly added venue appears in with the calibrated floor plan.

- Verify that the name of the venue you have created appears on the venue list.

You have completed creating a venue.

NOTE

Click the pencil icon if you want to edit the venue. Click the globe icon to recalibrate the floor plan.

Editing LTE Settings for a Venue

Using RUCKUS LTE AP Management, you can configure a venue profile with advanced LTE settings for optimal resource management.

Follow these steps to configure a venue profile.

- On the Dashboard, click **Venues**.
The **Venues** page appears displaying the existing venues.
- Select a venue to configure advance settings.
The **Venue Overview** page appears.

3. Locate **LTE Settings** under **Venue Settings** and click **Edit**.

The **Venue LTE Settings** dialog box appears.

FIGURE 7 Venue LTE Settings

Venue LTE Settings [?] [X]

General | SAS Account | AP Models' Build

Timing Masters: [Manage](#)
No timing masters are defined for this venue

Management VLAN:

PTP VLAN:

Venue Type Properties

Venue Type:

TDD Configuration: [?]

Add Macro EARFCN

Macro EARFCN:

Ruckus Private LTE Network Service Access Restriction OFF [?]

AP LEDs ON

DHCP Allocation: [?]

Cancel Save

4. To configure Timing Masters, click **Manage**.

The **Manage Timing Masters** dialog box appears. By default, the APs tab opens.

NOTE

You can configure up to 6 APs or external device as the Timing Master for a venue.

Use these instructions to configure Timing Masters:

- Select up to 6 APs to configure them as Timing Masters.
 - To locate an AP, enter the name of the AP in the **Search box** and click the magnifying glass icon to run a search.
- Click **Save** to configure the APs as Timing Masters.

The LTE settings are updated.

- Click the **External Devices** tab, select up to 6 external devices and click **Save** to configure them as Timing Masters.
 - To add an external device, click **Add Device**. The **Add Device** dialog box appears. Enter the IPv4 address of the external device in the **Timing Master Device IP** field and click **OK**.

NOTE

The valid Timing Master format namely IPv4 or IPv6 is derived from the DHCP allocation that was defined for the venue.

- Click **Edit** to change the IP address of an external device.
- Click **Remove** to remove an external device.

5. (Optional) Enter the VLAN ID of the **Management VLAN**.

Supported VLAN ID value is from 1 through 4094.

6. (Optional) Enter the VLAN ID of the **Timing VLAN**.

Supported VLAN ID value is from 1 through 4094.

7. From the drop-down list, select a **Venue Type**.

You can choose one of these venue types:

- Dense (~ AP spacing \leq 8,000 sq. ft.)
- Moderate (8000 sq. ft. $<$ ~ AP spacing $<$ 20,000 sq. ft.) (Default)
- Sparse (~AP spacing \geq 20,000 sq. ft.)

NOTE

A reboot of certain LTE APs in the venue is required when you change the venue type.

8. From the drop-down list, select a **TTD Configuration**.

You can choose one of these TTD configurations:

- Configuration 1 (Default)
- Configuration 2 (for better downlink performance)
- Configuration 6 (for better uplink performance)

The default is TDD configuration 1. The TDD configuration 2 and 6 configure the APs to have a better downlink and uplink performance.

NOTE

Changing the TDD Configuration may require a reboot of some LTE APs in the venue.

9. The **Macro EARFCN** section shows information on **Carrier**, **Cell Individual Offset**, and **EARFCN Bandwidth**. By default, Macro EARFCN is disabled.

You can choose the following actions:

- Click **Add Macro EARFCN** to add enable specific Macro. Specify the following fields and then click **OK**

FIGURE 8 Add Macro EARFCN

- **Carrier**: Specify a unique and valid range from 0 through 262143.
- **Cell Individual Offset**: Specify a valid range from -1 to -24 or from 0 through 20.
- **EARFCN Bandwidth**: Enter one of these: BW6, BW15, BW25, BW50, BW75, or BW100

- Click the pencil icon to edit the Macro EARFCN. Edit the required parameters and then click **OK**.
- Click the delete icon to remove the Macro EARFCN. Enter **Delete** to confirm deletion of the Macro EARFCN when prompted.

10. Toggle the **IPv6 DHCP allocation** to **ON** or **OFF**.

If enabled, the DHCP server can allocate a local IPv6 address to APs for a specific venue. This is necessary when an enterprise has only IPv6 for LAN and it cannot allocate an IPv4 address to the APs.

11. Toggle the **Ruckus Private LTE Network Service Access Restriction** to **ON** or **OFF**.

This feature can be enabled from **Administration -->Access Restriction**. By default, this feature is disabled.

- If the toggle is set to **OFF**, this option is greyed out and cannot be enabled from the **Venue LTE Settings** dialog box.
- If this feature is enabled (**ON**) at the admin level, you can turn it to **OFF/ON** while editing the LTE settings.

12. Toggle the **AP LEDs** to **ON** or **OFF**.

13. Click **Save**.

The system displays `Updating LTE Settings....`

Configuring SAS Account for a Venue

Beginning with the Ruckus LTE Release 20.01, you can configure SAS accounts for each venue. For each tenant, the SAS account is defined in the **Administrator** section. SAS accounts will appear in the drop-down in the Venue LTE Settings only if they were added by you earlier. For information on how to add a SAS account, refer to [Adding a SAS Account](#) on page 184.

Follow these steps to configure a SAS account for a venue.

14. In the **Venue LTE Settings** dialog box, select the **SAS Account** tab.

You can configure a custom venue SAS account or use the default SAS account for the selected venue.

FIGURE 9 Editing a SAS Account

The screenshot shows the 'Venue LTE Settings' dialog box with the 'SAS Account' tab selected. The dialog has three tabs: 'General', 'SAS Account', and 'AP Models' Build'. The 'SAS Account' tab is active and contains the following fields:

- Custom venue SAS account:** A radio button is selected, and a blue link 'Use default SAS account' is visible to its right.
- SAS Account:** A dropdown menu showing 'FW_adi'.
- Provider:** A text field containing 'FEDERATED'.
- URL:** A text field containing 'https://developer-sc-02.federatedwireless.com:443'.
- Version:** A text field containing 'v1.2'.
- CBSD User ID:** A text field containing 'e54tvert5g&^U76u'.

At the bottom of the dialog, there is a legend for '* Required field', a 'Cancel' button, and a 'Save' button.

15. To configure a customer venue SAS account, select an account from the **SAS Account** drop-down.
16. (Optional) Click the **Use Default SAS account** to configure the default SAS account to the venue.
17. Review the selected SAS account details and click **Save**.

The **Updating LTE Settings** progress bar appears.

Configuring Software Build Version of the AP Model for a Venue

Follow these steps to configure the software build version of each APs for a venue.

18. In the **Venue LTE Settings** dialog box, Select the **AP Models' Build** tab.

The screenshot shows the 'Venue LTE Settings' dialog box with the 'AP Models' Build' tab selected. The dialog has three tabs: 'General', 'SAS Account', and 'AP Models' Build'. Below the tabs, there is a section titled 'Select build version per AP model' containing a table with columns for 'AP Model', 'Build', and 'Description'. The table lists four AP models: Q710, Q910, Q410, and Q950. Each model has a dropdown menu set to 'Default official build' and a description of 'Default official build'. At the bottom of the dialog, there is a legend for '* Required field', a 'Cancel' button, and a 'Save' button.

AP Model	Build	Description
Q710	Default official build	Default official build
Q910	Default official build	Default official build
Q410	Default official build	Default official build
Q950	Default official build	Default official build

19. Select the desired software build for each AP models.
20. Click **Save**.

You have completed configuring a venue profile.

Adding Macro EARFCN

Follow these steps to add Macro EARFCN (E-UTRA Absolute Radio Frequency Channel Number).

1. On the Dashboard, click **Venues**.
The **Venues** page appears displaying the existing venues, if any.
2. Select the venue to configure advance settings.
The **Venue Overview** page appears.

3. Locate **LTE Settings** under **Venue Settings** and click **Edit**.

The **LTE Settings** dialog box appears.

FIGURE 10 Venue LTE Settings

Venue LTE Settings [?] [X]

General | SAS Account | AP Models' Build

Manage

Timing Masters: No timing masters are defined for this venue

Management VLAN: *VLAN ID can be a value between 1 to 4094*

PTP VLAN: *VLAN ID can be a value between 1 to 4094*

Venue Type Properties

Venue Type: Moderate (8000 sq. ft. < ~ AP spacing < 20,000 sq. ft.)

TDD Configuration: Configuration 1 (Default) [?]

Add Macro EARFCN

Macro EARFCN: No Macro EARFCN defined

Ruckus Private LTE Network Service Access Restriction OFF [?]

AP LEDs ON

DHCP Allocation: IPv6 [?]

Cancel Save

4. In the **Macro EARFCN** section, click **Add Macro EARFCN**.

You can add up to 8 Macro EARFCNs. After adding 8 Macro EARFCN, the add option is disabled.

The **Add Macro EARFCN** dialog box appears.

FIGURE 11 Adding Macro EARFCN

The screenshot shows a dialog box titled "Add Macro EARFCN" with a close button (X) in the top right corner. The dialog contains three required fields, each marked with a yellow star:

- Carrier:** A text input field with the subtext "Range between 0 to 262143".
- Cell Individual Offset:** A dropdown menu.
- EARFCN Bandwidth:** A dropdown menu.

At the bottom of the dialog, there is a grey bar containing a yellow star icon followed by the text "* Required field", a blue "Cancel" button, and a grey "OK" button.

5. Enter the following parameters.

- – **Carrier:** Enter a unique and a valid number. The range from 0 through 262143.
- **Cell Individual Offset:** Enter a valid number. The range from -1 to -24 or from 0 through 20.
- **EARFCN Bandwidth:** Enter one of these: BW6, BW15, BW25, BW50, BW75, or BW100

6. Click **OK**.

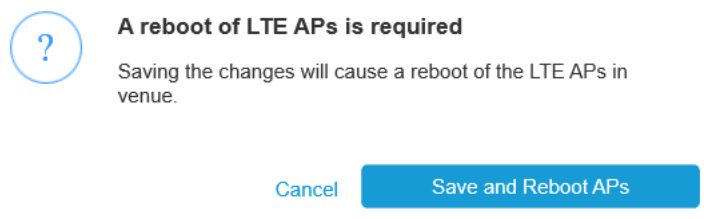
NOTE

Changing Macro EARFCN will require a reboot of LTE APs in venue.

7. Click **Save**.

The Macro EARFCN configuration is saved and the LTEs APs in the venue are rebooted.

FIGURE 12 Saving and Rebooting LTE APs



Editing Macro EARFCN

Follow these steps to edit Macro EARFCN (E-UTRA Absolute Radio Frequency Channel Number).

1. On the Dashboard, click **Venues**.
The **Venues** page appears displaying the existing venues, if any.
2. Select the venue to configure advance settings.
The **Venue Overview** page appears.

3. Locate **LTE Settings** under **Venue Settings** and click **Edit**.

The **LTE Settings** dialog box appears.

FIGURE 13 Venue LTE Settings

Venue LTE Settings [?] [X]

General | SAS Account | AP Models' Build

Timing Masters: Manage
No timing masters are defined for this venue

Management VLAN:

PTP VLAN:

Venue Type Properties

Venue Type:

TDD Configuration: [?]

Add Macro EARFCN

Macro EARFCN:

Ruckus Private LTE Network Service Access Restriction OFF [?]

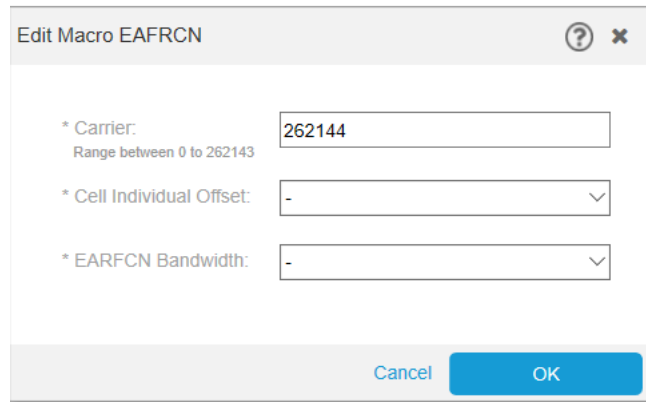
AP LEDs ON

DHCP Allocation: [?]

Cancel Save

- In the **Macro EARFCN** section, click the pencil icon to edit the Macro EARFCN configuration.
The **Editing Macro EARFCN** dialog box appears.

FIGURE 14 Editing Macro EARFCN



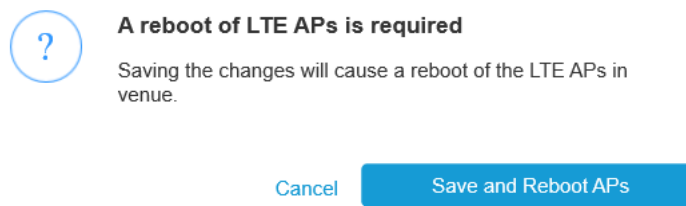
- You can edit the following parameters.
 - **Carrier:** Enter a unique and a valid number. The range from 0 through 262143.
 - **Cell Individual Offset:** Enter a valid number. The range from -1 to -24 or from 0 through 20.
 - **EARFCN Bandwidth:** Enter one of these: BW6, BW15, BW25, BW50, BW75, or BW100
- Click **OK**.

NOTE

Changing Macro EARFCN will require a reboot of LTE APs in venue.

- Click **Save**.
The Macro EARFCN configuration is saved and the LTEs APs in the venue are rebooted.

FIGURE 15 Saving and Rebooting LTE APs



- (Optional) Click the delete icon to delete the Macro EARFCN configuration.

Configuring SAS Account for a Venue

Beginning with the Ruckus LTE Release 20.01, you can configure SAS accounts for each venue. For each tenant, the SAS account is defined in the **Administrator** section. SAS accounts will appear in the drop-down in the Venue LTE Settings only if they were added by you earlier. For information on how to add a SAS account, refer to [Adding a SAS Account](#) on page 184.

Follow these steps to configure a SAS account for a venue.

1. On the Dashboard, click **Venues**.

The **Venues** page appears displaying the existing venues.

2. Select the venue to configure the SAS account.

The **Venue Overview** page appears.

3. Locate **LTE Settings** on the right-bottom corner and click **Edit**.

The **Venue LTE Settings** dialog appears.

4. Select the **SAS Account** tab.

You can configure a custom venue SAS account or use the default SAS account for the selected venue.

Venue LTE Settings

General **SAS Account** AP Models' Build

Custom venue SAS account [Use default SAS account](#)

SAS Account: FW_adi

Provider: FEDERATED

URL: https://developer-sc-02.federatedwireless.com:443

Version: v1.2

CBSD User ID: e54tvert5g&^U76u

* Required field Cancel Save

5. To configure a customer venue SAS account, select an account from the **SAS Account** drop-down.
6. (Optional) Click the **Use Default SAS account** to configure the default SAS account to the venue.
7. Review the selected SAS account details and click **Save**.

The **Updating LTE Settings** progress bar appears.

You have completed configuring a SAS account for a venue.

Configuring Software Build Version of the AP Model for a Venue

Follow these steps to configure the software build version of each APs for a venue.

1. On the Dashboard, click **Venues**.
The **Venues** page appears displaying the existing venues, if any.
2. Select the venue to configure the software build version for its APs.
The **Venue Overview** page appears.
3. Locate **LTE Settings** under **Venue Settings** and click **Edit**.
The **LTE Settings** dialog box appears.
4. Select the **AP Models' Build** tab.

The screenshot shows the 'Venue LTE Settings' dialog box with the 'AP Models' Build' tab selected. The dialog contains a table for selecting build versions for different AP models. The table has three columns: 'AP Model', 'Build', and 'Description'. There are four rows, each representing an AP model (Q710, Q910, Q410, Q950) with a dropdown menu set to 'Default official build' and a description of 'Default official build'. At the bottom of the dialog, there is a legend for '* Required field', a 'Cancel' button, and a 'Save' button.

AP Model	Build	Description
Q710	Default official build	Default official build
Q910	Default official build	Default official build
Q410	Default official build	Default official build
Q950	Default official build	Default official build

5. Select the desired software build for each AP models.
6. Click **Save**.

You have completed configuring software build version for each AP models in the venue.

Viewing Existing Venues

By default, a venue named My Venue exists.

Follow these steps to view venues that exist in your Ruckus LTE AP Management Service account.

Working with Venues

Viewing Venue Information

On the Dashboard, click **Venues**.

The **Venues** page displays a list of existing venues, including the following information:

- **Venue:** The name assigned to the venue. To view details about this venue, click the venue name.
- **Description:** A brief description of the venue.
- **City:** The city where the venue is physically located.
- **Country:** The country where the venue is located.
- **Networks:** The number of networks that exist at the venue. To view details about the network, pause the mouse pointer over or click the network number.
- **APs:** The number of access points that have been added to the venue. To view details about the APs, pause the mouse pointer over or click the AP number.
- **Clients:** The number of clients that are currently associated with the access points at the venue. To view details about the clients, click the client number.

Viewing Venue Information

The **Venues** page displays information about the venues that you have created in your account, including their locations, number of WLANs, number of APs, and number of currently associated clients.

Complete the following steps to view information about a venue.

1. From the navigation pane, click **Venues**.

The **Venues** page displays a list of existing venues.

2. Click a venue name to view more information about it. Information pertaining to the selected venue is displayed across five tabs: **Overview, WiFi Clients, APs, Networks, and Events**.

To view the clients, APs, networks, and events in the venue, click the corresponding tab.

Viewing Clients Connected to a Venue

You can review the WiFi clients that are connected to a particular venue.

Follow these steps to view details about clients that are currently associated with APs in a particular venue.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue that you want to check for connected clients.
3. In the same row as the venue name, click the number under the **Clients** column.

The **Clients** tab for the venue appears displaying the number of clients.

You have completed viewing information about clients that are connected to a venue.

Viewing APs Assigned to a Venue

You can review the APs that are assigned to a particular venue.

Follow these steps to view details about APs that are assigned to a particular venue.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue that you want to check for assigned APs.

3. In the same row as the venue name, click the number under the **APs** column.

NOTE

If the number under the **APs** column is 0 (zero), it will display a screen to allow you to add an AP.

The **APs** tab for the venue appears. Under the APs, two separate tabs, **LTE** and **WiFi** appear. These tabs display the following information about each AP that is assigned to the venue.

- **AP:** Name of the AP. LTE and Wi-Fi APs will have respective labels below the AP icon, which distinguish them between LTE APs and Wi-Fi APs. For more information about the APs, refer to [Viewing AP Details](#) on page 64.
- **Status:** Indicates the status of the AP. For example, if the AP is powered on and is providing wireless service to clients, a green check mark appears with the word **Operational** next to it.
- **Model:** Model number of the AP
- **IP Address:** IP address of the AP
- **Serial Number:** Serial Number, if the AP is not connected to the AP Management.
- **Venue:** Name of the venue.
- **Timing Role:** Timing role of the AP.
- **Timing Sync Status:** Time synchronization status.

Click the gear icon to display the **Add Columns** dialog and select an option.

- **AP Firmware:** AP firmware version
- **Last Seen:** Status of the AP when it was last connected to the cloud.
- **eNodeB ID:** Global eNodeB Identifier.
- **CBSD ID:** Citizens Broadband Radio Service Device (CBSD) identifier. This is allocated to the AP by SAS after successful registration.
- **EPC Connection:** The Evolved Packet Core (EPC) connection status.
- **Clients:** Number of LTE clients.
- **EARFCN:** E-UTRA Absolute Radio Frequency Channel Number that uniquely identifies the LTE band and carrier frequency.
- **PCI:** Physical Cell Identifiers (PCIs) that provides a pseudo-unique value for identifying nodes. PCI is unique per AP during operation and it is used to identify the serving cell on client devices.
- **MAC Address:** MAC Address of the AP.
- (Optional) Toggle the **CPI Certification related column** to **ON/OFF** and select or deselect the desired fields.

4. To add an AP, click **Add AP**.

The venue information is prepopulated with the current venue. Add the other AP details and click **Create**. For more information about adding an AP, refer to the [Adding an AP](#) on page 53.

You are returned to the **APs** tab under **Venues**.

You have completed viewing information about APs assigned to a venue.

Working with Floor Plans

Floor plans help you visualize the actual physical locations of the managed APs in your venues.

NOTE

For LTE APs, the location is required by SAS to grant bandwidth to APs, Therefore, the coordinates are mandatory for successful communication with SAS. Ruckus recommends that you add a floor plan and calibrate the AP on it to set the coordinates of an AP. For WiFi, the floor plan is a good to have option, but it is not mandatory.

Importing a Floor Plan

Importing a floor plan to a venue helps you visualize the actual physical locations of your managed APs and to configure the location of LTE APs.

To import a floor plan to your Ruckus LTE AP Management Service account, a floor plan image in the .GIF, .JPG or .PNG format. is required. The floor plan image must conform to the following parameters:

- Monochrome or grayscale
- No larger than 1MB in size
- No larger than 10 inches (720 pixels) per side.

Also, before you start this procedure, save the floor plan image to a location that you can access from the computer that you are using to access the Ruckus LTE AP Management Service web interface.

Follow these steps to import a floor plan.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue for which you want to import a floor plan.
3. In the **Overview** page, Click **Get Started** tab.
4. Complete the following fields to add a new floor in this venue:
 - **Floor Plan Name:** Type a name that you want to assign to the floor. For example, you can type "First Floor" or "Sales".
 - **Floor Number:** Type or select the floor or level number. Note that "0" is the ground floor, "1" is the first floor, "2" is the second floor, and so on.
 - **Floor Plan Image:** To upload a floor plan image for this floor, click **Upload**. When the **Open** dialog box appears, browse to the location where you saved the floor plan image, select the image, and then click **Open**.

NOTE

If you want to calibrate the floor plan to a map while uploading, select the check box at the bottom left corner of the **Add New Floor Plan** dialog box. You can choose to calibrate later by clearing the check box. By default, the check box is selected.

5. Click **Add**. If you selected the check box to calibrate while uploading, the **Floor Plan Calibration** dialog box appears.
6. In the **Floor Plan Calibration** window, first calibrate your floor plan image to a map, to accurately geo-position your APs. Drag and drop to position the two pins on corresponding features in the floor plan and on the map.

If you did not select the check-box in the previous step, the imported floor plan appears on the **APs** tab. A list of APs that have not been placed on any existing floor plans also appear on the right side of the imported floor plan.

NOTE

Click the globe icon on top left side of the floor plan to calibrate the floor plan as mentioned in Step 7.

7. Click **Save**.

A progress bar appears as AP Management Service creates the floor plan and uploads the floor plan image to your account. After the process is complete, the floor plan image you imported appears on the list of thumbnails at the bottom of the page.

You have completed importing a floor plan to a venue.

Calibrating the floor plan

From the RUCKUS LTE AP Management user interface, you can add a floor plan and calibrate it to a map.

Follow these steps to calibrate a floor plan.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue from which you want to calibrate a floor plan.
The venue **Overview** page appears.
3. From the list of image thumbnails at the bottom of the page, click the floor plan image that you want to calibrate.

The floor plan is displayed.

4. In the upper-right corner, click the **More**.
The action drop-down appears with these three options:

- **Edit Floor Plan**
- **Calibrate Floor Plan**
- **Delete Floor Plan**

5. Click **Calibrate Floor Plan**.

The **Floor Plan Calibration** dialog, which prompts you to calibrate the floor plan image to a map. Calibrating the floor plan allows you to properly geo-position the APs.

6. Click **Save**.

You are prompted with a message that the floor plan is being updated. The new Venue which you created appears in the window and the floor plan which you calibrated is displayed.

You have completed calibrate a floor plan from a venue.

Editing a Floor Plan

Follow these steps to edit a floor plan.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue from which you want to edit a floor plan.
The venue **Overview** page appears.
3. From the list of image thumbnails at the bottom of the page, click the floor plan image that you want to edit.

The floor plan is displayed.

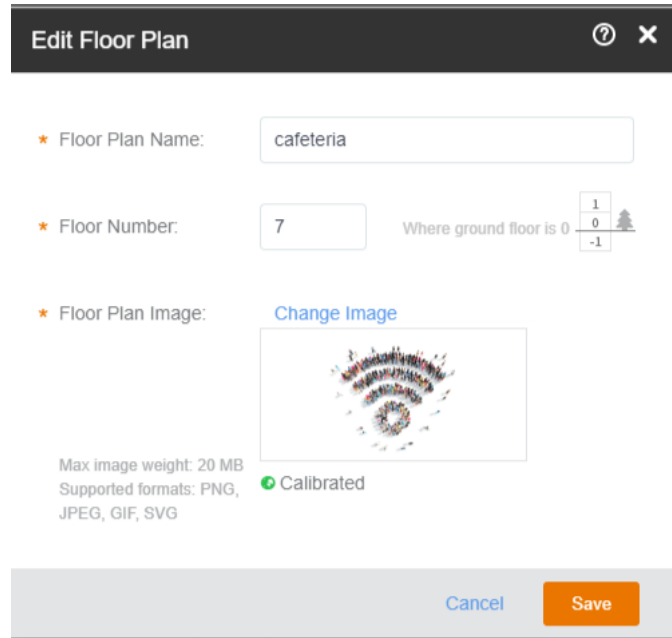
4. In the upper-right corner, click **More**.
The action drop-down appears with these three options:

- **Edit Floor Plan**
- **Calibrate Floor Plan**
- **Delete Floor Plan**

5. Click **Edit Floor Plan**.

The **Edit Floor Plan** dialog appears.

FIGURE 16 Edit Floor Plan



6. Edit the floor plan as necessary.
 - **Floor Plan:** Enter a name for the floor plan.
 - **Floor Number:** Specify the floor number.
 - **Floor Plan Image:** Upload a different floor plan. Click **Change Image** to change the floor plan image.
7. Click **Save**.

You have completed editing a floor plan from a venue.

Editing AP Placement

Follow these steps to edit AP placement.

1. On the Dashboard, click **Venues**.
2. From the list **Venues**, select the venue in which you want to edit AP placement.

The **Overview** tab is displayed. This page displays the total number of APs, APs in setup phase, and the total number of unplaced APs.
3. Click **Edit AP Placement**.
4. In the upper-right corner, click **Unplaced APs**.

The unplaced APs drop-down appears
5. Drag and drop an existing AP on the floor plan or select an unplaced AP and drag and drop on the floor plan and then click **Save**.

The selected AP is placed on the desired location on the floor plan.

You have completed editing AP placement for a venue.

Deleting a Floor Plan

If you no longer use a floor plan that you previously imported, delete it.

Follow these steps to delete a floor plan.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue from which you want to delete a floor plan.
The venue **Overview** page appears.
3. From the list of image thumbnails at the bottom of the page, click the floor plan image that you want to delete.
The floor plan is displayed.
4. In the upper-right corner, click **More**.

The action drop-down appears with these three options:

- **Edit Floor Plan**
- **Calibrate Floor Plan**
- **Delete Floor Plan**

5. Click **Delete Floor Plan**.

A confirmation message appears.

6. Click **Yes**.

The message `Deleting floor plan` appears as the Ruckus LTE AP Management deletes the floor plan image from your account. After the process is complete, the page refreshes, and then the image disappears from the thumbnail list.

You have completed deleting a floor plan from a venue.

Viewing Networks Configured for a Venue

The **Network** page displays details of the network configurations for a particular venue.

Follow these steps to view details about networks that are configured for a particular venue.

1. On the Dashboard, click **Venues**.
2. On the **Venues** page, locate the venue that you want to check for configured networks.

- In the same row as the venue name, click the number under the **Networks** column.

NOTE

To view the names of the networks assigned to this venue, hover your mouse pointer over the number.

NOTE

If the number under the **Networks** column is 0 (zero), you get the following message when you click it: No networks activated in this venue. Use the ON/OFF switches in the list to select the Networks to activate..

The **Networks** tab for the venue appears and displays information about each network that is assigned to the venue.

- Network name:** The name of the network. For more information about this network, click the network name.
- VLAN:** Displays the VLAN ID that is assigned to the network.
- Network ID:** The unique identification number of the LTE network.
- Activation:** The activation status toggle button. This button allows you to click and activate the LTE network. Clicking the button in activated state will deactivate the LTE network.

You have completed viewing information about the LTE network that is configured for this venue.

Viewing Events That Have Occurred in a Venue

Periodically viewing events that have occurred in a venue can help alert you to potential issues with Ruckus Cloud-managed APs and wireless clients that associate with them.

Follow these steps to view events that have occurred in a particular venue.

- On the menu, click **Venues**.
- On the **Venues** page, locate the venue in which you want to view events.
- Click the venue name.

The venue details page appears.

- Click the **Events** tab.

The **Events** tab appears and displays the latest events that have occurred in the venue over the last 24 hours. The following columns display the event details:

- Date:** The date and time when the event occurred.
- Severity:** The severity level of the event. See [#unique_52](#) for information on what each severity level means.
- Event Type:** The component that generated the event. Possible values include user (for example, a user disassociated from the network) and AP (for example, an AP was rebooted).
- Source:** The name of the AP on which the event occurred.
- MAC Address:** The MAC address of the AP on which the event occurred.
- Description:** A brief description of the event. The event description is dynamic, not static. Information specific to the event including identification of the related entity displays giving customers more information and allowing easier troubleshooting of events, if required. For example, the MAC address of the connected client is displayed.

By default, the **Events** tab displays all severities and all event types.

5. To filter the events that appear on the **Events** tab, use any or a combination of the following filters:
 - **All Severities:** Click this drop-down menu, and then select the specific severity that you want to display.
 - **All Event Types:** Click this drop-down menu, and then select the event type that you want to display.
 - **Jump To:** Click **Time**, and then select a date on the calendar for which you want to display events. If you want to view events that occurred at a specific time on the selected date, click the clock icon below the calendar, and then select the specific time from the hour and second picker. The Events tab will display all events that have occurred in the venue during the 24-hour period following the time you selected.
 - **Search for events:** In the search box, type a keyword that you want to use for any matching events. Click the magnifying glass icon to start the search.

You have completed viewing events that have occurred at a particular venue.

Customizing the LTE Setting for a Venue

If you want to customize the LTE settings of a venue, you can override the default parameters.

Follow these steps to customize the LTE settings of a venue.

1. On the Dashboard, click **Venues**.
2. Click the name of the venue for which you want to customize the LTE settings.
The venue overview page appears.
3. In the **Venue Settings** section, click **Edit** after the **LTE Settings**.
The **Edit LTE Settings** page appears.
4. Configure the following parameters:
 - In the **Timing Masters** field, click the **Manage** button to manage the timing masters. The **Manage Timing Masters** dialog appears. You can select up to six LTE APs to be designated as Timing Masters per Venue. Click **Save** to save the settings.

NOTE

Unless all LTE APs are configured as GPS, or the Venue has only one LTE AP configured, each Venue must have at least one Timing Master selected. If a Venue has just one LTE AP configured, the AP can operate in a stand alone mode and it will not require GPS synchronization.

- In the **Management VLAN ID** field, enter the VLAN number. This can be any value ranging from 1 through 4094.
Users in other VLANs cannot establish remote access sessions unless they are routed to the management VLAN. This provides an additional layer of security.
- In the **PTP VLAN ID** field, enter a valid VLAN ID. The valid value can be ranging from 1 through 4094.

NOTE

The Management VLAN, PTP VLAN, and External Device are optional fields.

- In the **Venue Type** field, select one of these venue types: dense, moderate, or sparse.
 - In the **TTD Configuration** field, select one of the TTD configurations. By default, TDD configuration is set to TDD config. 1
5. Click **Save** to complete the settings.

You have completed customizing the LTE settings of a venue.

Customizing the Wireless Radio Settings

If you want the Wi-Fi radio settings of a venue to be different from the default radio settings, you can override them for a particular venue.

NOTE

The 2.4 GHz and 5 GHz radio settings, although very similar, must be configured separately.

Complete the following steps to customize the radio settings of a venue.

1. From the navigation pane, click **Venues**.
2. Click the name of the venue for which you want to customize the radio settings.

The venue overview page is displayed.

3. In the **Wi-Fi Settings** section, click **Edit** after the **Wireless Radio Settings**.

The **Radio Settings** dialog box is displayed.

Radio Settings: Lab-Test

Reset to Default Settings

2.4 GHz

Channel selection method: Background Scanning

* Run background scan every: 20 Seconds

Bandwidth: Auto

Tx Power adjustment: Full

Channel selection:

1 2 3 4 5 6 7 8 9 10 11

Disable this channel

5 GHz

Channel selection method: Background Scanning

* Run background scan every: 20 Seconds

Bandwidth: Auto

Tx Power adjustment: Full

Channel selection:

Indoor APs

36 40 44 48 52 56 60 64 100 104 108 112 116

120 124 128 132 136 149 153 157 161

Outdoor APs

36 40 44 48 52 56 60 64 100 104 108 112 116

120 124 128 132 136 149 153 157 161

* Required field

Cancel Save

4. Configure the following settings for both the 2.4 GHz and 5 GHz radios:
 - **Channel Selection Method:** Select either **Background Scanning** or **ChannelFly**.
 - **Run background scan every [] seconds:** If you selected **Background Scanning**, interval at which Ruckus Cloud will run the scan. The interval ranges from 1 through 65535 seconds. The default is 20 seconds.
 - **Bandwidth:** Select **Auto**, **20 MHz**, or **40 MHz** channel width for the 2.4 GHz radio, or **Auto**, **20**, **40**, **80**, or **160 MHz** channel width for the 5 GHz radio.
 - **Tx Power Adjustment:** Manually set the transmit power on all 2.4 GHz or 5 GHz radios. The default is **Max**.
 - **Channel Selection:** A blue icon above the channel number indicates that the channel is enabled for the radio. If there are channels that you do not want the radio to use, disable them by clicking their respective icons. When a channel is disabled, its blue icon changes to gray.

NOTE

For the 5 GHz radio, you must configure a different set of channels for indoor APs and outdoor APs.

5. Click **Save**, and then click **Close**.

Editing a Venue

You can edit information pertaining to a venue (for example, the venue name or address).

Complete the following steps to edit a venue.

1. From the navigation pane, click **Venues**.
The **Venues** page displays a list of existing venues.
2. Click a venue name to view more information about the venue.
The **Overview** tab of the venue information page appears.
3. Click **Edit Venue** in the upper-right corner of the page.
The **Edit Venue** page is displayed.
4. Update the venue settings as required.
 - **Venue Name**
 - **Description**
 - **Address**
 - **Address Notes**
5. Click **Save**.

Deleting a Venue

You can delete a venue that you no longer need.



DANGER

Deleting a venue will also delete the APs and switches (and networks) that are deployed to that venue. Without any APs or switches and networks, users in the venue cannot access the Internet.

Working with Venues

Deleting a Venue

Complete the following steps to delete a venue.

1. From the navigation pane, click **Venues**.

The **Venues** page appears and displays a list of existing venues.

2. Click the venue name of the venue you want to delete.

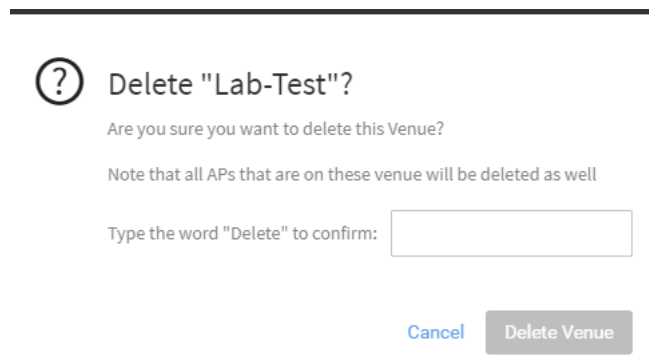
The **Overview** tab of the venue information page is displayed.

3. Click **More** in the upper-right corner of the page.

4. Click **Delete Venue**.

A dialog box appears prompting you to enter **Delete** for the selected venue that you want to delete.

FIGURE 17 Deleting a Venue



5. Enter **Delete** to delete the venue.

The **Venues** page appears.

6. Verify that the venue you deleted is no longer listed on the **Venues** page.

Managing Network Devices: APs

• AP Overview.....	53
• Adding an AP.....	53
• Adding ECGI Records.....	54
• Adding Certified Professional Installer Details.....	56
• Certifying an LTE AP.....	57
• Viewing LTE APs.....	59
• Viewing ECGI Records.....	60
• Viewing CPI Details.....	61
• Viewing Wi-Fi APs.....	62
• Exporting AP Screen Details.....	63
• Filtering APs.....	63
• Viewing AP Details.....	64
• Editing an LTE AP.....	70
• Editing ECGI Records.....	72
• Editing Certified Professional Installer Details.....	73
• Configuring Bonjour Services (Wi-Fi Only).....	74
• Downloading the AP Logs.....	77
• Turning AP LEDs ON/OFF.....	78
• Blink AP LEDs.....	81
• Rebooting an AP.....	82
• Resetting an AP to Factory Defaults.....	83
• Disabling or Enabling AP Service.....	83
• Deleting an AP from Ruckus LTE AP Management.....	84

AP Overview

Before adding an AP to your Ruckus LTE AP Management account, make sure that it is supported by the AP Management Service. For more information, refer to [Supported AP Models](#) on page 26.

Record the serial number of the AP, which is needed while adding the AP to Ruckus LTE AP Management Service. You can find the serial number on the serial number sticker affixed to the bottom of the AP.

Adding an AP

Follow these steps to add an LTE AP to your LTE AP Management account, account.

1. Connect the AP that you want to add to the LTE AP Management Service to a network that is connected to the Internet, and then plug it into a power source to power it on.
2. On the Dashboard, click **Add AP**. Alternatively, click **APs** on the menu, and then click **Add AP** in the upper-right corner of the page.

The **Create AP** form appears.

3. Complete the following fields to add an AP:

- **Venue:** Select the venue from the drop-down to which you want to deploy this AP.
- **AP Name:** Type a name for the AP. We recommend that you use the AP model number or another name that helps you identify this AP.
- **Description:** Type a brief description of the AP.
- **Tag:** Type a tag (keyword or term) that you want to assign to this AP. Using tags is another method to help describe this AP.
- **Serial Number:** Type the 12-digit serial number of the AP.

NOTE

The serial number for LTE AP has 2 and 9 in the fifth and sixth position respectively (for example, 123429132456). If you enter an LTE serial number, additional information fields pertaining to LTE are displayed as follows.

- **Set timing source as GPS:** Select this check box if you want to set GPS as the timing source.

NOTE

Ensure that the AP is installed in a location where it has good GPS signal reception. For example, line-of-sight to open sky or as close to a door or window as possible.

- **Set as timing master:** This check box is displayed when you select GPS as the timing source and allows you to set GPS as the timing master.

4. Optionally, you can click the box next to **Go to floor plan to place this AP.**

After the AP is created, the floor plan screen displays to allow you to identify the location of this AP.

5. Click **Create.**

After the addition of the AP, the page refreshes and displays the newly added AP under **Access Points**. Initially, the **Status** column shows **Never Contacted Cloud**. However, after the update, it takes up to 5 minutes for the status changes to **Connected** or **Operational**, depending on the existing configuration.

AP Statuses

Checking the status of an LTE AP periodically helps you detect and address existing or potential issues.

AP statuses are grouped into four main status categories containing additional status:

- **Green (Operational)** : Indicates that the AP is operating normally and is transmitting; capable of providing LTE service to clients.
- **Red (AP Disconnected)**: Indicates that the LTE AP is currently experiencing issues and unable to connect to Management platform.
- **Gray (Never Contacted Cloud)**: Indicates that the LTE AP is currently in the setup process and yet to establish first contact with LTE AP Management.
- **Yellow or Orange (Connected)**: Indicates that the AP is connected with the AP Management, albeit is unable to transmit due to a disruption of one of its essential requirements to provide service. For more information, refer to [#unique_17/unique_17_Connect_42_GUID-F6B7E509-1D90-4020-9570-F69DB1EA3D07](#) on page 15

Adding ECGI Records

In order to create networks with CBRS-A designated Shared HNI (PLMN ID) value of 315-010, tenants must add ECGI Records under the Administration Tab. An ECGI Record is unique per PLMN ID + Macro eNB ID combination.

If you desire to create an LTE Network with CBRS-A designated Shared HNI (PLMN ID) value of 315-010, you must obtain your own/ range of Macro eNB ID from CBRS Alliance. For more information, visit: <http://imsiadmin.com> and <http://atis.org/ioc>.

Creating ECGI records is basically defining and allocating a range of ECGI values. Then when you associate such records with a network, all APs within venues, designated with such a Network, obtain their ECGIs from these records until the record is depleted. When this happens, to add more APs to the Venue, you must add more ECGIs by defining additional ECGI records.

If you want to create an LTE Network with any other PLMN ID, you have a choice of configuring the Macro eNB ID and thereby creating ECGI records or skipping this step and allowing the AP management to create unique ECGIs for connected APs.

To add ECGI records, follow these steps.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, click the **ECGI Records** tab.
3. Click **Add ECGI Record**.

The **Add ECGI Record** dialog box appears.

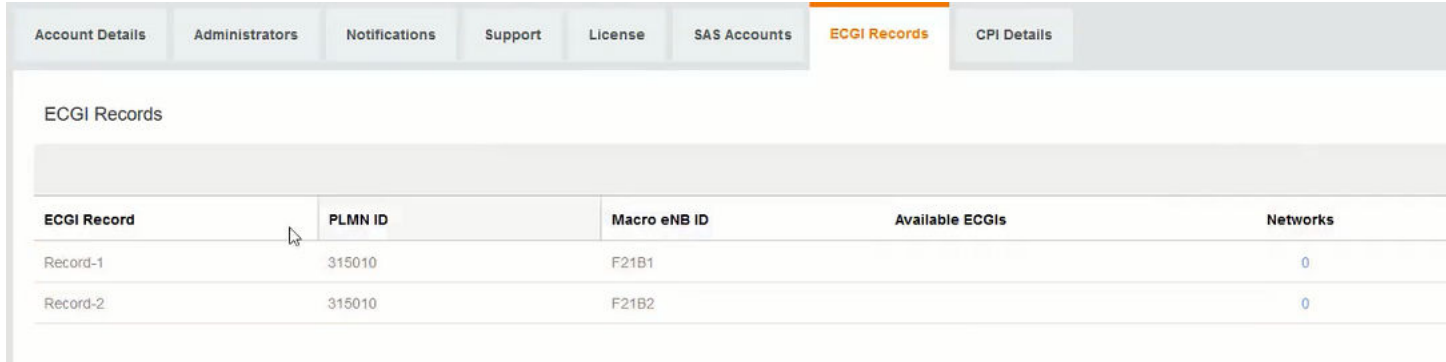
The screenshot shows the 'Administration' page with the 'ECGI Records' tab selected. The page contains a table with the following columns: ECGI Record, PLMN ID, Macro eNB ID, Available ECGIs, and Networks. A large blue 'Add ECGI Record' button is centered on the page. The 'ECGI Records' tab is highlighted with an orange underline. The 'Add ECGI Record' button is also highlighted with a blue underline. The 'Refresh' button is located in the top right corner of the table area.

4. Enter the following details in the appropriate fields.
 - **Name:** The ECGI record name.
 - **PLMN ID:** The PLMN ID. By default, the value is pre-populated as 315010.
 - **Macro eNB ID:** The Macro eNB ID.
 - **Cell Type:** You can select either **Home-eNB** or **Macro-eNB**.

5. Click **Save** to save the ECGI record.

A status message appears displaying `Creating ECGI Records`.

You can view the details of available of ECGI records under **ECGI Records**.



ECGI Record	PLMN ID	Macro eNB ID	Available ECGIs	Networks
Record-1	315010	F21B1		0
Record-2	315010	F21B2		0

You have completed adding an ECGI record.

For information on how to add an LTE Network, refer to [Creating an LTE Network](#) on page 87.

Adding Certified Professional Installer Details

The CPI details are not saved on the portal. They are used to use the private key within the p12 package to encrypt the AP location data and are purged after that. Only a Certified Professional Installer (CPI) can certify an AP.

To add the CPI details, follow these steps.

NOTE

The CPI must be certified by Ruckus and has the following:

- CPI ID
- p12 package issued by issuing authority such as INSTA.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, click the **CPI Details** tab.

3. Click **Add CPI Details**.

The **Add CPI Details** dialog box appears.

FIGURE 18 Add CPI Details

The screenshot shows a dialog box titled "Add CPI Details". It contains the following fields and controls:

- CPI Name:** A text input field containing "Ruckus_VAR".
- CPI ID:** A text input field containing "dummy1".
- CPI Certificate File:** A button labeled "Select File" with "P12 file" text below it.
- CPI Certificate File Password:** A password input field with masked characters "....." and an eye icon to toggle visibility.

At the bottom of the dialog, there is a legend for the asterisk (*), a "Cancel" button, and a "Save" button.

4. Enter the name of the CPI ID in the **CPI Name** field.
5. Enter the CPI ID in the **CPI ID** field.
6. Click **Select File** and browse to the p2 package.
7. Enter the password for the CPI certificate file in the **CPI Certificate File Password** field.
8. Click **Save** to save the CPI details.

NOTE

CPI details are not saved and may be requested again after a timeout.

You have completed adding CPI details.

For information on how to add a SAS account, refer to [Adding a SAS Account](#) on page 184.

Certifying an LTE AP

Only a CPI can certify an AP.

Follow these steps to save and certify an AP.

1. On the Dashboard, click **APs**.
The **Access Points** page appears.
2. From the access point list, click the name of the AP that you want to save and certify.
The AP information page appears.

3. In the upper-right corner of the page, click **Edit AP**.
The **Edit AP** dialog box appears.

FIGURE 19 Edit AP

AP Location (Required for US FCC rules)

Latitude: 37.410255

Longitude: -122.017267

Height (AGL): 127.95 Feet

Deployment: Indoor Outdoor

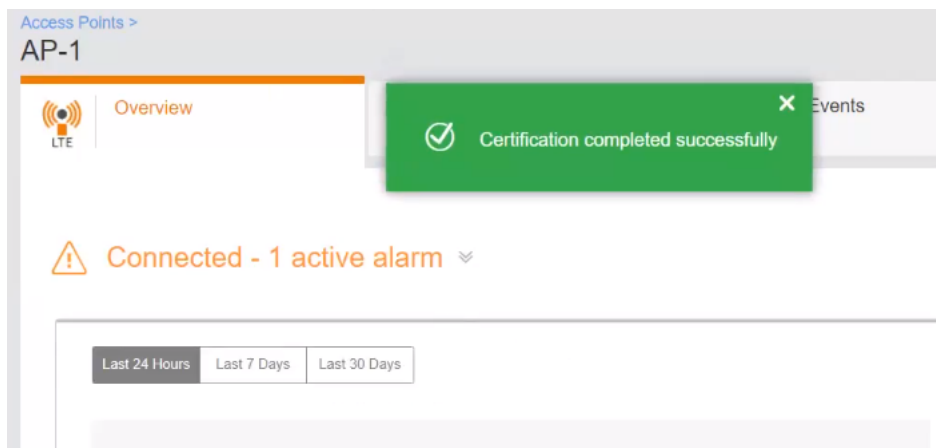
[View full details](#) [Copy details](#)

CPI Certified (with STA) [Remove CPI Certification](#)
Date: 25/09/2019

* Required field [Cancel](#) [Save](#)

4. Edit the AP as needed.
5. Click **Save and Certify**.

After sending the AP details to SAS, the following message appears, and the **AP properties** window displays the AP as **Certified**.



NOTE

If you modify or change the AP location information, AP type or SAS information, the AP certification gets revoked and you have to certify the AP again.

Removing the AP Certification

6. From the list of certified APs, select the AP which you want to uncertify.
7. Click the down arrow next to **Certified** and click **Remove Certification**.

[Export to CSV](#)

AP	Timing Role	Timing Sync Status	Up Time	Tags	Latitude	CPI Certification
AP-4	Venue	Slave (PTP)	Initializing	2 days, 11 hours	47.2351	✓ Certified
AP-3	Venue	Slave (PTP)	Initializing	2 days, 11 hours	10.2563	Remove Certification
AP-1	Venue	Slave (PTP)	Initializing	2 days, 17 hours	35.1231	✓ Certified
AP-2	Venue	Slave (PTP)	Initializing	2 days, 17 hours	15.2525	✓ Certified

Viewing LTE APs

You can view a summary of LTE APs that are added to Ruckus LTE AP Management account and review all of their statuses from the **Access Points** list.

Follow these steps to view APs from the LTE tab. To view Wi-Fi APs, refer to [Viewing Wi-Fi APs](#) on page 62.

NOTE

When viewing the APs, table columns can be added and removed, and the columns are sortable on all relevant screens (APs, Dashboard, Venue Details, and Network screens). On the client side, the columns and their order is saved and are applied to all relevant tables. After a user deselects a column, its order is not saved. For the APs screen, the AP column is pinned and cannot be moved or removed.

1. On the Dashboard, click **APs**.
The **Access Points** page appears with the **LTE** tab, by default. The number in brackets indicates the number of managed LTE APs in your account.
2. Review the information about your LTE APs under the following default columns.
 - **AP:** The name of the access point. To view details about this LTE AP, click the AP name.
 - **Status:** The current status of the AP, for example, **Operational**.
 - **Model:** The hardware model of the Ruckus LTE AP.
 - **IP Address:** The IP address assigned to the LTE AP by the local network of tenant that is used to connect to the Cloud.
 - **Serial Number:** The serial number of the LTE AP.
 - **Venue:** The name of the venue.
 - **Timing Role:** The timing role, for example, Master, Slave or Independent.
 - **Timing Sync Status:** The time synchronization status, for example, Locked.
 - **Up Time:** Time in days and hour since the last reboot.
 - **Tags:** Shows any tags assigned to the AP.

- Review the information about your LTE APs under the following columns that can be selected by users.
 - AP Firmware:** The current firmware (software) version which is running on the LTE AP.
 - Last Seen:** The status of the AP when it was last connected to the cloud.
 - eNodeB ID:** The global eNodeB Identifier.
 - CBSID ID:** Citizens Broadband Radio Service Device (CBSID) identifier. This is allocated to the AP by SAS after successful registration.
 - EPC Connection:** The Evolved Packet Core (EPC) connection status.
 - Clients:** The number of LTE clients that are currently served by this AP.
 - EARFCN:** E-UTRA Absolute Radio Frequency Channel Number that uniquely identifies the LTE band and carrier frequency.
 - PCI:** Physical Cell Identifiers (PCIs) that provides a pseudo-unique value for identifying nodes. PCI is unique per AP during operation and it is used to identify the serving cell on client devices.
 - MAC Address:** MAC Address of the AP.

CPI Certification-related Column

- Latitude:** The latitude of the location.
 - Longitude:** The longitude of the location.
 - Height:** The height above the ground level.
 - Deployment:** Where the AP is deployed.
 - FCC ID:** The FCC ID of the AP
 - Antenna Beamwidth:** The antenna beam width.
 - Antenna Azimuth:** The antenna azimuth.
 - Antenna Down Tilt:** The antenna down tilt.
 - Antenna Gain:** The antenna gain.
 - CPI Certification:** The CPI Certification.
- To sort a large number of APs by the column name, click the name of the column, for example, by **Status**.

You have completed viewing a summary of all LTE APs that are added to your LTE AP Management account.

Viewing ECGI Records

To view the ECGI records, follow these steps.

- On the Dashboard, click **Administration**.

- On the **Administration** page, click the **ECGI Records** tab.
In the **ECGI Records** tab, the following information is displayed.

FIGURE 20 ECGI Records

The screenshot shows the 'Administration' page with the 'ECGI Records' tab selected. The table below lists five ECGI records with their respective IDs and network counts.

ECGI Record	PLMN ID	Macro eNB ID	Available ECGIs	Networks		
RecordNonShared_1	00101	BCDEF	128	2	Edit	Delete
RecordNonShared_2	00101	CDEFB	128	1	Edit	Delete
RecordNonShared_PLMNchange	00102	DEFBC	128	1	Edit	Delete
RecordShared_1	315010	ABCCE	128	1	Edit	Delete
RecordShared_2	315010	BCDEA	128	1	Edit	Delete

- **ECGI Record:** The ECGI record name.
- **PLMN ID:** The PLMN ID.
- **Macro eNB ID:** The Macro eNB ID within the ECGI identifies a group of cells within an PLMNID (SHNI). This will be assigned by the CBRS Alliance and will leave 8 bits to be assigned by the operator to identify individual cells. The full ECGI format is PLMN ID(SHNI) (6dec/24bin) + Macro eNB ID (5hex/20bin) + Cell Identity (2hex/8bin). Each PLMN ID + Macro eNB ID.
- **Available ECGIs:** The available ECGIs.
- **Networks:** Number of Networks the ECGI records are being used.

For more information, visit the [Technical Support bulletin](#) published under KB articles.

You have completed viewing the ECGI records.

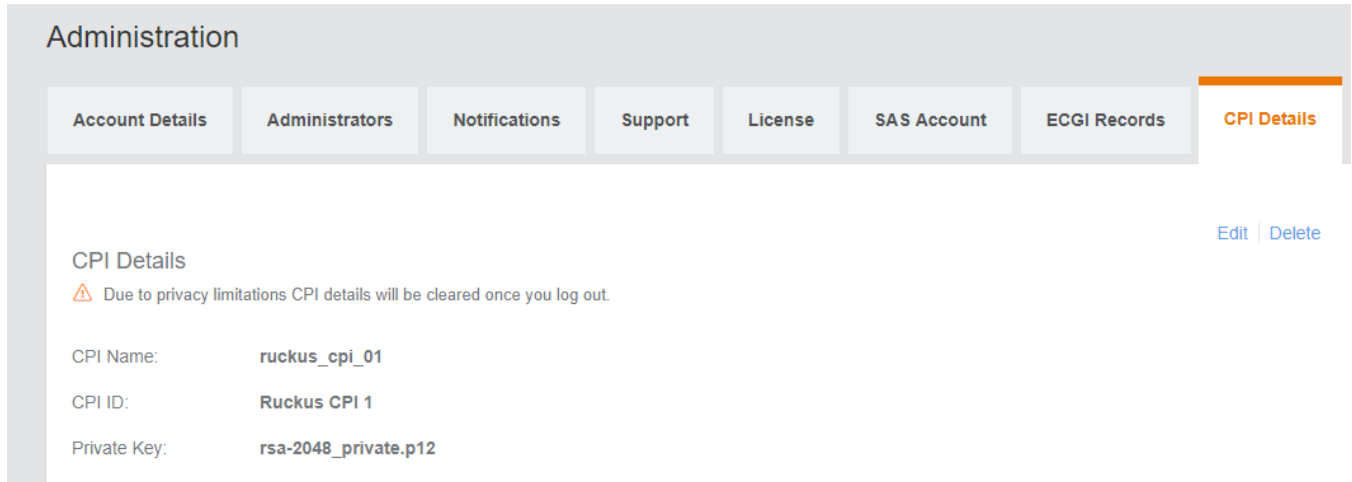
Viewing CPI Details

To view CPI details, follow these steps.

- On the Dashboard, click **Administration**.

2. On the **Administration** page, click the **CPI Details** tab.
In the **CPI Details** tab, the following information is displayed.

FIGURE 21 CPI Details



- **CPI Name** : The name of the Certified Professional Installer.
- **CPI ID**: The ID of the Certified Professional Installer.
- **Private Key**: The P12 package file (this package includes the private key).

You have completed viewing the CPI details.

Viewing Wi-Fi APs

You can view a summary of Wi-Fi APs that you have added to your Ruckus Cloud account and review all of their statuses. The **WiFi** tab is displayed on Ruckus LTE AP Management Service if you have added at least one Wi-Fi AP to it.

Follow these steps to view APs from the **WiFi** tab. To view LTE APs, refer to [Viewing LTE APs](#) on page 59.

NOTE

When viewing the APs, table columns can be added, removed, and columns are sortable on all relevant screens (APs, Dashboard, Venue Details, and Network screens). On the client side the columns and their order is saved and are applied to all relevant tables. Once a user deselects a column, its order is not saved. For the APs screen, the AP column is pinned and cannot be moved or removed.

1. On the menu, click **APs**.
The **Access Points** page appears and displays the **LTE** tab by default.
2. Click the **WiFi** tab.
The **Access Points** page appears and displays the **WiFi** tab. The number in brackets indicates how many managed Wi-Fi APs are in your account.

3. View information about your Wi-Fi APs under the following default columns.
 - **AP:** The name of the access point. To view details about this access point, click the AP name. This field is sortable.
 - **Status:** The current status of the AP (for example, **Operational**).
 - **Model:** The hardware model of the Ruckus AP. Sortable field.
 - **IP :** The IP address assigned to the AP. Sortable field.
 - **Identifier:** The unique serial number of the AP, assigned to the AP network interface while creating the AP.
 - **Uptime:** Time in days and hours that the AP has been operational.
 - **Tags:** Shows any tags assigned to the AP.
4. View information about your Wi-Fi APs under the following columns.
 - **Clients:** The number of LTE clients that are currently associated with this access point. To view details about the wireless clients, click the client number.
 - **Mesh :** (Only for Wi-Fi AP) If Wi-Fi mesh networking is enabled on the AP, this column shows the role of the AP on the mesh network.
5. If a large number of APs appear on the page, you can sort them by the column names. To sort APs by the column name, click the name of the column (for example, **Status**).

You have completed viewing a summary of Wi-Fi APs that you have added to your account.

Exporting AP Screen Details

If you want to export the AP details viewable on the LTE AP or Wi-Fi AP screens, you can export them in a comma-separated value (CSV) file to your computer. This feature can be used as an option for inventory management for all APs in your account.

Follow these steps to export AP screen details.

1. On the Dashboard, click **APs**.
The **Access Points** page appears displaying details of your LTE APs.
2. (Optional) Click the **WiFi** tab to display details of your Wi-Fi APs.
3. In the upper-right corner of the **Access Points** screen, click **Export To CSV**.
A file named `LTE_AP_LIST_MMDDYY.csv` is downloaded to your system.
4. From the default downloads location on your system, open the .csv file to review its contents.
The .csv file containing AP details opens in Microsoft Excel or other selected program.

You have completed exporting AP screen details.

Filtering APs

Use the filtering options on the **Access Points** page (both **LTE** and **WiFi** tabs contain the same filters) to display LTE or Wi-Fi APs based on the criteria you specify. These filtering options are especially useful when you have a large number of LTE or Wi-Fi APs.

Searching for APs Based on AP Name, MAC Address, IP Address, Model, and Tags

To search for an LTE client based on the AP name that was used to access the network or its MAC address, type the partial or full AP name, MAC address, IP address, model, or tags in the search box. The page refreshes and displays any matching APs.

NOTE

Searches for AP name and MAC address are not case sensitive.

Displaying APs That Are in Specific Status

By default, the **Access Points** page displays all LTE or Wi-Fi APs in all statuses. To display only LTE or Wi-Fi APs that are in a specific status, click the down arrow after **All Statuses**, and then select the status for which you want to view associated LTE or Wi-Fi APs.

Displaying a Specific AP Model

By default, the **Access Points** page displays all LTE or Wi-Fi APs of all models. To display LTE or Wi-Fi APs of a specific AP model, click the down arrow after **All Models**, and then select the AP model for which you want to view associated LTE or Wi-Fi APs.

Displaying APs Associated With a Specific Tag

By default, the **Access Points** page displays all LTE or Wi-Fi APs and their associated tags. To display only LTE or Wi-Fi APs that are associated with a specific tag, click the down arrow after **All Tags**, and then select the tag for which you want to view associated LTE or Wi-Fi APs.

Viewing AP Details

From the **APs** page, you can select elements on the web interface to display detailed information about wireless clients associated with an AP, networks that are active on an AP, and events that have occurred on the AP within the last 24 hours.

Complete the following steps to view the AP details.

1. From the navigation pane, click **Networking Devices** and select the **WiFi** tab.

Click an AP name to view details about the AP.

2. Click the name of the AP that you want to view for clients.

The **Overview** tab displays the following information:

- An informational message if the AP has a configuration error or failure.
- A graph showing the traffic volume (downstream traffic and upstream traffic). To change the time period, click one of the following check boxes:
 - Last 24 Hours (This is the default display.)
 - Last 7 Days
 - Last 30 Days
- A photo of the device model.
- The following properties of the AP:
 - **Name:** The name of the AP.
 - **Venue:** The venue in which this AP is located.
 - **Description:** The description of the AP.
 - **AP service:** Displays the status of the service (ready [configuration is complete] or not ready). If the services are not fully ready, a percentage of the readiness status is displayed. Pause the pointer on the percentage to view the percentage you must provide to enable the services. You are prompted to complete the information to make the AP service operational.

NOTE

Although the AP service may be ready, the AP may not be operational if you manually disable the service from the portal.

- **Up time:** Displays how long the AP has been providing service.
- **Last Seen:** The last time the AP refreshed its connection to Cloud.
- **IP address:** The IP address allocated to the AP.
- **Channel:** The radio channels used by the AP on 2.4GHz and 5GHz.

Click **More** to view additional properties of the AP. For additional information, refer to [Viewing AP Properties](#) on page 68.

- The floor plan information if configured.
- The settings for Bonjour or Wi-Fi Radio if configured (for Wi-Fi only).

Viewing Wi-Fi Clients Associated with an AP

Follow these steps to view a list of clients associated with a specific Wi-Fi AP.

1. On the menu, click **APs**.
The **Access Points** page appears.
2. Click the name of the AP that you want to check for clients.
The **Overview** tab of the AP information page appears.

3. Click the **Clients** tab.

The page refreshes, and then **Clients** tab displays a list of Wi-Fi clients that are currently connected to the Wi-Fi AP, including the following information:

- **OS:** Displays the operating system that the wireless client is running.
- **MAC Address:** Displays the MAC address of the wireless client.
- **IP Address:** Displays the IP address of the wireless client.
- **Username:** Displays the user name that was used to authenticate with the AP.
- **Hostname:** Displays the host name (or device name) of the wireless client.
- **Network (VLAN):** Displays the network service and VLAN ID in brackets to which the wireless client is connected.
- **Time Connected:** Displays the length of time that the wireless client has been associated with the AP.

NOTE

The information on the **Clients** tab is not updated in real time. To view the latest information, click the refresh button in the upper-right corner of the tab.

4. Type the partial or full user name or host name, MAC address, IP address, OS type, AP name or VLAN ID in the search box, and then click the search (magnifying glass) button to search for connected client.

The **Clients** tab displays both connected and disconnected (historical) wireless clients. Two lists will display and you may have to scroll down or filter the results using the **search** box.

NOTE

Search criteria for historical clients is restricted to partial or full user name or host name, or MAC address.

The list of historical (disconnected) clients includes the following information:

- **MAC Address:** MAC address of the client
- **Last IP:** The last recorded IP address of the client
- **Username:** User name used by the user to join the wireless network
- **Hostname:** Host name of the client
- **Last Venue:** Name of the venue with which the client was last associated
- **Last AP:** Name of the last access point with which the client was connected
- **Last Network:** Name of the last wireless network that the client had joined
- **Last Seen:** The date and time that the client was last connected with the AP

5. From the list of either connected or disconnected clients, locate the wireless client for which you want to view details, and then click its MAC address.

The **Client MAC Address** page appears and displays three sections across two panes followed by five report-type sections. For more details, refer to the [Viewing Client Details](#) on page 146.

You have completed viewing the wireless clients that are currently associated with an AP.

Viewing Networks Configured on an AP

Review the networks and that have been configured on an AP.

Follow these steps to view the networks that are currently active on a particular AP.

1. On the Dashboard, click **APs**.

The **Access Points** page appears.

2. From the list of access points, click the name of the AP that you want to view.

The AP information page appears.

3. Click the **Networks** tab.

The page refreshes, and then **Networks** tab displays the list of networks that are currently active on the AP, including the following information:

- **Network:** The name of the network. To view more information about this network, click the network name.
- **Network ID:** The unique network identification number.

NOTE

For LTE networks, the Network ID is the PLMN ID.

- **Venues:** The name of the venue to which this AP is physically deployed.

You have completed viewing information about the networks that are currently active on this AP.

Viewing Events That Have Occurred on the AP

By periodically monitoring the events that have occurred on an AP or on clients that are associated with the AP, you can detect potential issues.

Follow these steps to view events that have occurred on a particular AP.

1. On the Dashboard, click **APs**.

The **Access Points** page appears.

2. From the access point list, click the name of the AP that you want to check.

The AP information page appears.

3. Click the **Events** tab.

The **Events** tab appears and displays the latest events that have occurred on the AP in the last 24 hours. The following columns display the event details:

- **Date:** The date and time when the event occurred.
- **Severity:** The severity level of the event. refer to [Event Severity Levels](#) on page 159 for information on what each severity level means.
- **Event Type:** The component that generated the event. Possible values include Admin, AP (for example, an AP was rebooted), Client (for example, a user left the Wi-Fi network) and Notification.
- **Source:** If the event occurred on the AP, this column shows the AP name. If the event occurred on a client, this column shows the MAC address of the client.
- **Identifier:** The MAC address of the AP on which the event occurred.
- **Description:** The Alarm ID and a brief description of the event.

4. (Optional) Click the **View Event** icon to view the event details.

To view the next page, click the right arrow (>). To jump to the last page of events, click the >| arrow.

You have completed viewing events that have occurred on the AP.

Viewing AP Properties

The AP properties dialog box displays information about the AP including name, venue, serial number MAC address, IP address, timing source, firmware version, SAS, and so on.

To view detailed information about an AP from the **Access Point** overview page, go to the **AP Properties** section, and then click **More**.

The page that loads displays the following information:

- **Name:** The name of the AP.
- **Venue:** The name of the venue to which the AP is deployed.
- **Description:** The description currently assigned to the AP.
- **S/N:** The serial number of AP.
- **MAC Address:** The MAC address of the AP.
- **IP Address:** The IP address that is currently assigned to the AP.
- **Model:** The AP model.
- **Band:** The frequency band, which is a specific range of frequencies in the radio frequency (RF) spectrum, ranging from low frequencies to high frequencies. Each **band** has a defined upper and lower frequency limit.
- **FW Version:** The firmware release that is currently installed on the AP.
- **NTP Sync Status:** Status of NTP synchronization.
- **NTP Local Time:** The current date and time.
- **NTP Server IP:** The host name or IP address.

Radio Parameters

- **ECGI:** ECGI is the Identifier which is used to identify cells globally. The ECGI is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code) and the ECI (E-UTRAN Cell Identifier).
- **Physical Cell ID:** The identification of a cell at the physical layer.

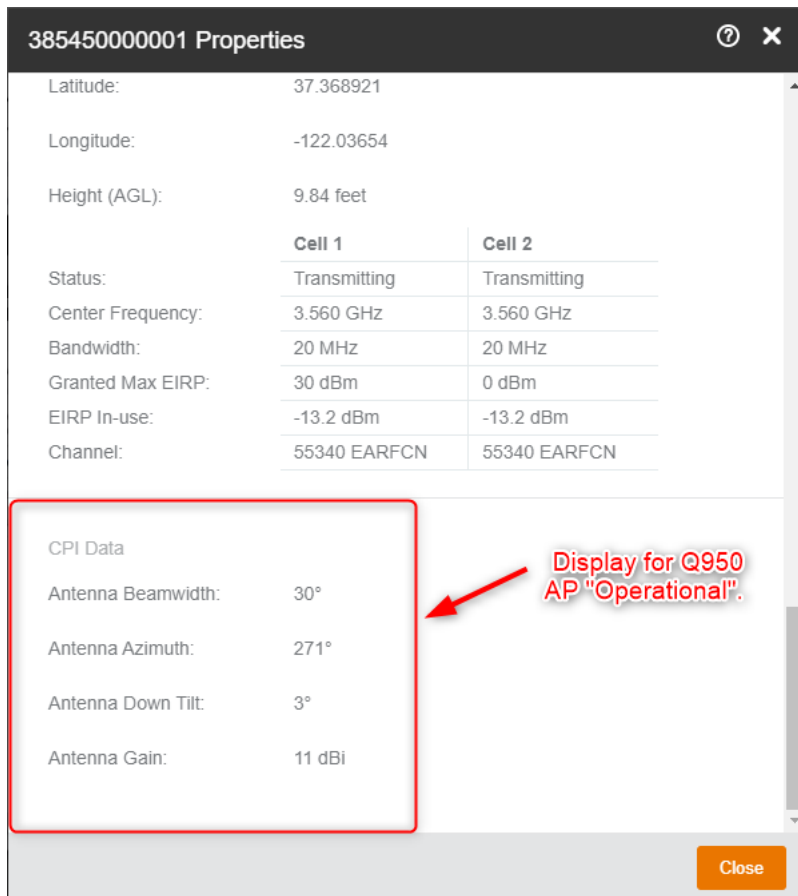
Networking Parameters

- **EPC (S1) Connection status:** The S1 connection status. For example, Connected
- **Timing Role:** The timing role: master, slave, or independent. For example, Independent (internal clock).
- **Timing source:** The timing source. For example, Internal Clock
- **Timing Sync Status:** The time synchronization status. For example, Lock.
- **VLANS**
 - **Management VLAN:** The number of management VLAN.
 - **Data VLAN:** The number of data VLANs.
 - **Timing VLAN:** The number of timing VLANs.
- **SAS Information:** The information pertaining to the spectrum allocation servers, which automates the process of assigning spectrum.
- **CBSD ID :** The CBSID Identifier.
- **Latitude:** The latitude of the location.
- **Longitude:** The longitude of the location

- **Height (AGL):** The height above the ground level.
- **Status:** The status of the AP.
- **Center Frequency:** The center frequency.
- **Bandwidth:** The network bandwidth.
- **Granted Max EIRP:** The maximum EIRP granted.
- **EIRP In-use:** The EIRP in use.
- **Channel:** The channel number.

When LTE AP operates in Carrier Aggregation (CA) mode and obtain appropriate grants to transmit from SAS, Cell 2 and Cell 2 details are displayed:

FIGURE 22 AP Properties



The CPI data for Q950 is displayed as follows.

- **Antenna Beamwidth:** The Beamwidth of the antenna.
- **Antenna Azimuth:** The azimuth of the antenna.
- **Antenna Down Tilt:** The downtilt angle of the antenna.
- **Antenna Gain:** The antenna gain.

Editing an LTE AP

You can edit an AP to change its venue and/or name.

Follow these steps to edit an AP.

1. On the Dashboard, click **APs**.
The **Access Points** page appears.
2. From the access point list, click the name of the AP that you want to edit.
The AP information page appears.
3. In the upper-right corner of the page, click **Edit AP**.
The **Edit AP** form appears.

Edit AP

* Venue: My Venue

* AP Name: AP-972035000051

Description:

Tags: Add a tag

* Serial Number: 972035000051

* Cell Type: Macro-eNB

Set timing source as GPS
Make sure parent AP is installed where GPS signal is available such as near a window or outdoors

* Required field Cancel Certify (CPI) & Save Save

4. Update the AP settings as required.

You can edit the following fields:

- **Venue:** Change the venue to which you want to deploy this AP.
 - **AP Name:** Change the name for the AP. You could use the AP model number or another name that helps you identify this AP.
 - **Description:** Change the description of the AP.
 - **Tag:** Change the tag (keyword or term) of this AP. Using tags is another method to help describe this AP.
 - **Serial Number:** You cannot edit the serial number.
 - **Cell Type:** You can change the cell type as Home-eNB (default) to Macro-eNB.
5. Select or clear the **Set timing Source as GPS** button. This action enables the GPS clock synchronization. If you select this option, you are prompted with another **Set as Timing Master** button. Select or clear the button as required. If selected, it is set as the master clock and is distributed throughout the network, providing frequency synchronization.
 6. Edit the AP location by updating the latitude, longitude, and height from the sea level (in feet and meters).

NOTE

The location parameters cannot be changed if an AP is placed on the floor plan.

7. Choose the deployment as **Indoor** or **outdoor** by selecting the respective button.



WARNING

Saving changes in deployment type will remove current AP certification.

You are prompted with a **Not Certified** messages, if the Federal Communications Commission identification number (FCC ID), Maximum EIRP and related antenna configuration provided for the AP lacks certification. Effective Isotropic Radiated Power (EIRP) is used to figure out if a radio solution is within the values allowed by local regulatory bodies.

NOTE

The deployment type is partially developed for current release. The **Save and Certify** option is highlighted after the LTE AP is powered on and is placed on a calibrated floor plan, and it obtains its Geo-co-ordinates. When you click **Save and Certify**, LTE AP starts its registration process with the SAS.

For Q950, additional information is displayed in the **Edit AP** dialog. Click **Copy details** to copy the information.

Edit AP

Deployment: Indoor

FCC ID: S9GQ950US02

Antenna Model: P01-Q950-US02

Antenna Beamwidth: 30 Degrees

Antenna Azimuth: 271 Degrees

Antenna Down Tilt: 3 Degrees

Antenna Gain: 11 dBi

[Copy details](#)

CPI Certified (with STA) [Remove CPI Certification](#)

* Required field Cancel Save

8. Click **Save**.

You have completed editing an AP.

Editing ECGI Records

To edit ECGI records, follow these steps.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, click the **ECGI Records** tab.

3. Click **Edit** corresponding to the ECGI record that you want to edit.

The screenshot shows a modal dialog titled "Edit ECGI Record". It features three input fields, each preceded by a red asterisk indicating it is a required field. The first field is "Name" with the text "Record-1". The second is "PLMN ID" with the text "315010". The third is "Macro eNB ID" with the text "F21B1" and a blue question mark icon to its right. At the bottom left, a legend shows an asterisk followed by the text "* Required field". At the bottom right, there are two buttons: "Cancel" and "Save".

4. Edit the ECGI record as needed and then click **Save**.
A status message appears displaying `Updating ECGI Records`.
5. (Optional) Click **Refresh** to refresh the list of ECGI record view.
6. (Optional) Click **Delete** to delete an ECGI record.

NOTE

You cannot delete an ECGI record while it is assigned to an existing Network. You must remove the record from any Networks prior to deleting it.

You have completed editing an ECGI record.

Editing Certified Professional Installer Details

To edit CPI details, follow these steps.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, click the **CPI Details** tab.

The existing CPI details such as CPI Name, CPI ID, and private key are displayed under the **CPI Details**.

3. Click **Edit**.

The **Edit CPI Details** dialog box appears.

Edit CPI Details

* CPI Name:

* CPI ID:

* CPI Certificate File: [Change](#)
P12 file

* CPI Certificate File Password:

* Required field [Cancel](#) [Save](#)

4. You can edit the following: field.
 - **CPI Name:** The name of the CPI.
 - **CPI ID:** The ID of CPI.
 - **CPI Certificate File (P12 file):** The CPI certificate file. Click **Change** to select and upload another CPI certificate file from your computer.
 - **CP Certificate File Password:** The password for the CPI file.
5. Click **Save** to save the updated CPI details.

NOTE

The CPI details are saved in the browser only. You must add the CPI details again after closing the session or reloading the page.

6. (Optional) Click **Delete** to remove the CPI details.

You have completed editing CPI details.

Configuring Bonjour Services (Wi-Fi Only)

Bonjour[®] is the Apple implementation of a zero-configuration networking protocol for Apple[®] devices over IP. It allows OS X[®] and iOS devices to locate other devices such as printers, file servers, and other clients on the same broadcast domain and use the services offered without any network configuration required.

NOTE

This Bonjour services feature is only supported in release 2016.05 and later.

Multicast applications, such as Bonjour, require special consideration when being deployed over wireless networks. Bonjour only works within a single broadcast domain, which is usually a small area. This is by design to prevent flooding a large network with multicast traffic. However, in some situations, a user may want to offer Bonjour services from one VLAN to another.

The controller's Bonjour gateway feature addresses this requirement by providing an mDNS proxy service configurable from the web interface to allow administrators to specify which types of Bonjour services can be accessed from and to which VLANs.


Creating or Editing a Bonjour Service

By default, no Bonjour services exist on all managed APs. You can create or edit a Bonjour service to define the Apple services that you want to advertise on an AP.

NOTE

To reach the **AP Bonjour Services** page described in this procedure, click **APs** on the menu, and then click an AP name. When the AP information page appears, locate the **Settings** box in the bottom-right corner of the page, and then click **Edit**. The **AP Bonjour Services** page appears.

Complete the following steps to create or edit a Bonjour service.

1. From the navigation pane, click Networking Devices and select the **WiFi** tab.
2. Click an AP name to view details about the AP.
3. In **Settings** in the bottom-right corner of the page, click **Edit**. The AP Bonjour Services page is displayed.
4. On the **AP Bonjour Services** page, complete one of the following steps:
 - To add a Bonjour service, click **+ Add Service**. The Create Bonjour Service dialog box is displayed.
 - To edit a Bonjour service, locate the service that you want to edit on the list, and then click  .

Depending on what you clicked, the **Create Bonjour Service** or **Edit Bonjour Service** dialog box appears. The Edit Bonjour Service dialog box is displayed.

5. Complete the following fields to create or edit a Bonjour service:
 - **Service Type**: Select the Bonjour service that you want to advertise on the AP.
 - **From VLAN**: Enter the VLAN ID from which the Bonjour service will be advertised.
 - **To VLAN**: Enter the VLAN ID to which the Bonjour service will be made available.
6. Click **Create** if you are adding a new Bonjour service or **Save** if you are editing one.
7. Click **OK** to close the **AP Bonjour Services** dialog box.

Enabling or Disabling a Bonjour Service

By default, Bonjour services are enabled as soon as you create them. You can disable them anytime.

Complete the following steps to enable or disable a Bonjour service.

1. From the navigation pane, click Networking Devices and select the **WiFi** tab.
2. Click an AP name to view details about the AP.
3. On the **Access Points** page, locate the AP on which you want to enable or disable a Bonjour service.
4. Click the AP name.

The **Overview** tab of the AP details page is displayed.

5. In **Settings** in the bottom-right corner of the page, click **Edit**.

NOTE

If at least one Bonjour service exists on the AP and it is currently enabled, the value for Bonjour is **Enabled**. If no Bonjour service exists or all Bonjour services are disabled, the value is **Disabled**.

The **AP Bonjour Services** page is displayed.

6. Locate the Bonjour service that you want to enable or disable.
7. Under the **Enable** column, set the switch to **ON** to enable the Bonjour service or to **OFF** to disable it.
8. Repeat the previous step for every Bonjour service that you want to enable or disable on this AP.
9. Click **OK**.

The value for Bonjour Gateway changes to **Enabled** if you set at least one Bonjour service to **ON**. If you disabled all Bonjour services on the AP, the value changes to **Disabled**.

10. Click **OK** to close the **AP Bonjour Services** page.

Viewing Existing Bonjour Services

You can open the **AP Bonjour Services** dialog box to view a summary of Bonjour services that exist on an AP.

Complete the following steps to view a list of Bonjour services that have been configured on an AP.

1. From the navigation pane, click Networking Devices and select the **WiFi** tab.
2. Click an AP name to view details about the AP.
3. On the **Access Points** page, locate the AP on which you want to view Bonjour services.
4. Click the AP name.

The **Overview** tab is displayed.

5. In **Settings** in the bottom-right corner of the page, click **Edit**.

NOTE

If at least one Bonjour service exists on the AP and it is currently enabled, the value for Bonjour is **Enabled**. If no Bonjour service exists or all Bonjour services are disabled, the value is **Disabled**.

The **AP Bonjour Services** page displays a summary of the Bonjour services that exist on the AP, including the name of the services that have been defined on the AP, the source and target VLAN IDs, and whether they are currently enabled or disabled.

Deleting a Bonjour Service

If you are no longer using a particular Bonjour service on an AP, you can delete the service.

Complete the following steps to delete a Bonjour service.

1. From the navigation pane, click Networking Devices and select the **WiFi** tab.
2. Click an AP name to view details about the AP.
3. On the **Access Points** page, locate the AP on which you want to view Bonjour services.
4. Click the AP name.

The **Overview** tab of the AP information page is displayed.

5. In **Settings** in the bottom-right corner of the page, click **Edit**.

The **AP Bonjour Services** page displays a summary of the Bonjour services that exist on the AP, including the name of the services that have been defined on the AP, the source and target VLAN IDs, and whether they are currently enabled or disabled.

6. Locate the Bonjour service that you want to delete.
7. Click X in the same row as the Bonjour service that you want to delete.

A confirmation message is displayed.

8. Click **Yes**.

Downloading the AP Logs

An AP log contains information such as the AP system, configurations, and the AP runtime status, which are useful for troubleshooting. When you request for technical support, Ruckus asks you to download and share the AP log for analysis.

Follow these steps to download the AP log.

1. On the Dashboard, click **APs**.

The **Access Points** page appears.

2. Click the name of the AP from which you want to download the AP log.

The Access Points **Overview** page appears.

3. In the bottom right corner of the page, under **Actions**, click **Generate new log**.

Ruckus LTE AP Management generates a log and uploads it to Google Cloud. A new icon for downloading the log appears next to the **Last Log** timestamp.

NOTE

This action is asynchronous. You must wait until an updated download link appears.

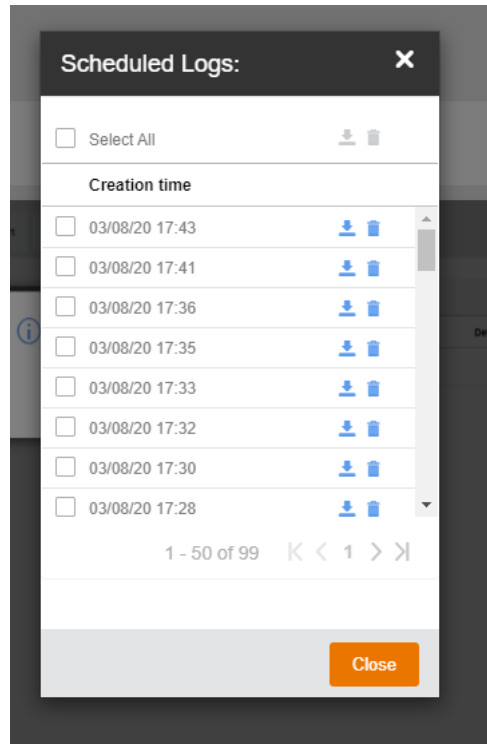
A progress bar appears while your web browser downloads the AP log to its default download location. When the download progress bar disappears, go to your default download location and locate the log file, which is named similar to this:

RSC_Logs_xxx_2018_11_29T08_31_43.tar. Use the Linux shell to decompress and review the contents of the AP log file. In general, an AP log contains AP system message files, as shown in the following example.

```
4631894 2018-12-04 12:32 var/log/messages
9500066 2018-12-04 12:29 var/log/messages.prev
9500571 2018-12-04 12:23 var/log/messages.prev1
9500524 2018-12-04 12:15 var/log/messages.prev2
```

To view scheduled logs, log in to the support portal as a tenant.

4. From the **Support** page, select a **Customer Accounts**, and then choose an AP.



The **Scheduled Logs** dialog appears.

5. Click the download icon to download a log or click the delete icon to delete a log.

You have completed downloading the AP log.

Turning AP LEDs ON/OFF

You can choose to turn the LEDs of a connected and operational AP ON or OFF.

To turn on or off AP LEDs, follow these steps.

1. From the navigation pane, click **APs** to navigate to the **Access Points** page.

- Click an AP name to view details about the AP.

The **Overview** page of the AP appears. Under the **AP Properties** section, you can see the status of the AP LEDs. You can click **More** to expand the **AP Properties** to view the status of the AP LEDs. By default, the AP LEDs are set to ON. You can also configure the AP LEDs at the Venue level. The AP LEDs status is displayed as **Same As Venue**, if the default value of the associated venue is inherited by the AP. If the AP LEDs setting is different from the venue the AP is associated with, the **AP LEDs** status is displayed as **Customized**.

FIGURE 23 Access Points Overview

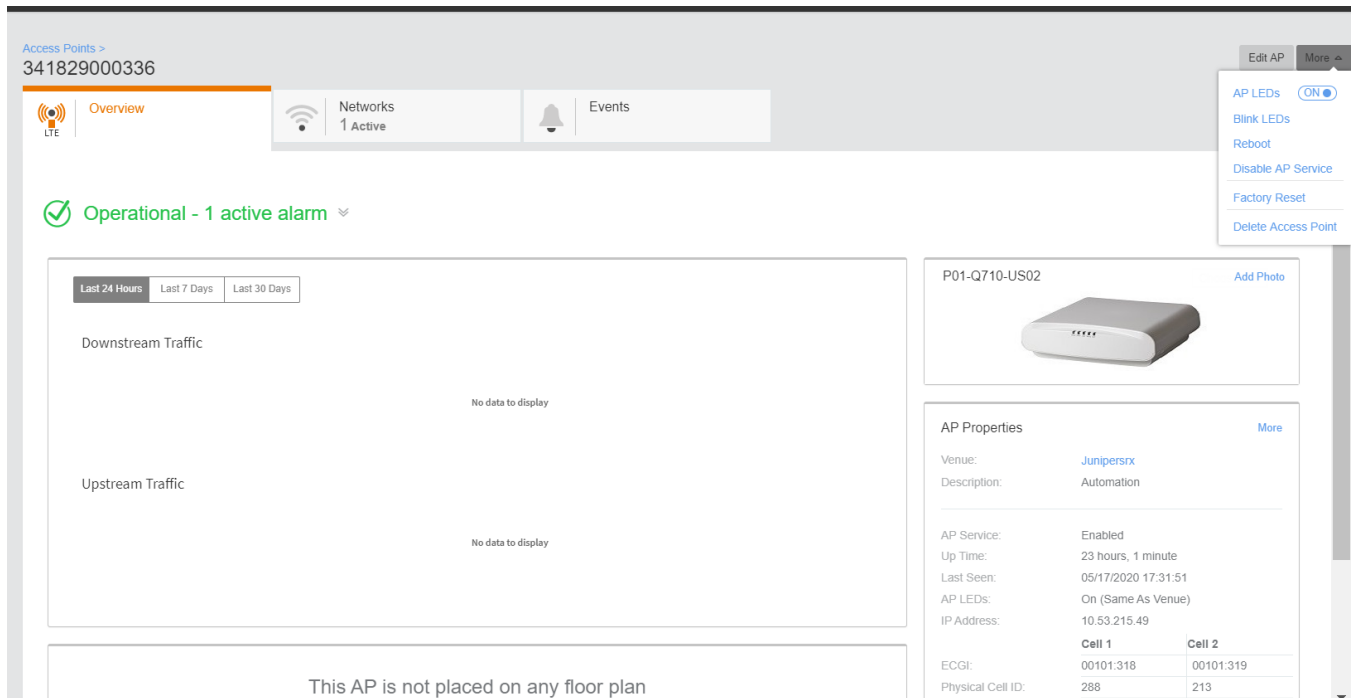
The screenshot displays the 'Access Points Overview' page for a specific AP. The interface includes a navigation bar with 'Overview', 'Networks', and 'Events' tabs. The main content area is divided into several sections:

- Traffic Monitoring:** Two charts for 'Downstream Traffic' and 'Upstream Traffic' are shown, both with 'No data to display' messages. Filter buttons for 'Last 24 Hours', 'Last 7 Days', and 'Last 30 Days' are present.
- AP Device:** A photo of the AP model P01-Q710-US02 is displayed with an 'Add Photo' link.
- AP Properties:** A detailed section showing:
 - Venue: Junipersx
 - Description: Automation
 - AP Service: Enabled
 - Up Time: 22 hours, 51 minutes
 - Last Seen: 05/17/2020 17:21:55
 - AP LEDs: On (Same As Venue)
 - IP Address: 10.53.215.49
- Cellular Information:** A table showing details for two cells:

	Cell 1	Cell 2
ECGI:	00101:318	00101:319
Physical Cell ID:	288	213
EIRP In-use:	28.79 dBm	28.79 dBm
Channel:	56340 EARFCN	56540 EARFCN
- Floor Plan:** A message states 'This AP is not placed on any floor plan' with a link to 'Go to floor plans to place the AP'.

- From the upper-right corner of the AP **Overview** page, click **More** to access the AP LEDs configuration option.
A drop-down menu appears.

FIGURE 24 AP Settings

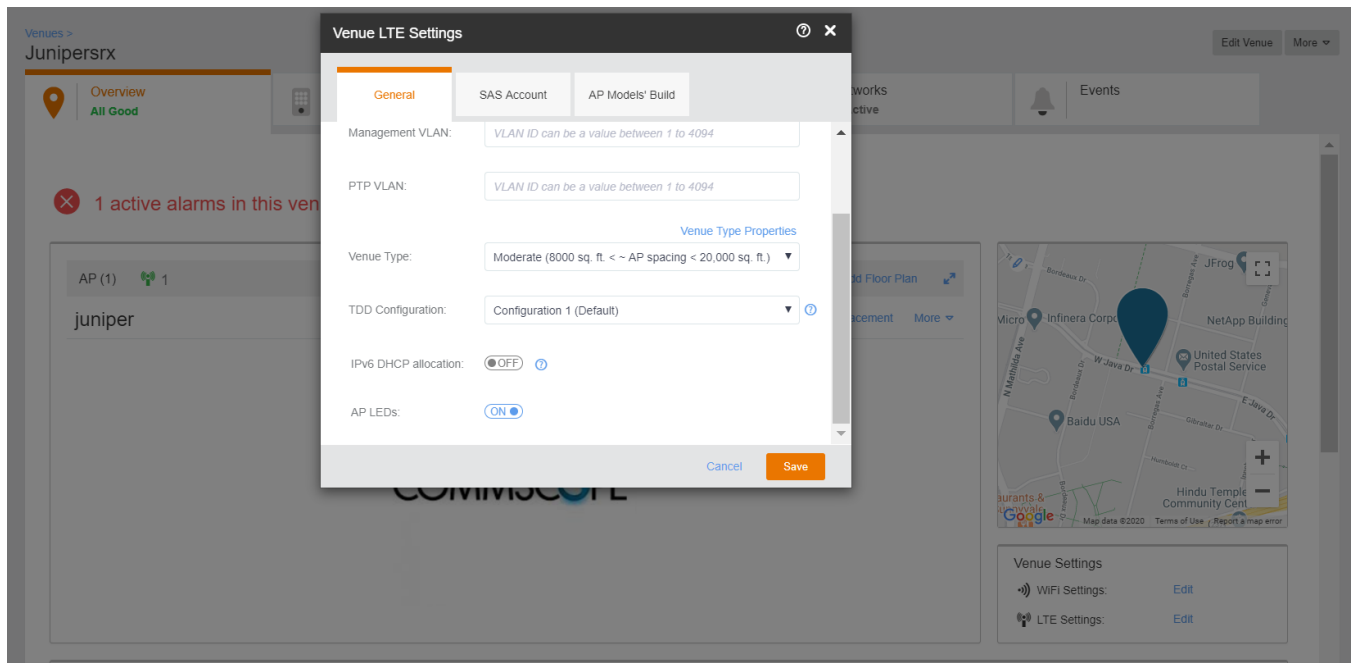


- Toggle the **AP LEDs** to **ON** or **OFF**.
A progress bar appears displaying updating access point and then it displays the turning AP LEDS off or on was successful .
- Alternatively, from the navigation pane, click **Venues** to navigate to the **Venues** page.
- Select the **Venue** for which you want to configure the AP LEDs settings.
The venue **Overview** page appears

7. From the bottom-right corner click **Edit** for **LTE Settings**.

The **Venue LTE Settings** dialog appears.

FIGURE 25 Venue LTE Settings



8. In the **General** tab, toggle the **AP LEDs** to **ON** or **OFF**.
9. Click **Save**.

A progress bar appears displaying

Updating LTE Settings...

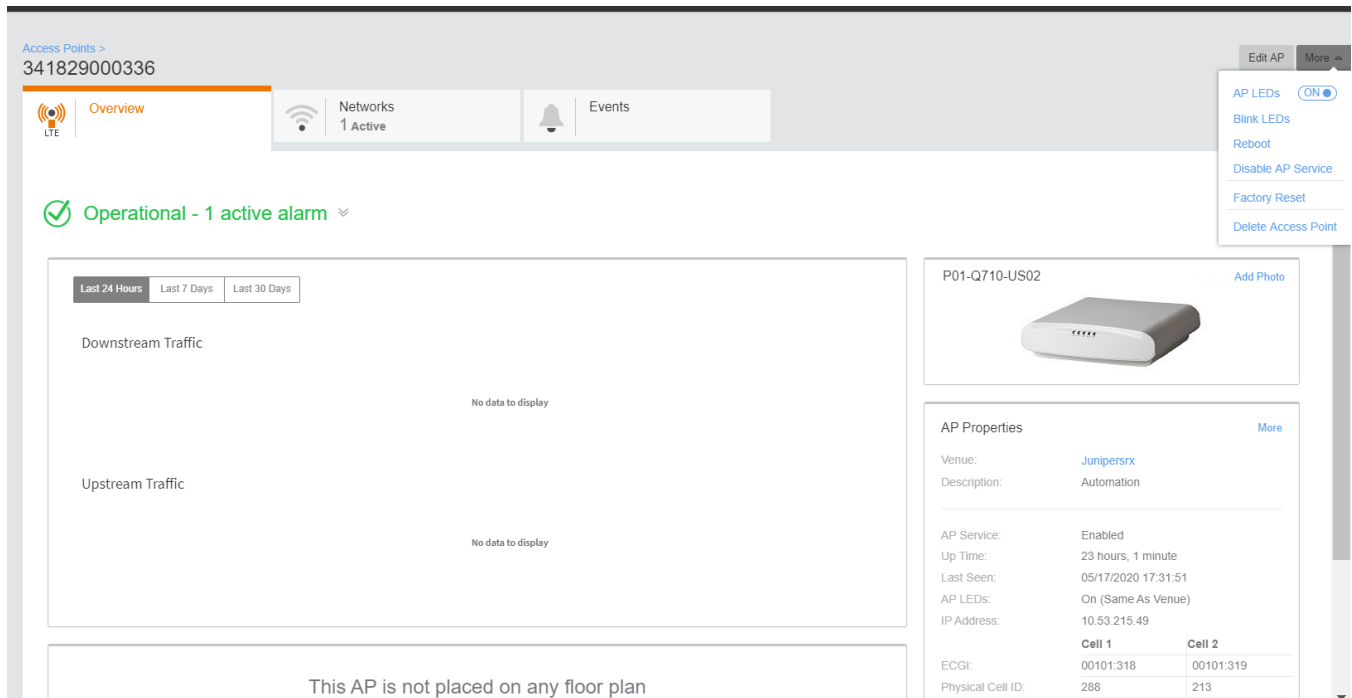
Blink AP LEDs

To blink the AP LEDs, follow these steps.

1. From the navigation pane, click **APs** to navigate to the **Access Points** page.
2. Click an AP name that you want to blink.

- From the upper-right corner of the AP Overview page, click **More** to access the **Blink LEDs** option.
A drop-down menu appears.

FIGURE 26 Blink LEDs



- Click **Blink LEDs**.
The AP will blink for 30 seconds.

Rebooting an AP

Complete the following steps to reboot an AP.



DANGER

Rebooting an AP temporarily turns off any active networks that the AP is providing and disconnects wireless clients that are connected to these networks.

- From the navigation pane, click **Networking Devices** and select the **WiFi** tab.
- Click an AP name to view details about the AP.
- Click the name of the AP that you want to reboot.
The AP information page is displayed.
- In the upper-right corner of the page, click **Manage** to display a menu, and click **Reboot**.
A confirmation message is displayed.

5. Click **Reboot Access Point**.

A message displays the result of the reboot attempt. The following example of the message is displayed after a successful reboot attempt:

```
Successfully rebooted Access Point 'AP-1'.
```

If the AP is still in the process of rebooting, the AP status (only for Wi-Fi) shows AP rebooting on the **APs** page. The reboot process might take several minutes. After a reboot, the AP status shows Operational.

Resetting an AP to Factory Defaults

Reset an AP to remove all configurations and revert to factory default settings.

To erase all configurations on the AP, follow these steps.



WARNING

When you reset an AP, all settings on the AP including networks are currently providing LTE or Wi-Fi service to users in your venues get erased.

1. On the Dashboard, click **APs**.
The **Access Points** page appears.
2. From the access point list, click the name of the AP that you want to reset to factory defaults.
The AP information page appears.
3. In the upper-right corner of the page, click **More** to display a menu, and then click **Factory Reset**.
A confirmation message appears.
4. Click **Yes**.

You have completed resetting the AP to its factory default settings.

NOTE

Factory Reset is executed asynchronously, when AP is connected to the LTE AP Management Service. After the factory reset, the status of the AP is updated from **Operational** to **Connected**.

Disabling or Enabling AP Service

You can disable and enable service of connected and certified APs and operational APs.

To disable AP service, follow these steps.

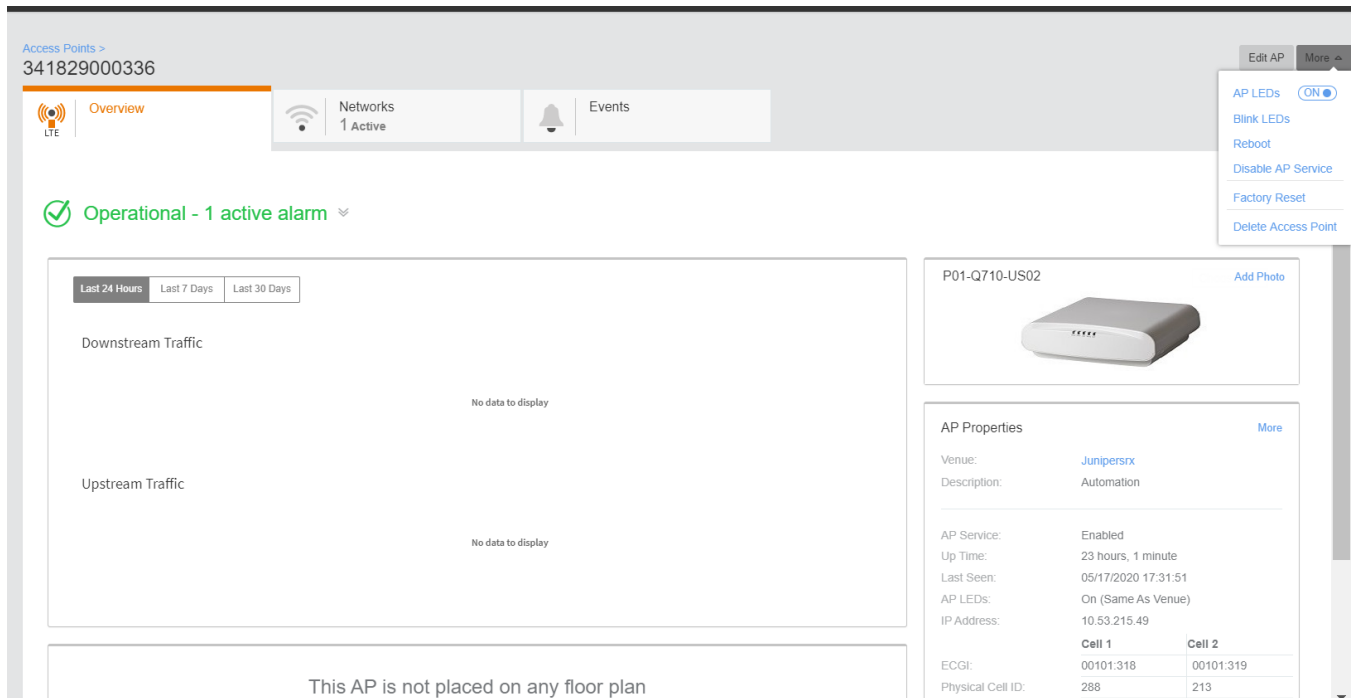
1. From the navigation pane, click **APs** to navigate to the **Access Points** page.
2. Click an AP name that you want to disable or enable service.

Managing Network Devices: APs

Deleting an AP from Ruckus LTE AP Management

- From the upper-right corner of the AP **Overview** page, click **More** to access the **Disable AP Service** option.
A drop-down menu appears.

FIGURE 27 Disabling AP Service



- Click **Disable AP Service** to disable service of an operational AP.
A status bar appears displaying Updating access point.
- Click **Enable AP Service** to enable service of an AP, which service was disabled.
A status bar appears displaying Updating access point.

Deleting an AP from Ruckus LTE AP Management

Delete an AP to remove it from your Ruckus LTE AP Management account .

To delete an AP from Ruckus LTE AP Management, follow these steps.

- On the Dashboard, click **APs**.
The **Access Points** page appears.
- Click the name of the AP that you want to delete.
The AP information page appears.
- In the upper-right corner of the page, click **More** to display a menu, and then click **Delete Access Point**.
A confirmation message appears.

4. Click **Yes**.

NOTE

Deleting an AP will reset the AP to its factory defaults (configuration and firmware version).

You have completed deleting the AP from your AP Management account. If you want to add it back, follow the steps in [Adding an AP](#) on page 53.

Managing Wi-Fi Networks

- [LTE Networks in Ruckus LTE AP Management.....](#) 87
- [Wi-Fi Networks in Ruckus LTE AP Management.....](#) 96

LTE Networks in Ruckus LTE AP Management

The AP Management supports two network standards—LTE and Wi-Fi (demo only).

On the Dashboard, click **Networks** to view existing networks and create your LTE or Wi-Fi network.

LTE Network

Long Term Evolution (LTE) is a 4G wireless communications standard developed by the 3rd Generation Partnership Project (3GPP) and is designed to provide up to ten times the speeds of 3G networks for mobile devices.

Adding and configuring an LTE network on the Ruckus LTE AP Management provides LTE APs with details on how to connect to an Evolved Packet Core (EPC) network and provides LTE service.

It is highly recommended that Network configuration is done with consultation of the EPC provider as many fields need to be obtained after prior discussions with the provider.

Creating an LTE Network

The CBRS Alliance has provided detailed guidelines for computing a unique E-UTRAN Cell Global Identifier (ECGI) per CBSD to all CBSD (LTE AP) vendors.

You are presented with following two options:

- WiFi Network

Managing Wi-Fi Networks

LTE Networks in Ruckus LTE AP Management

- LTE Network

1. Click **LTE Network**.

The **Create New LTE Network** page appears to allow you to complete the settings on the **Network Details** tab.

Create New LTE Network

1 Network Details 2 Venues

* Name: Emirates

* PLMN ID (Primary): 3150 [Add Secondary PLMN ID](#)

* Tracking Area Code: 971

* ECGI Records: Using default PLMN ID 315010 requires defining ECGI Records. Please [add an ECGI record](#) for PLMN ID 315010 or use a different PLMN ID ?

* MME: FE80::5EFE:192.168.1.000 [Add Another MME](#)
IPv4, IPv6 or FQDN Format

* LTE Security Gateway: ON

Disable IPv6 inside IPv4 tunnel allocation (security gateway only)

* Security Gateway: FE80::5EFE:192.168.1.123 [Add Another SecGW](#)
IPv4, IPv6 or FQDN Format

PKI OFF

* Physical Cell ID: From: 1 To: 123
Range between 0 to 503

EPC VLAN:

* Required field [Cancel](#) [Next](#)

2. In the **Name** field, enter a name that you want to assign to the LTE network.

- By default, the shared CBRS-A PLMN ID, 315010 is populated in the PLMN ID field. The **PLMN ID** can be overwritten with any other valid PLMNID, if desired.

A PLMN is identified by the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Each operator that provides mobile services has its own unique PLMN ID.

NOTE

According to the CBRS-A guidelines, to create a new CBRS Network using the shared PLMN ID (315010), all operators must purchase "Macro eNB ID" from the Alliance. For more information, refer to [Adding ECGI Records](#) on page 54.

Configure the Macro eNB IDs and PLMN ID to create globally unique ECGI records/ range that can be assigned to Cells coming up within the network.

If the PLMN ID used is not the shared CBRS PLMN ID, operators have two options as elaborated below. For more information, visit: <http://imsiadmin.com> and <http://atis.org/ioc>.

- Click **Add Secondary PLMN ID** to add a secondary PLMN ID. Optionally, click **Add Another PLMN ID** to add an another PLMN ID.

You can add up to six secondary PLMN IDs.

- Enter the tracking area code in the **Tracking Area Code** field.
- In the **ECGI Records** drop-down, select a desired record and click **OK**.

The number of available ECGI records are displayed in the **Available ECGI** field.

- (Optional) Click **+Add ECGI Record** to add a new ECGI record.

Add ECGI Record ⓘ ✕

* Name:

* PLMN ID: ⓘ

* Macro eNB ID: ⓘ

Note: To view and manage all PLMN IDs ECGI records, you can use 'ECGI Records' tab in the [administration area](#).

* Required field Cancel Save

- In the **MME** section, enter the address of the Mobility Management Entity (MME).
The address can be an IPv4, IPv6, or a Fully Qualified Domain Name (FQDN). The MME is the key control-node for the LTE network access. It works with the LTE AP (eNodeB) and Serving Gateway (SGW) within the Evolved Packet Core (EPC) and is responsible for initiating paging and authentication of the mobile device. You can configure multiple MME control points.

To add more than one MME IP control points, click **Add another MME** link and enter the MME IP address or FQDN (domain name) in the additional field that appears. Click the **Remove MME** link that appears adjacent to each MME added, to remove an MME IP.

9. In the **LTE Security Gateway** section, click the toggle button to enable or disable the Security Gateway (SecGW).

The SecGW protects network elements and secure communication links across the LTE network by providing traffic encryption between LTE APs and EPC. It authenticates network elements to avoid a rogue LTE AP connecting to the network. It manages and controls traffic delivered to avoid network downtime.

NOTE

Confirm the SecGW availability and connection details with your EPC vendor.

Contact Ruckus Support to upload root certificates for your SecGW using this menu.

10. Check the **Disable IPv6 inside IPv4 tunnel allocation (security gateway only)** check box if you want to disable IPv6 inside IPv4 tunnel allocation.

By default, this option is enabled.

11. Complete the following Security Gateway settings which are presented to you when you enable the LTE Security Gateway.

- In the **Security Gateway** section, enter the IPV4 address, IPv6, or FQDN of the SceGW, in the field provided. You can add multiple SceGW by clicking **Add Another SecGW** link.
- In the **PKI** section, click the toggle button to enable the PKI. You are now provided with fields to enter CMP server URL and the CA.
- In the optional **CPM server URL** section, select the check box and enter the URL to connect to the CPM Server using the HTTPS protocol. When a CPM server boots for the first time, it will automatically create a self-signed SSL certificate.
- In the optional **Certificate Authority** section, select the check box and enter the repository URL, user name, password and the URL Hash in the respective text fields provided.
 - (mandatory) Repository URL: Enter the URL of the Web server that hosts the CA.
 - (optional) User Name: The user name to access the Web Server.
 - (optional) Password: The password to access the Web Server.
 - (mandatory) URL Hash: Enter the 64 hex character certificate hash.
- In the **Tracking Area Code** section, enter the unique Tracking Area Code (TAC) assigned to the LTE tracking area (TA), which helps in identifying the UE location. When an LTE device (UE) is in active state, its location is known by the LTE network at the LTE AP level. However, when the UE is in idle state, its location is known by the LTE network at TA level. An operator defines a group of neighboring LTE APs as a TA. Each TA has a Tracking Area Identifier (TAI). A TAI consists of a PLMN ID and a TAC. A PLMN ID is a combination of a Mobile Country Code (MCC) and a Mobile Network Code (MNC), which is the unique code assigned to each operator
- In the **Physical Cell ID** section, enter the physical layer cell ID (PCI) range. The physical cell ID identifies a network cell in the physical layer. This property is limited to 504 values ranging from 0 through 503; and therefore, it needs to be reused in the network. SON will allocate PCIs with optimal separation between neighbor Cells; however, ensure that enough range is provided. The physical cell ID of each AP should differ from physical cell ID of its neighbors. The tenant must ensure that enough range is provided for the correct distribution.
- **EPC VLAN:** This is an optional field. You can leave it blank unless specific VLAN requirements are provided by your IT.

12. Check the **Enable Crypto Profile** check box, click **Profile Settings** and complete the profile setting, and then click **OK**.

13. (Optional) Enter remote ID in the the **Remote ID** field.

14. Toggle the **PKI** button to **ON** or **OFF**.

Complete the following:

- CMP server URL
- CMP v2 SecGW
- Certificate Authority

Configure the Repository URL. Enter the user name and password

Enter the Certificate Hash.

15. Configure the **Physical Cell ID**. The valid range for physical cell ID is from 0 through 503

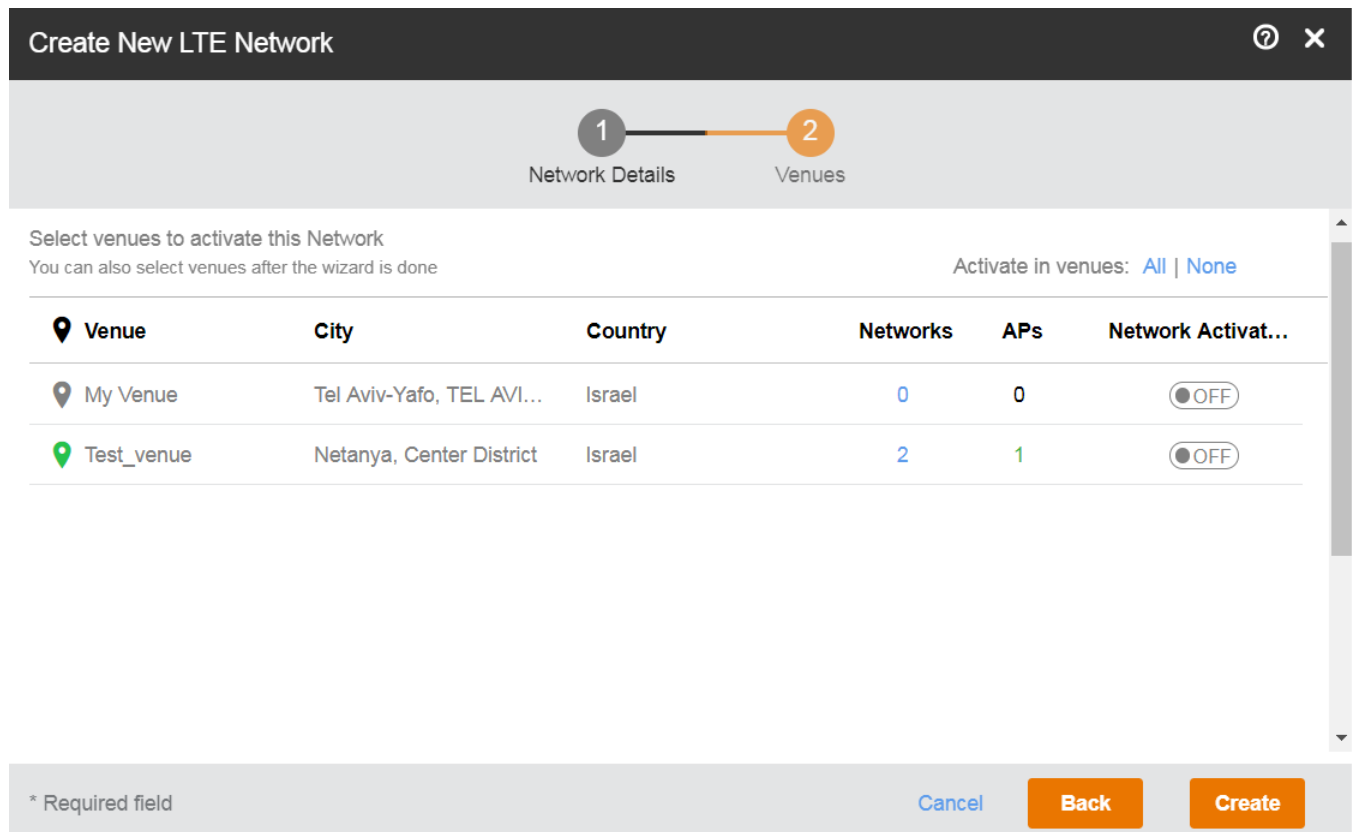
16. Click the **Next** button to navigate to the **Venues** tab. The **Venues** tab allows you to select venues in which you want to activate the network.

Venues are displayed in the tabular format as displayed in following figure. Each row displays venue details such as City, Country and the number of Networks, APs, and clients. For the venues which have networks and APs configured, the flag against them appears in green, and for the ones without any configuration, the flags are grayed out. Pause the mouse pointer over the green flag prompts you that the venue is *All good*. Pause the mouse pointer over the grayed out flag prompts you that the venue is *In setup phase*.

NOTE

You can skip this step and choose to select venues after the LTE network is created.

FIGURE 28 Selecting Venues



17. Click the toggle button available in the **Network Activation** column to activate the desired venue.

NOTE

If the venue already has an activated LTE network, you are prompted with a dialog box, stating that the venue already has an activated LTE network. If you want to deactivate the existing one and activate the new LTE which you are creating, click **Activate Network** to continue.

You can choose to activate your LTE network in all the venues by clicking the **All** button available on top of the **Network Activation** column. If any of the venues has an already activated LTE network, you are prompted with a dialog box stating that the venues already has an activated LTE network. If you want to deactivate the already active LTE network and activate the one which you are creating, click the **Activate Network** button to continue. You can choose to not activate your LTE network in any of the venues by clicking the **None** button on top of the **Network Activation** column.

18. The number of networks configured in any venue is listed under the **Networks** column. Pause the mouse over the number to display other networks activated in that venue. Click to display the corresponding venue details page where you can change the already existing configuration, before proceeding to create your LTE network.
19. The number of APs configured in any venue is listed under the **APs** column. Pause the mouse over the number to display the configured APs in that venue. Click to display the corresponding AP details page where you can change the already existing configuration, before proceeding to create your LTE network.
20. After completing all the required configurations for your LTE network, click the **Create** button. A dialog box prompts you that your network is being activated. If the process is successful, you are navigated to the **Networks** page, where your newly created LTE network is listed.

Viewing LTE Network (EPC) details

View more information about a network, including a summary its settings, a diversity chart of its wireless clients, and volume of the wireless traffic that it has handled.

Follow these steps to view detailed information about a network.

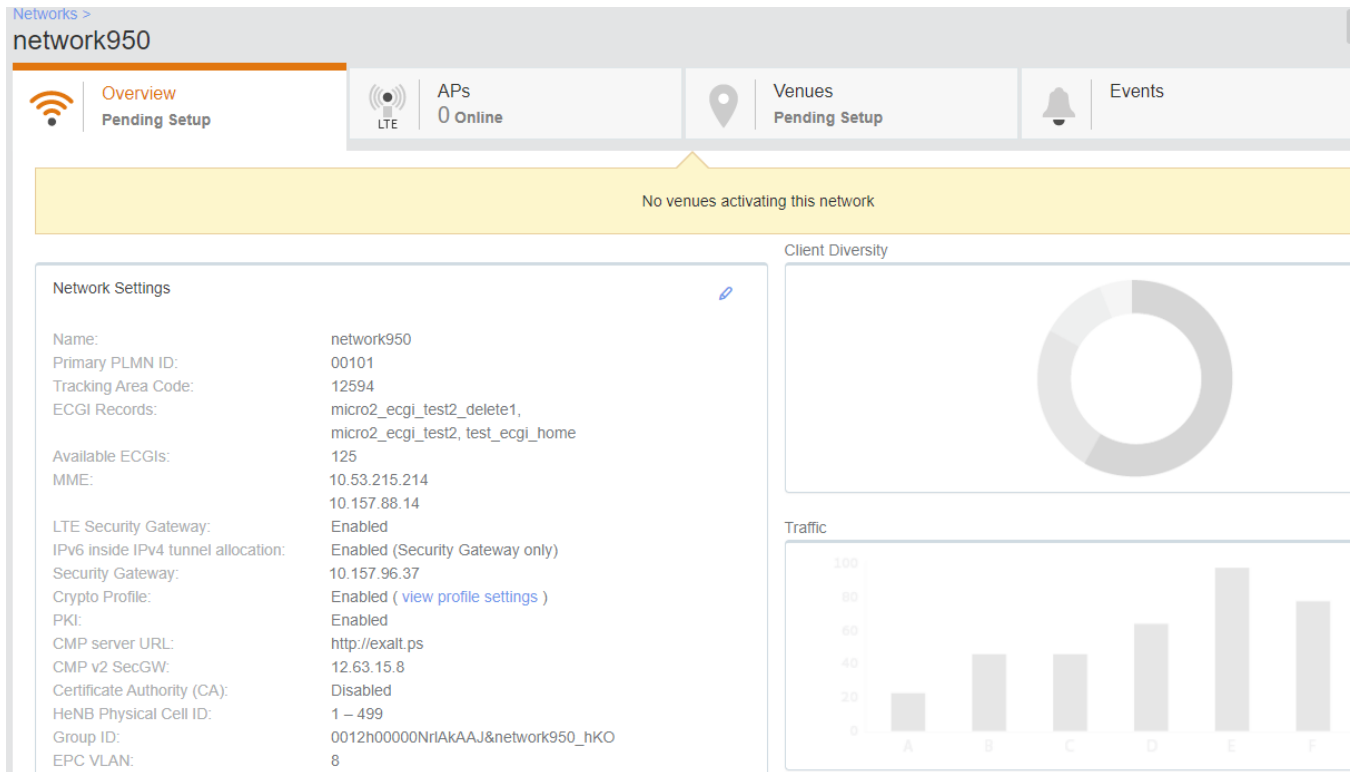
1. On the Dashboard, click **Networks**.

The **Networks** page appears displaying a list of network that you previously created.

- Click the name of the network for which you want to view detailed information.

The **Overview** tab of the network information page appears and displays the following information:

FIGURE 29 Network Overview



- **Network Overview:** Displays a summary of the network properties, including the network name, PLMN ID, ECGI records, available ECGIs, MME, LTE Security Gateway, tracking area code, HeNB physical cell ID, and group ID. To know more about configuring each of the properties, refer to [Creating an LTE Network](#) on page 87. A chart view of the client summary and traffic is displayed on the right side of the page.
- **APs:** Lists all the APs which are providing network services, along with the status (for example, Operational). In addition, it shows other AP properties such as Model, IP Address, Identifier, Venue, Timing Role, Timing Sync Status, and Tags. A venue pinned with a green label shows that the venue functioning status is good. To know more about configuring each of the AP properties, refer to [Managing Network Devices: APs](#) on page 53.
- **Venues:** This section list all the venues that are using the network (Active and in setup state), along with the city, country and the networks and APs (Active and in setup state). You can activate the network using the toggle button available in each row. To know more about configuring each of the Venue properties, refer to [Viewing Venue Information](#) on page 42.
- **Events:** Displays the events that occurred in the network within the last 24 hours. For more information on events , refer to [Event Types](#) on page 159.

Viewing LTE APs that are provisioned on a LTE Network (EPC)

From the **APs** tab on the **Networks** page, you can view information about LTE APs that are providing a particular network.

To view the list of APs that are providing a particular network, follow these steps.

1. On the Dashboard, click **Networks**.

The **Networks** page appears.

2. From the list of networks, click the name of the network that you want to view.

The network information page appears and displays the **Overview** tab.

3. Click the **APs** tab.

The page refreshes and then **APs** tab displays a list of APs that are currently providing the network service, including the following information:

- **AP**—The name of the AP.
- **Status**—The status of AP. If everything is operating normally, the **Status** column shows **Operational**.
- **Model**—The hardware model of the AP.
- **IP Address**—The IP address or the serial number of the AP.
- **MAC address**—The MAC address of the AP.
- **Venue**—The name of the venue in which is this AP is physically deployed.
- **Clients**—The length of time that the wireless client has been associated with the network.
- **Tags**—The tags that have been assigned to this network.

You have completed viewing the APs that are currently providing this network.

Viewing Venues That Are Advertising a Network

Use the **Venues** tab on the **Networks** page to view information about venues are advertising a particular network.

Follow these steps to view a list of venues that are advertising a particular network.

1. On the Dashboard, click **Networks**.

The **Networks** page appears.

2. From the network list, click the name of the network that you want to check.

The network information page appears and displays the **Overview** tab.

3. Click the **Venues** tab.

The page refreshes and then **Venues** tab displays a list of all existing venues in your Ruckus LTE AP Management Service account.

4. View the **Network Activated** column. Venues that are showing **ON** indicate that venues in which this network is being advertised.

You have completed viewing the venues that are currently advertising this network.

Viewing Events That Have Occurred on a Network

Use the **Events** tab on the **Networks** page to view events that have occurred on a network in the last 24 hours.

Follow these steps to view a list of events that have occurred on a network.

1. On the Dashboard, click **Networks**.

The **Networks** page appears.

2. From the network list, click the name of the network that you want to check.

The network information page appears and displays the **Overview** tab.

3. Click the **Events** tab.

The page refreshes and then **Events** tab displays a list of events that have occurred within the last 24 hours. For each event the following information is displayed:

- **Date:** The date and time when the event occurred.
- **Severity:** The severity level of the event. For information on what each severity level means, refer to [Event Severity Levels](#) on page 159.
- **Event Type:** The component that generated the event. Possible values include **Admin**, **AP** (for example, an AP was rebooted), **Client** (for example, a user left the network), and **Notification**.
- **Source:** The MAC address of the client on which the event occurred.
- **Identifier:** The MAC address of the AP to which the client was connected when the event occurred.
- **Model:** The AP model.
- **Description:** A brief description of the event.

You have completed viewing the event that have occurred on this network.

Editing an LTE Network

Edit a network if you need to update any its current settings (for example, if you want to change the network name, network type, security method, or even the venue at which it is advertised.)

Follow these steps to edit a network.

1. On the menu, click **Networks**.

The **Networks** page appears.

2. From the network list, click the LTE network that you want to edit.

The network information page appears.

3. In the upper-right corner of the page, click **Edit Network**.

The **Network Details** and **Venue** tab is displayed where you can update settings as required.

- **Network Details:** Displays the network configuration data in editable format. To understand the various configuration fields for LTE network and update the fields, refer to the [Creating an LTE Network](#) on page 87.
- **Venue:** Displays the venues which uses the network. You can use the toggle button at the end of each row to activate or de-activate the venue. Venue names which are pinned in green are accessed to be in good condition. Venues pinned in gray are in set-up stage.

4. Click **Save**.

You have completed editing a network.

Deleting a Network

If you no longer need a network that you previously created, you can delete it.

Follow these steps to delete a network from your Ruckus Cloud account.

1. From the navigation pane, click **Networks**.

The **Networks** page is displayed.

Managing Wi-Fi Networks

Wi-Fi Networks in Ruckus LTE AP Management

2. From the network list, click the name of the network that you want to delete.

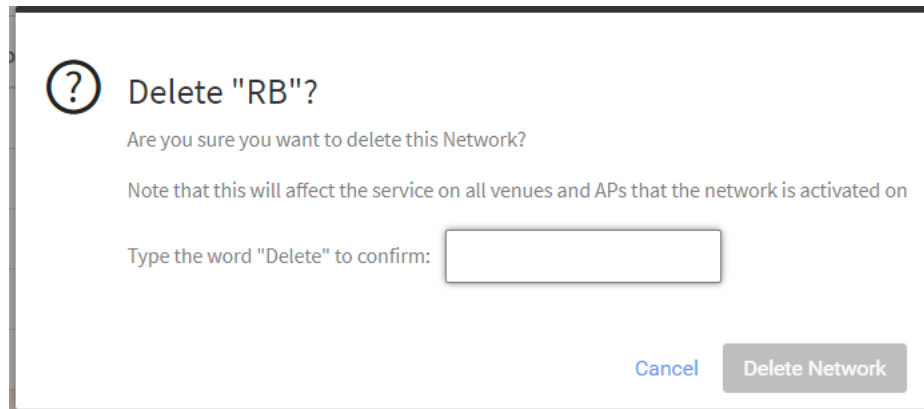
The network information page displayed displays the number of networks selected, **Edit** and **Delete** options. Click **Delete** to delete the network.

3. Alternatively, in the upper-right corner of the page, click **Manage** to display a menu, and then click **Delete Network**.

Deleting this network will stop service to the following entities currently using this Network.

A confirmation message is displayed.

FIGURE 30 Deleting a Network



4. Enter **Delete** in the dialog box and click **Delete Network**.

If you want to add the network back, follow the steps in [Creating Networks Overview](#) on page 96.

Wi-Fi Networks in Ruckus LTE AP Management

The AP Management supports two network standards—Wi-Fi and LTE.

On the Dashboard, click **Networks** to view existing networks and create your Wi-Fi or LTE network.

Creating Networks Overview

Before you can offer wireless services in your venue, you must create at least one wireless network.

The procedure for creating a network depends on the type of wireless network that you want to create and the authentication method that you want users to use to join the network.

Ruckus Cloud supports the following authentication methods:

- **Pre-Shared Key:** Requires users to enter the passphrase (that you have defined for the network) to connect to Ruckus Cloud. Refer to [Creating a Network That Uses a Pre-Shared Key](#) on page 97.
- **Enterprise AAA:** Uses the 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network. This authentication method requires an AAA server on the network. See [Creating a Network That Uses an Enterprise AAA Server](#) on page 106.
- **Cloudpath:** Uses an authentication server and Cloudpath onboarding to authenticate users. See [Creating a Network That Uses Cloudpath Onboarding](#) on page 110.

- **Captive Portal:** Uses a third-party captive portal and authentication service to authenticate users. There are five methods that can be used to gain access through the captive portal:
 - **Click-Through:** Allows users to accept terms and conditions to access the network. Refer to [Creating a Network That Uses a Captive Portal with Click-Through](#) on page 114.
 - **Self Sign In:** Allows users to access the network temporarily using a social media account, or register their details and get a personal password. Refer to [Creating a Network That Uses a Captive Portal with Self Sign In](#) on page 118.
 - **Host Approval:** Allows users to register their details in the portal including their host email. A host must approve the guest request to provide the temporary network credentials to the guest user. Refer to [Creating a Network That Uses a Captive Portal with Host Approval](#) on page 126.
 - **Guest Pass:** Allows users to access the network temporarily using a personal password which they receive in advance from the network administration staff. See [Creating a Network That Uses a Captive Portal with a Guest Pass](#) on page 131.
 - **Third-Party Captive Portal (WISPr):** Allows users to access the network through a third-party captive portal, authenticated by a RADIUS server. Refer to [#unique_107](#).
- **Open(not recommended):** Allows users to access the network without any authentication. Refer to [Creating an Open Network \(No Authentication\)](#) on page 135.

Supported Network Types

Ruckus Cloud supports many network types that you can deploy to your venue.

Network types supported by Ruckus Cloud range from networks that are typically deployed in enterprise or office environments in addition to networks that are typically deployed in public places (such as coffee shops, libraries, airports, hotels, and so on) where there is a high, but temporary, number of network users. Ruckus Cloud supports the following authentication methods:

- **Pre-Shared Key (PSK):** Require users to enter the passphrase (that you have defined for the network) to connect.
- **Dynamic Pre-Shared Key (DPSK):** A unique passphrase is dynamically created for each user to connect to the network.
- **Enterprise AAA:** Use 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network.
- **Cloudpath:** Use an authentication server and Cloudpath onboarding to authenticate users.
- **Captive Portal:** Use a third party captive portal and authentication service to authenticate users. There are five methods that allow users to gain access through the captive portal:
 - **Click-Through:** Allow users to accept Terms and Conditions to access the network.
 - **Self Sign In:** Allow users to access the network temporarily using their social media account, or register their details and get a personal password.
 - **Host Approval:** Allow users to register their details in the portal including their host email. A host must approve the guest request in order to provide the temporary network credentials to the guest user.
 - **Guest Pass:** Allow users to access the network temporarily using a personal password which they receive in advance from the network administration staff.
 - **3rd Party Captive Portal (WISPr):** Allow users to access the network through a 3rd party captive portal, authenticated by a RADIUS server.
- **Open Network** (not recommended): Allow users to access the network without any authentication .

Creating a Network That Uses a Pre-Shared Key

You can create a network that requires users to enter a pre-shared key (PSK).

Complete the following steps to create a PSK-protected network.

1. From the navigation pane, click **Networks**.

Managing Wi-Fi Networks

Wi-Fi Networks in Ruckus LTE AP Management

2. Click **Add Network**.

The **Add Network** dialog box is displayed.

3. Complete the settings on the **Network Details** page.

- **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
- **Description:** Enter a description (up to 64 characters) to help you identify the network using.
- **Network Type:** Click **Pre-Shared Key**.

When the network type is selected, a structure diagram of a PSK type of network displays.

4. Click **Next**.

The **PSK Settings** page is displayed.

5. Complete the settings on the **PSK Settings** page.

- **Passphrase:** Enter a passphrase that you want users to provide before they can access the network.
- **SAE Passphrase:** Enter a SAE passphrase that you want users to provide before they can access the network. This option is available only when the security protocol is **WPA3** or **WPA3/WPA2 mixed mode**.
- **Security Protocol:** Select the security protocol that you want this network to use. The default security protocol is WPA2, Other options include WPA, WPA3, WPA3/WPA3 mixed mode, and WEP.

6. Click **Next**.

The **Venues** page is displayed.

7. Select the venues in which you want to activate this network:

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the **Activated column**.
- The **Select APs on venue *venue-name*** page is displayed.

8. In the **Select APs on venue *venue-name*** page, you have two choices for defining how the network will be activated:

- Click the **All APs** button to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the **Select specific AP groups** button to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. The **APs not assigned to any group** option is displayed. After **APs not assigned to any group** is selected, two more options are displayed:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

9. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

10. Click **OK**.

Returns to **Add Network** dialog box.

11. Click **Next**.

The **Summary** page is displayed.

12. Review the settings that you configured. To display the passphrase in plain text, click the eye icon.

Managing Wi-Fi Networks

Wi-Fi Networks in Ruckus LTE AP Management

13. Select the **Advanced** tab.

The **Advance** tab is displayed.

FIGURE 31 Advance Network Settings

? ✕

Network Details

PSK Settings

Venues

Advanced

*** VLAN ID:**

Load control

Max rate:

Max clients per radio:

Enable load balancing between 2.4GHz & 5GHz radios

Enable load balancing between APs

Access control

Device Connection Policy: [Set up a policy](#)

Traffic Policy: [Set up a policy](#)

Device & OS Access Policy: OFF

Wi-Fi Calling: ON [Select Profiles](#)

Selected Profile	Description	QoS Priority
Verizon		Voice

Enable Client Isolation ?

Force DHCP ?

Hide SSID ?

Enable logging client data to external syslog

Enable OFDM only (Disables 802.11b) ?

BSS Min Rate:

Mgmt Tx Rate:

Enable 802.11k neighbor reports ?

Enable 802.11r Fast BSS Transition ?

*** Client Inactivity Timeout:** ?

*** Directed MC/BC Threshold:** ?
Per radio client count at which an AP will stop converting group

14. (Optiona) Toggle the **VLAN Pooling** to turn it ON . By default, it is set to OFF.
15. In **VLAN ID**: Type the VLAN ID number (default is 1) that you want to assign to this network. The valid range is from 0 to 4096.
16. (Optiona) Toggle the **Proxy ARP** to turn it ON. By default, it is set to OFF.
17. In **Max. Number of Devices**: (Only for Captive Portal Host Approval and Self Sign In networks) Select the maximum number of devices that can connect to the network.
The drop-down list allows up to 10 devices.
18. In **User Connection Settings (Default)**: (Only for Captive Portal networks except Click-Through)
 - **Allow the user to stay connected for**: Select Minutes or Hours from the drop-down arrow box and then use the up/down arrows to select the number of minutes or hours of connection time after which the client is disconnected.
 - **Do not redirect to the portal when reconnecting within**: You can set the grace period which sets the number of minutes during which previously authenticated clients that disconnect from the network can rejoin the network without going through the authentication process again. The default grace period is 60 minutes, but this time cannot be longer than the allowed user connection period.
19. In **User Connection Settings (Time Limited)**: (Only for Captive Portal Click-Through networks) If you have clicked the **Change to Time limited connection** option.
 - **Allow users to connect for**: Enter an aggregated time period after which the user is disconnected. The default is 24 hours.
 - **After that time, don't allow to reconnect for**: Sets a lock-out time during which users are not allowed to sign-in again. The default is 2 hours.
20. In the **Load Control** section:
 - **Max rate**: There are three options:
 - Unlimited—no limits on bandwidth allocation.
 - Per AP—The max bandwidth allocation limit of all connections to that specific network on the AP. If selected, two other options appear, Upload Limit and Download Limit. If either (or both) boxes are checked, a sliding scale appears and you can drag your cursor along the line to choose the Mbps limits.
 - Per Client—The max bandwidth allocated for a device connected to this network. If selected, two other options appear, Upload Limit and Download Limit. If either (or both) boxes are checked, a sliding scale appears against each option and you can drag your cursor along the line to choose the Mbps limits.
 - **Max clients per radio**: Limit the number of clients that can associate with this network per AP radio (default is 100).
 - **Enable load balancing between 2.4GHz & 5GHz radios**: Select this check box to enable load balancing between the 2.4GHz and 5GHz radios. Load balancing helps improve network performance by helping to spread the client load between the two radios on the AP.
 - **Enable load balancing between APs**: Select this check box to spread the client load between nearby access points, so that one AP does not get overloaded while another sits idle.

21. Navigate to the **Access Control** section.

- a) Click **Set up a Policy** corresponding to **Device Connection Policy**.

The **Device Connection Policy** dialog box is displayed.

By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided.

- b) Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed.
c) Enter the MAC address and click **Add**.
d) Click **Clear list** to clear the MAC address list.
e) Click **OK** to return to the **Edit Network** screen.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- f) Configure a user traffic policy by clicking the **Set up a Policy** link. The **Traffic Policy** dialog box is displayed.

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red) provided.

22. To create a new traffic rule, click the **Add Rule** link. The **Add Traffic Access Rule** dialog box is displayed. You can create rules only for up-stream traffic.

NOTE

L3/L4 traffic policy rules will not be applied to traffic between clients attached to the same WLAN on the same AP.

- Enter a description for the rule in the text field provided.
- You can create a rule to allow or block up-stream traffic by clicking and selecting the **Allow Traffic** or **Block Traffic** option, respectively.
- Select the protocol which you wish to use for the new traffic rule, from the **Protocol** drop down list. Following are the list of protocols available for use.
 - **TCP**: Transmission Control Protocol
 - **UDP**: User Datagram Protocol
 - **UDPLITE**: Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - **ICMP (ICMPV4)**: Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - **IGMP**: Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - **ESP**: Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - **AH**: Authentication Header protocol, which is used to authenticate SNMP.
 - **SCTP**: Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
- Specify the source address in the **Source** field. You can either specify a range (a network address and a Subnet Mask, in the field provided) or you can specify a source IP address in the field provided. Also, specify a port number or a range of ports (for example, 22-34) for the source, in the field provided.
- Specify the destination address in the **Destination** field. You can either specify a range (a network address and a Subnet Mask, in the field provided) or you can specify a source IP address in the field provided. Also, specify a port number or a range of ports (e.g: 22-34) for the destination, in the field provided.

NOTE

If you choose the ICMP protocol in the previous step, you do not need to specify ports for the source and the destination. Hence, the option to select ports will not be presented to you.

23. Click **Save**. The rule which you created appears in the **Traffic Control Policy** dialog box.

NOTE

The rule which you initially create appears in a row with priority set a "1", by default. When you create a second rule, it appears in the row with priority "1" and the previous rule which you created appears as second in the row, with priority "2". When you have multiple rules created, you can use the "up" and "down" arrows available at the end of each row, to shift respective rows up or down in the order, to set the desired priority.

The edit and delete links available at the end of each row allow you to edit and delete respective rules. Each time you click the edit button, the **Add Traffic Access Rule** dialog box is displayed. where you can edit any of the rule properties.

24. Click **OK** in the **Traffic Policy** dialog box, once you have all the required rules added.

You are navigated back to the **Advanced Network Settings** dialog box, where you can click the **Traffic Policy** toggle button to "ON" or "OFF", activating or de-activating the traffic policy which you created, respectively. The **Edit** option allows you to navigate to the **Traffic Control Policy** dialog box, where you can edit the policy which you created. The **Clear** button allows you to delete the traffic policy.

25. To add a device and OS access policy, toggle the **Device & OS Access Policy** option to **ON**.
 - a) Choose a device and OS access policy from the **Select policy** drop down.
 - b) Click **Add** to add a device and OS access policy. The **Add Device & OS Access Policy** dialog box appears.
 - c) Complete the following:
 - **Policy Name:** Enter the name of the policy.
 - **Description:** Enter description for the policy.
 - **Default Access:** Select either **Allow** or **Block**.
 - d) Click **Add Rule** and then complete the following:
 - **Rule Name:** Enter the name of the rule.
 - **Action:** Select either **Allow Devices** or **Block Devices**.
 - **Device Type:** Select a device type from the list of devices.
 - **OS Vendor:** Select the OS vendor for the devices.
 - **Rate Limit:** Configure the rate limit using the sliders: **From client** and **To client**.
 - **VLAN:** Enter the VLAN ID.
 - e) Click **ADD** to add the rule to the device and OS access policy for the network .
26. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**
27. In **Enable Client Isolation:** Select this check box to prevent clients on the same network from communicating with each other.
28. In **Force DHCP:** Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
29. In **Hide SSID:** Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.
30. In **Enable OFDM only (Disables 802.11b):** Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.
31. In **Enable logging client data to external syslog:** Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.
32. In **BSS Min Rate:** Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.
33. In **Mgmt Tx Rate:** This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.
34. **Enable 802.11k neighbor reports:** Enhances roaming by providing a list of neighbor APs to the client device.
35. **Enable 802.11r Fast BSS Transition:** 802.11r Fast BSS Transition fast roaming protocol.
36. **Client Inactivity Timeout:** Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.
37. **Airtime Decongestion:** Toggle the switch to ON to activate the airtime decongestion feature.

38. **RSSI Threshold:** Toggle the switch to ON and then configure the threshold value.
39. **Transient Client Management:** Toggle the switch to ON and then configure parameters for **Join Wait Time**, **Join Expire Time**, and **Join Wait Threshold**.
40. **Optimized Connectivity Experience (OCE):** Toggle the switch to ON and then configure parameters for **Broadcast Probe Response Delay** and **RSSI-Based Association Rejection Threshold**.
41. Click **Reset to defaults** button in the lower left side of the screen to reset all the advanced settings back to their defaults.
42. Click **Save** to save your settings.
43. Click **Save** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Creating a Network That Uses an Enterprise AAA Server

You can create a network that authenticates users against a remote authentication, authorization, and accounting (AAA) server.

Before you create a network, write down the IP address, port number, and shared secret of the primary and secondary (if any) RADIUS server that you want to use to authenticate network users.

Complete the following steps to create a network that uses a remote AAA server.

1. From the navigation pane, click **Networks**.
2. Click **Add Network**.
The **Add Network** dialog box is displayed.
3. Complete the settings on the **Network Details** page.
 - **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
 - **Description:** Enter an optional description (up to 64 characters).
 - **Network Type:** Click **Enterprise AAA (802.1X)**.

When the network type is selected, a structure diagram of an Enterprise AAA type of network displays.

4. Click **Next**.
The **AAA Settings** page is displayed.
5. Complete the settings on the **AAA Settings** page.

In the **Authentication Service** section, complete the following configuration:

- **IP Address:** Enter the IP address of the primary RADIUS server.
- **Port:** Enter the listening port used by the primary RADIUS server.
- **Shared Secret:** Enter the shared secret configured on the RADIUS server.

NOTE

If you do not have a secondary RADIUS server, do not complete the **Add Secondary Server** section.

In the **Add Secondary Server** section (if you have another RADIUS server on the network), complete the following configuration:

- **IP Address:** Enter the IP address of the secondary RADIUS server.
- **Port:** Enter the listening port used by the secondary RADIUS server.
- **Shared Secret:** Enter the shared secret configured on the RADIUS server.

6. In the **Accounting Service** section, set the switch to **ON**, and complete the following configuration:

- **IP Address:** Enter the IP address of the primary RADIUS Accounting server.
- **Port:** Enter the listening port used by the primary RADIUS Accounting server.
- **Shared Secret:** Enter the shared secret configured on the RADIUS Accounting server.

NOTE

If you do not have a secondary RADIUS Accounting server, do not complete the **Add Secondary Server** section.

In the **Add Secondary Server** section (if you have another RADIUS Accounting server on the network), complete the following configuration:

- **IP Address:** Enter the IP address of the secondary RADIUS Accounting server.
- **Port:** Enter the listening port used by the secondary RADIUS Accounting server.
- **Shared Secret:** Enter the shared secret configured on the RADIUS Accounting server.

7. Click **Next**.

The **Venues** page is displayed.

8. Select the venues in which you want to activate this network:

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the Activated column. The **Select APs on venue <venue-name>** page is displayed.

9. In the **Select APs on venue <venue-name>** page, you have two choices for defining how the network will be activated:

- Click the **All APs** button to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the **Select specific AP groups** button to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. The **APs not assigned to any group** option is displayed. After **APs not assigned to any group** is selected, two more options are displayed:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1. Check the **Dynamic VLAN** if desired.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

10. Click **Save** to save the settings and return to the **Venues** page.

The **Venues** page is displayed.

11. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

12. Click **OK**.

Returns to **Add Network** dialog box.

13. Click **Next**.

The **Summary** page is displayed.

14. Review the settings that you configured. To display the passphrase in plain text, click the eye icon.

15. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.

- Enter the VLAN ID.
- In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
- In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP**: Transmission Control Protocol
 - › **UDP**: User Datagram Protocol
 - › **UDPLITE**: Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4)**: Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP**: Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - › **ESP**: Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - › **AH**: Authentication Header protocol, which is used to authenticate SNMP.
 - › **SCTP**: Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
 - Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
 - Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

16. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enables you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

17. Click **OK** in the **Traffic Policy** dialog box, added all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

18. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**

19. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.
20. **Single Session ID Accounting**: Select this check box to enable Wi-Fi clients roam across access points and to maintain a single session ID for RADIUS Accounting.
21. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.
If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
22. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.
23. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.
24. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.
25. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.
26. In **Mgt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.
27. **Enable 802.11k neighbor reports**: Enhances roaming by providing a list of neighbor APs to the client device.
28. **Enable 802.11r Fast BSS Transition**: 802.11r Fast BSS Transition fast roaming protocol.
29. **Client Inactivity Timeout**: Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.
30. **Directed MC/BC Threshold**: Directed multicast/broadcast threshold.

31. Click **OK** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Creating a Network That Uses Cloudpath Onboarding

You can learn to create a network that authenticates users using Ruckus Cloudpath.

Before you begin this procedure, write down the Cloudpath SSID and Cloudpath portal URL that you want to use, as well as the IP address, port number, and shared secret of the RADIUS server.

Complete the following steps to create a network that uses Cloudpath onboarding.

1. From the navigation pane, click **Networks**.
2. Click **Add Network**.

The **Add Network** dialog box is displayed.

3. Complete the settings on the **Network Details** page.

- **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
- **Description:** Enter a description (up to 64 characters) to help you identify the network using.
- **Network Type:** Click **Cloudpath**.

When the network type is selected, a structure diagram of a Cloudpath type of network displays.

4. Click **Next**.

The **Cloudpath Settings** is displayed.

5. Complete the settings on the **Cloudpath Settings** page:

- **Onboarding SSID:** Enter the SSID to which users must connect to go through the authentication process.
- **Onboarding Portal URL:** Enter the URL to which users that have associated with the onboarding SSID will be redirected to for authentication purposes. Users attempting to access this network must pass the authentication process before they can be allowed access to the network.
- **MAC auth bypass:** Check this if MAC address authentication is not required.
- **Walled Garden:** Enter the network destinations (URLs or IP addresses) that users can access without going through authentication. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the walled garden.

6. In the **Authentication Service** section, complete the following configuration:

- **IP Address:** Enter the IP address of the RADIUS server of your Cloudpath system.

NOTE

If you previously added a RADIUS server for another network, the IP address and port fields are prepopulated with the information you used for the that RADIUS server. If you using a different RADIUS server, overwrite the information in the IP address and port fields.

- **Port:** Type the listening port used by the RADIUS server.
- **Shared Secret:** Type the shared secret configured on the RADIUS server.

7. In the **Accounting Service** section, set the switch to **ON**, and complete the following configuration:

- **IP Address:** Enter the IP address of the primary RADIUS Accounting server.
- **Port:** Enter the listening port used by the primary RADIUS Accounting server.
- **Shared Secret:** Type the shared secret configured on the RADIUS Accounting server.

NOTE

If you do not have a secondary RADIUS Accounting server, do not complete the **Add Secondary Server** section.

In the **Add Secondary Server** section (if you have another RADIUS Accounting server on the network), complete the following boxes:

- **IP Address:** Enter the IP address of the secondary RADIUS Accounting server.
- **Port:** Enter the listening port used by the secondary RADIUS Accounting server.
- **Shared Secret:** Enter the shared secret configured on the RADIUS Accounting server.

8. Click **Next**.

The **Venues** page is displayed.

9. Select the venues in which you want to activate this network:

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the Activated column. The **Select APs on venue <venue-name>** page is displayed.

10. In the **Select APs on venue <venue-name>** page, you have two choices for defining how the network will be activated:

- Click the **All APs** button to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the **Select specific AP groups** button to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. The **APs not assigned to any group** option is displayed. After **APs not assigned to any group** is selected, two more options are displayed:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1 for onboarding. Check the **Dynamic VLAN** if desired.
 - In the **Radio** option, select a radio band of 2.4 GHz, 5 GHz, or both.

11. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

12. Click **OK**.

Returns to **Add Network** dialog box.

13. Click **Save** to save the settings and return to the **Venues** page.

The **Venues** page is displayed.

14. Click **Next**.

The **Summary** page is displayed.

15. Review the settings that you configured. To display the passphrase in plain text, click the eye icon.

16. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.

- Enter the VLAN ID.
- In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
- In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP**: Transmission Control Protocol
 - › **UDP**: User Datagram Protocol
 - › **UDPLITE**: Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4)**: Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP**: Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - › **ESP**: Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - › **AH**: Authentication Header protocol, which is used to authenticate SNMP.
 - › **SCTP**: Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
 - Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
 - Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

17. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enables you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

18. Click **OK** in the **Traffic Policy** dialog box, added all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

19. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**

20. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.

21. **Single Session ID Accounting**: Select this check box to enable Wi-Fi clients roam across access points and to maintain a single session ID for RADIUS Accounting.

22. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.

23. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.

24. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.

25. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.

26. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.

27. In **Mgmt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.

28. **Enable 802.11k neighbor reports**: Enhances roaming by providing a list of neighbor APs to the client device.

29. **Enable 802.11r Fast BSS Transition**: 802.11r Fast BSS Transition fast roaming protocol.

30. **Client Inactivity Timeout**: Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.

31. **Directed MC/BC Threshold**: Directed multicast/broadcast threshold.

32. Click **OK** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Creating a Network That Uses a Captive Portal with Click-Through

You can learn to create a network that allows users attempting to join the network to click through a portal to gain access.

Complete the following steps to create a network that uses the captive portal option of click-through.

1. From the navigation pane, click **Networks**.
2. Click **Add Network**.
The **Add Network** dialog box is displayed.
3. Complete the settings on the **Network Details** page.
 - **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
 - **Description:** Enter an optional description (up to 64 characters).
 - **Network Type:** Click **Captive Portal**.

When the network type is selected, a structure diagram of a Captive Portal type of network displays.

4. Click **Next**.
The **Portal Type** page is displayed.
5. Click **Click-Through**.
To access the network, users are required to accept the Terms and Conditions.
The Click-Through type of network diagram is displayed.
6. Click **Next**.
The **Onboarding** page is displayed.
7. Select the **Redirect Users to** check box and enter a valid URL.
You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.
8. Click **Next**.
The **Portal Web Page** page is displayed.

9. Configure the logo, welcome message, and terms and conditions that you want users to see and agree to before they can join the network:
 - **Display Language:** By default, the language is English. Use the list to select another language.
 - **Logo:** By default, the Ruckus Cloud logo is displayed. To use your own logo, click **Change**, select your own logo image, and then click **Open**.
 - **Welcome Text:** Enter some welcome text for the portal web page. For example, you can type "Welcome to Willowdale Dental Clinic". The welcome text (up to 100 characters) is displayed beneath the logo.
 - **Advert:** If you want to display an advertisement or announcement banner (in image format), click **Upload**, select the banner image, and then click **Open**. This banner will appear under the logo.
 - **Marketing Message:** Enter a marketing message that you want to display on the portal web page. The marketing message (up to 140 characters) is displayed beneath the welcome text.
 - **Terms & Conditions:** Enter the terms and conditions that you want users to agree to before they can access this network.
 - **Insert WiFi4EU Snippet:** Toggle the to **ON** or **OFF**.
 - **WiFi4EU UUID::** Enter the WiFi4EU UUID.

A preview of the portal web page is displayed on the right side of the **Portal Web Page** page.

10. Click **Next**.

The **Venues** page is displayed.

11. Select the venues in which you want to activate this network.

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the **Activated** column. The **Select APs on venue <venue-name>** page is displayed.

12. In the **Select APs on venue <venue-name>** screen, you have two choices for defining how the network will be activated:

- Click the button next to **All APs** to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the button next to **Select specific AP groups** to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. An option to allow the network to be activated on any **APs not assigned to any group** is displayed. When selected by clicking the box, two more options display:
 - In the **VLAN** option, click the pencil icon to edit the VLAN number. The default is VLAN 1. Click options to reset to the default, OK, or cancel.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

13. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

- a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

14. Click **OK**.

Returns to **Add Network** dialog box.

15. Click **Next**.

The **Summary** page is displayed.

16. Review the settings that you configured on the previous pages.

17. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.
- Enter the VLAN ID.
 - In the **User Connection Settings** section, configure the following.
 - **Allow the user to stay connected for:** Select Minutes or Hours from the drop-down arrow box and then use the up/down arrows to select the number of minutes or hours of connection time after which the client is disconnected.
 - **Do not redirect to the portal when reconnecting within:** You can set the grace period which sets the number of minutes during which previously authenticated clients that disconnect from the network can rejoin the network without going through the authentication process again. The default grace period is 60 minutes, but this time cannot be longer than the allowed user connection period.
 - In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
 - In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP:** Transmission Control Protocol
 - › **UDP:** User Datagram Protocol
 - › **UDPLITE:** Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4):** Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP:** Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - › **ESP:** Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - › **AH:** Authentication Header protocol, which is used to authenticate SNMP.

- › **SCTP:** Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
- Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
- Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

18. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enables you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

19. Click **OK** in the **Traffic Policy** dialog box, added all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

20. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**

21. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.
22. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
23. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.
24. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.
25. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.
26. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.
27. In **Mgt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.
28. **Enable 802.11k neighbor reports**: Enhances roaming by providing a list of neighbor APs to the client device.

29. **Client Inactivity Timeout:** Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.
30. **Directed MC/BC Threshold:** Directed multicast/broadcast threshold.
31. Click **Save** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Creating a Network That Uses a Captive Portal with Self Sign In

You can learn to create a network that allows users attempting to join the network to sign in using a social media account or to register their details for a personal password to gain access.

Complete the following steps to create a network that uses the self-sign-in captive portal option..

1. From the navigation pane, click **Networks**.
2. Click **Add Network**.

The **Add Network** dialog box is displayed.

3. Complete the settings on the **Network Details** page.

- **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
- **Description:** Enter a description (up to 64 characters) to help you identify the network using.
- **Network Type:** Click **Captive Portal**.

When the network type is selected, a structure diagram of a Captive Portal type of network displays.

4. Click **Next**.

The **Portal Type** page is displayed.

5. Click **Self Sign In**.

To access the network, users enter their social media account password, or register their details and get a personal password.

The Self Sign In type of network diagram is displayed.

6. Click **Next**.

The **Onboarding** page is displayed.

7. Complete the settings on the **Onboarding** page.

If you want users to self-register using their social media accounts or an SMS token, complete the configuration under the **Allow Sign-In Using** section. If you created your own app on any of these social media platforms and you want to use your app, you can add details when you edit the option. You can select one or more of the following options:

- **SMS Token:** Select this check box if you want users to receive a single-use token on their mobile number. A **Password expires after** field is displayed and you can select a time period in hours or days after which the password expires. The default is 12 hours.
- **Facebook:** Select this check box if you want users to connect to the network using their Facebook account. Click the **Edit** (cog) icon to view the Edit Facebook App page and add further configuration. For details, refer to [Allowing Sign-In Using Facebook](#) on page 124.
- **Google:** Select this check box if you want users to connect to the network using their Google account. Click the **Edit** (cog) icon to view the Edit Google App page and add further configuration. For details, refer to [Allowing Sign-In Using Google](#) on page 124.
- **LinkedIn:** Select this check box if you want users to connect to the network using their LinkedIn account. Click the **Edit** (cog) icon to view the Edit LinkedIn App page and add further configuration. For details, refer to [Allowing Sign-In Using LinkedIn](#) on page 125.
- **Twitter:** Select this check box if you want users to connect to the network using their Twitter account. Click the **Edit** (cog) icon to view the Edit Twitter App page and add further configuration. For details, refer to [Allowing Sign-In Using Twitter](#) on page 126.

8. Check the **Allowed domains** check box to allow only the clients registering with email addresses from the specified domains to connect to the network.

- You can configure multiple domain names separated by commas.
- This does not apply to SMS Token registration.

9. Check the **Redirect Users to** check box and enter a valid URL.

You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.

10. Check the **Collect email addresses of users who connect to this network** check box to save email address of the user.

As required for privacy compliance, the user will be informed on email being saved.

11. Check the **Enable Ruckus DHCP service** check box if you want the clients to receive IP addresses in an isolated 172.21.132.0/32 network. Click **More details** to view the guest network pool details.

12. Click **Next**.

The **Portal Web Page** page is displayed.

13. Configure the logo, welcome message, and terms and conditions that you want users to see and agree to before they can join the network:
 - **Display Language:** By default, the language is English. Use the list to select another language.
 - **Logo:** By default, the Ruckus Cloud logo is displayed. To use your own logo, click **Change**, select your own logo image, and then click **Open**.
 - **Welcome Text:** Enter some welcome text for the portal web page. For example, you can type "Welcome to Willowdale Dental Clinic". The welcome text (up to 100 characters) is displayed beneath the logo.
 - **Advert:** If you want to display an advertisement or announcement banner (in image format), click **Upload**, select the banner image, and then click **Open**. This banner will appear under the logo.
 - **Marketing Message:** Enter a marketing message that you want to display on the portal web page. The marketing message (up to 140 characters) is displayed beneath the welcome text.
 - **Terms & Conditions:** Enter the terms and conditions that you want users to agree to before they can access this network. The text "By clicking a button, you are accepting the terms and conditions" appears with the terms and conditions text a link to your text and highlighted in blue.
 - **Insert WiFi4EU Snippet:** Toggle the to **ON** or **OFF**.
 - **WiFi4EU UUID::** Enter the WiFi4EU UUID.

A preview of the portal web page is displayed on the right side of the **Portal Web Page** page.

14. Click **Next**.

The **Venues** page is displayed

15. Select the venues in which you want to activate this network.

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and then set the switch to **ON** in the **Activated** column. The **Select APs on venue <venue-name>** page is displayed.

16. In the **Select APs on venue <venue-name>** screen, you have two choices for defining how the network will be activated:

- Click the button next to **All APs** to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the button next to **Select specific AP groups** to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. An option to allow the network to be activated on any **APs not assigned to any group** is displayed. When selected by clicking the box, two more options display:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

17. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

- a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

18. Click **OK**.

Returns to **Add Network** dialog box.

19. Click **Next**.

The **Summary** page is displayed.

20. Review the settings that you configured on the previous pages.

21. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.

- Enter the VLAN ID.
- **Max number of devices:** Select the maximum number of devices that can connect to the network.

The drop-down list allows up to 10 devices

- In the **User Connection Settings** section, configure the following.
 - **Allow the user to stay connected for:** Select Minutes or Hours from the drop-down arrow box and then use the up/down arrows to select the number of minutes or hours of connection time after which the client is disconnected.
 - **Do not redirect to the portal when reconnecting within:** You can set the grace period which sets the number of minutes during which previously authenticated clients that disconnect from the network can rejoin the network without going through the authentication process again. The default grace period is 60 minutes, but this time cannot be longer than the allowed user connection period.
- In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
- In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP:** Transmission Control Protocol
 - › **UDP:** User Datagram Protocol
 - › **UDPLITE:** Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4):** Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP:** Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.

- › **ESP:** Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
- › **AH:** Authentication Header protocol, which is used to authenticate SNMP.
- › **SCTP:** Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
- Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
- Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

22. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enable you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

23. Click **OK** in the **Traffic Policy** dialog box, adding all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

24. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**.

25. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.

26. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.

27. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.

28. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.

29. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.

30. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.

31. In **Mgmt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.

32. **Enable 802.11k neighbor reports:** Enhances roaming by providing a list of neighbor APs to the client device.
33. **Client Inactivity Timeout:** Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.
34. **Directed MC/BC Threshold:** Directed multicast/broadcast threshold.
35. Click **Save** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Allowing Sign-In Using Facebook

When creating a captive portal network with self sign in, you can allow users to register with their Facebook social media account.

Before using this task, perform Steps 1 through 6 in the [Creating a Network That Uses a Captive Portal with Self Sign In](#) on page 118.

1. From the **Onboarding** page of the Captive Portal Self Sign In network option, click the check mark next to the **Facebook** option.
This will allow users to connect to the network using their Facebook account.
2. Click the **Edit** icon which looks like a cog.
The **Edit Facebook App** window appears.
3. If you want to use the default Ruckus app, click the button next to the **Use Ruckus app** option.
This is the default. Proceed to Step 5.
4. If you created your own app on Facebook, click the button next to the **Use your own app** option.
More options are displayed. Enter your **App ID** and **Secret** code. Click the **Copy to clipboard** option to copy the URL that you must paste into your Facebook Developer Account.
5. Click **See sample** to view an example of the Self Sign In screen depending on your choice of app.
You can toggle between viewing the sample screen created by either of the app options by clicking **Ruckus App** or **Your Own App**.
6. When you have finished viewing the sample screens, click **Close**.
7. Check the **Redirect Users to** check box and enter a valid URL.
You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.
8. Check the **Collect email addresses of users who connect to this network** check box to save email address of the user.
As required for privacy compliance, the user will be informed on email being saved.
9. Click **Save**.
You are returned to the **Onboarding** page of the **Captive Portal Self Sign In** network option.

Allowing Sign-In Using Google

When creating a captive portal network with self sign in, you can allow users to register with their Google social media account.

Before using this task, perform Steps 1 through 6 in the [Creating a Network That Uses a Captive Portal with Self Sign In](#) on page 118.

1. From the **Onboarding** page of the Captive Portal Self Sign In network option, click the check mark next to the **Google** option.
This will allow users to connect to the network using their Google account.

2. Click the **Edit** icon which looks like a cog.
The **Edit Google App** window appears.
3. If you want to use the default Ruckus app, click the button next to the **Use Ruckus app** option.
This is the default. Proceed to Step 5.
4. If you created your own app on Google, click the button next to the **Use your own app** option.
More options are displayed. Enter your **App ID** and **Secret** code. Click the **Copy to clipboard** option to copy the URL that you must paste into your Google Developer Console.
5. Click **See sample** to view an example of the Self Sign In screen depending on your choice of app.
You can toggle between viewing the sample screen created by either of the app options by clicking **Ruckus App** or **Your Own App**.
6. When you have finished viewing the sample screens, click **Close**.
7. Check the **Redirect Users to** check box and enter a valid URL.
You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.
8. Check the **Collect email addresses of users who connect to this network** check box to save email address of the user.
As required for privacy compliance, the user will be informed on email being saved.
9. Click **Save**.
You are returned to the **Onboarding** page of the **Captive Portal Self Sign In** network option.

Allowing Sign-In Using LinkedIn

When creating a captive portal network with self sign in, you can allow users to register with their LinkedIn social media account.

Before using this task, perform Steps 1 through 6 in the [Creating a Network That Uses a Captive Portal with Self Sign In](#) on page 118.

1. From the **Onboarding** page of the Captive Portal Self Sign In network option, click the check mark next to the **LinkedIn** option.
This will allow users to connect to the network using their LinkedIn account.
2. Click the **Edit** icon which looks like a cog.
The **Edit LinkedIn App** window appears.
3. If you want to use the default Ruckus app, click the button next to the **Use Ruckus app** option.
This is the default. Proceed to Step 5.
4. If you created your own app on LinkedIn, click the button next to the **Use your own app** option.
More options are displayed. Enter your **Client ID** and **Secret** code. Click the **Copy to clipboard** option to copy the URL that you must paste into your LinkedIn Developer Console.
5. Click **See sample** to view an example of the Self Sign In screen depending on your choice of app.
You can toggle between viewing the sample screen created by either of the app options by clicking **Ruckus App** or **Your Own App**.
6. When you have finished viewing the sample screens, click **Close**.
7. Check the **Redirect Users to** check box and enter a valid URL.
You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.
8. Check the **Collect email addresses of users who connect to this network** check box to save email address of the user.
As required for privacy compliance, the user will be informed on email being saved.

9. Click **Save**.

You are returned to the **Onboarding** page of the **Captive Portal Self Sign In** network option.

Allowing Sign-In Using Twitter

When creating a captive portal network with self sign in, you can allow users to register with their Twitter social media account.

Before using this task, perform Steps 1 through 6 in the [Creating a Network That Uses a Captive Portal with Self Sign In](#) on page 118.

1. From the **Onboarding** page of the Captive Portal Self Sign In network option, click the check mark next to the **Twitter** option.
This will allow users to connect to the network using their Twitter account.

2. Click the **Edit** icon which looks like a cog.

The **Edit Twitter App** window appears.

3. If you want to use the default Ruckus app, click the button next to the **Use Ruckus app** option.

This is the default. Proceed to Step 5.

4. If you created your own app on Twitter, click the button next to the **Use your own app** option.

More options are displayed. Enter your **Consumer Key** and **Secret** code. Click the **Copy to clipboard** option to copy the URL that you must paste into Twitter Application Management.

5. Click **See sample** to view an example of the Self Sign In screen depending on your choice of app.

You can toggle between viewing the sample screen created by either of the app options by clicking **Ruckus App** or **Your Own App**.

6. When you have finished viewing the sample screens, click **Close**.

7. Check the **Redirect Users to** check box and enter a valid URL.

You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.

8. Check the **Collect email addresses of users who connect to this network** check box to save email address of the user.

As required for privacy compliance, the user will be informed on email being saved.

9. Click **Save**.

You are returned to the **Onboarding** page of the **Captive Portal Self Sign In** network option.

Creating a Network That Uses a Captive Portal with Host Approval

You can create a network that allows users attempting to join the network through a captive portal after obtaining approval from the host.

To access the network, users register their details in the portal including their email that is connected to the host. Only hosts from domains entered through the portal can approve guest requests. A host must approve the guest request via email in order to provide the temporary network credentials to the guest user.

Complete the following steps to create a network that uses the host approval captive portal option.

1. From the navigation pane, click **Networks**.

2. Click **Add Network**.

The **Add Network** dialog box is displayed.

3. Complete the settings on the **Network Details** page.
 - **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
 - **Description:** Enter an optional description (up to 64 characters).
 - **Network Type:** Click **Captive Portal**.

When the network type is selected, a structure diagram of a Captive Portal type of network displays.

4. Click **Next**.

The **Portal Type** page is displayed.

5. Click **Host Approval**.

To access the network, users register their details in the portal including their host email. A host must approve the guest request in order to provide the temporary network credentials to the guest user.

The Host Approved type of network diagram is displayed.

6. Click **Next**.

The **Host Settings** page is displayed.

7. In the **Host Domain** field, enter the domain names, separated by a comma, that are allowed to host the guest portal page.

8. In the **Password expiration options:**, select the password expiration periods that the host can select when granting access to the guest user.

The options are 1 Hour, 4 Hours, 1 Day, 1 Week, and 1 Month.

Only the selected options are displayed to the host.

9. Select the **Redirect Users to:** check box and enter a valid URL.

You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.

10. Click **Next**.

The **Portal Web Page** is displayed.

11. Configure the logo, welcome message, and terms and conditions that you want users to see and agree to before they can join the network.

- **Display Language:** By default, the language is English. Use the list to select another language.
- **Logo:** By default, the Ruckus Cloud logo is displayed. To use your own logo, click **Change**, select your own logo image, and then click **Open**.
- **Welcome Text:** Type a welcome text for the portal web page. For example, you can type "Welcome to Willowdale Dental Clinic". The welcome text appears below the logo. Up to 100 characters are allowed.
- **Terms & Conditions:** Type the terms and conditions that you want users to agree to before they can access this network.
- **Insert WiFi4EU Snippet:** Toggle the to **ON** or **OFF**.
- **WiFi4EU UUID:** Enter the WiFi4EU UUID.

A preview of the portal web page appears on the right side of the **Portal Web Page**.

12. Click **Next**.

The **Venues** page is displayed.

Managing Wi-Fi Networks

Wi-Fi Networks in Ruckus LTE AP Management

13. Select the venues in which you want to activate this network.

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the **Activated** column. The **Select APs on venue <venue-name>** page is displayed.

14. In the **Select APs on venue <venue-name>** screen, you have two choices for defining how the network will be activated:

- Click the button next to **All APs** to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the button next to **Select specific AP groups** to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. An option to allow the network to be activated on any **APs not assigned to any group** is displayed. When selected by clicking the check box, two more options display:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

15. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

a) Check one of the **Network Availability** options:

- **24/7**: Network is available 24/7.
- **Custom schedule**: Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

16. Click **OK**.

Returns to **Add Network** dialog box.

17. Click **Next**.

The **Summary** page is displayed.

18. Review the settings that you configured on the previous pages.

19. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.

- Enter the VLAN ID.
- **Max number of devices:** Select the maximum number of devices that can connect to the network.
The drop-down list allows up to 10 devices
- In the **User Connection Settings** section, configure the following.
 - **Allow the user to stay connected for:** Select Minutes or Hours from the drop-down arrow box and then use the up/down arrows to select the number of minutes or hours of connection time after which the client is disconnected.
 - **Do not redirect to the portal when reconnecting within:** You can set the grace period which sets the number of minutes during which previously authenticated clients that disconnect from the network can rejoin the network without going through the authentication process again. The default grace period is 60 minutes, but this time cannot be longer than the allowed user connection period.
- In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
- In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP:** Transmission Control Protocol
 - › **UDP:** User Datagram Protocol
 - › **UDPLITE:** Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4):** Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP:** Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.

- › **ESP:** Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
- › **AH:** Authentication Header protocol, which is used to authenticate SNMP.
- › **SCTP:** Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
- Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
- Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

20. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enable you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

21. Click **OK** in the **Traffic Policy** dialog box, adding all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

22. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**.

23. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.

24. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.

25. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.

26. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.

27. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.

28. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.

29. In **Mgmt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.

30. **Enable 802.11k neighbor reports:** Enhances roaming by providing a list of neighbor APs to the client device.
31. **Client Inactivity Timeout:** Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.
32. **Directed MC/BC Threshold:** Directed multicast/broadcast threshold.
33. Click **Save** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Creating a Network That Uses a Captive Portal with a Guest Pass

You can create a network that allows users attempting to join the network to use a guest pass that is generated by an administrator to gain access. In this type of network access, users sign in using a personal password that they receive in advance from a network administrator.

Complete the following steps to create a network that uses the guest pass captive portal option.

1. From the navigation pane, click **Networks**.
2. Click **Add Network**.
The **Add Network** dialog box is displayed.
3. Complete the settings on the **Network Details** page.
 - **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
 - **Description:** Enter an optional description (up to 64 characters).
 - **Network Type:** Click **Captive Portal**.

When the network type is selected, a structure diagram of a Captive Portal type of network displays.

4. Click **Next**.
The **Portal Type** page is displayed.
5. Click **Guest Pass**.
To access the network, users sign in with a personal password received in advance from the network administration staff.
The Guest Pass type of network diagram is displayed.
6. Click **Next**.
The **Onboarding** page is displayed.
7. Select the **Redirect Users to** check box and enter a valid URL.
You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.
8. Click **Next**.
The **Portal Web Page** page is displayed.

9. Configure the logo, welcome message, and terms and conditions that you want users to see and agree to before they can join the network.
 - **Display Language:** By default, the language is English. Use the list to select another language.
 - **Logo:** By default, the Ruckus Cloud logo is displayed. To use your own logo, click **Change**, select your own logo image, and then click **Open**.
 - **Welcome Text:** Type a welcome text for the portal web page. For example, you can type "Welcome to Willowdale Dental Clinic". The welcome text appears below the logo. Up to 100 characters are allowed.
 - **Advert:** If you want to display an advertisement or announcement banner (in image format), click Upload, select the banner image, and then click **Open**. This banner will appear under the logo.
 - **Marketing Message:** Type a marketing message that you want to display on the portal web page. The text appears below the Welcome Text. Up to 140 characters are allowed.
 - **Terms & Conditions:** Type the terms and conditions that you want users to agree to before they can access this network.
 - **Insert WiFi4EU Snippet:** Toggle the to **ON** or **OFF**.
 - **WiFi4EU UUID::** Enter the WiFi4EU UUID.

A preview of the portal web page is displayed on the right side of the **Portal Web Page**.

10. Click **Next**.

The **Venues** page is displayed.

11. Select the venues in which you want to activate this network.

- To activate the network in all of your venues, click **Activate in all venues**.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the **Activated** column. The **Select APs on venue <venue-name>** page is displayed.

12. In the **Select APs on venue <venue-name>** screen, you have two choices for defining how the network will be activated:

- Click the button next to **All APs** to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
- Click the button next to **Select specific AP groups** to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. An option to allow the network to be activated on any **APs not assigned to any group** is displayed. When selected by clicking the check box, two more options display:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

13. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

- a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

14. Click **OK**.

Returns to **Add Network** dialog box.

15. Click **Next**.

The **Summary** page is displayed.

16. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.
- Enter the VLAN ID.
 - In the **User Connection Settings** section, configure the following.
 - **Allow the user to stay connected for:** Select Minutes or Hours from the drop-down arrow box and then use the up/down arrows to select the number of minutes or hours of connection time after which the client is disconnected.
 - **Do not redirect to the portal when reconnecting within:** You can set the grace period which sets the number of minutes during which previously authenticated clients that disconnect from the network can rejoin the network without going through the authentication process again. The default grace period is 60 minutes, but this time cannot be longer than the allowed user connection period.
 - In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
 - In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP:** Transmission Control Protocol
 - › **UDP:** User Datagram Protocol
 - › **UDPLITE:** Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4):** Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP:** Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - › **ESP:** Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - › **AH:** Authentication Header protocol, which is used to authenticate SNMP.

- › **SCTP:** Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
- Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
- Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

17. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enables you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

18. Click **OK** in the **Traffic Policy** dialog box, added all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

19. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**

20. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.
21. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
22. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.
23. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.
24. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.
25. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.
26. In **Mgmt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.
27. **Enable 802.11k neighbor reports**: Enhances roaming by providing a list of neighbor APs to the client device.

28. **Client Inactivity Timeout:** Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.
29. **Directed MC/BC Threshold:** Directed multicast/broadcast threshold.
30. Click **Save** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Creating an Open Network (No Authentication)

You can create a network that allows users to join the network without going through any authentication process.



CAUTION

RUCKUS strongly advises against creating an open network. Wireless communication on an open network is not secure and information (including sensitive data, such as personal information, credit card information, and so on) that your users send over or through the network can easily be intercepted.

Follow these steps to create an open network.

1. From the navigation pane, click **Networks**.
2. Click **Add Network**.
The **Add Network** dialog box is displayed.
3. Complete the settings on the **Network Details** page.
 - **Network Name:** Enter a name (up to 32 characters) that you want assign to the network.
 - **Description:** Enter a description (up to 64 characters) to help you identify the network using.
 - **Network Type:** Click **Open Network**.
4. Click **Next**.
The **Venues** page is displayed.
5. Select the venues in which you want to activate this network.
 - To activate the network in all of your venues, click **Activate on all venues**.
 - To activate the network in a specific venue, locate the venue from the list, and set the switch to **ON** in the **Activated** column. The **Select APs on venue <venue-name>** page is displayed.
6. In the **Select APs on venue <venue-name>** screen, yx:
 - Click the radio button next to **All APs** to activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.
 - Click the radio button next to **Select specific AP groups** to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. An option to allow the network to be activated on any **APs not assigned to any group** is displayed. When selected by clicking the box, two more options display:
 - In the **VLAN** option, click the edit (pencil) icon to edit the VLAN number. The default is VLAN 1.
 - In the **Radios** option, select a radio band of 2.4 GHz, 5 GHz, or both.

Managing Wi-Fi Networks

Wi-Fi Networks in Ruckus LTE AP Management

7. Click the clock icon under **Schedule** to configure the schedule for the network in the selected venue.

The **Schedule for Network <network-name> in Venue <venue-name>** dialog appears.

- a) Check one of the **Network Availability** options:

- **24/7:** Network is available 24/7.
- **Custom schedule:** Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours).

8. Click **OK**.

Returns to **Add Network** dialog box.

9. Click **Next**.

The **Summary** page is displayed.

10. To configure advanced options for the network, click **Advanced Network Settings**. The **Advanced Network Settings** dialog box is displayed.

- Enter the VLAN ID.
- In the **Load Control** section, complete the following configuration:
 - Select the **Max Rate** from the list, based on which load will be controlled over the network.
 - Calibrate the maximum number of clients per radio.
 - If you want to enable load balancing between 2.4 GHz and 5 GHz radios, select the button.
 - If you want to enable load balancing between APs, select the button.
- In the **Access Control** section, you can define a user device policy by clicking **Set up a Policy**. By default, the **Allow Connections only from MAC addresses listed below** option (green) is enabled. You can choose to change this to **Block Connections from MAC addresses listed below** by clicking the option (red) provided. Click **Add** to add a MAC address. The **Add MAC address** dialog box is displayed. Enter the MAC address and click **Add**. Click **Clear list** to clear the MAC address list.

NOTE

As an admin user, you can assign a single policy of each type to the network as the default policy or as part of the Network and Venue activation. This action overrides the default network policy.

- In the **Access Control** section, you can define a user traffic policy by clicking **Set up a Policy**. The **Traffic Policy** dialog box is displayed.

NOTE

By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Block Traffic** by clicking the option (red).

- To create a new traffic rule, click the **Add Rule**. The **Add Traffic Access Rule** dialog box is displayed. You can create rules for upstream traffic only.
 - Enter a description for the rule.
 - You can create a rule to allow or block upstream traffic by selecting the **Allow Traffic** or **Block Traffic** option, respectively.
 - Select the protocol that you want to use for the new traffic rule from the **Protocol** list. The following protocols are available for use:
 - › **TCP**: Transmission Control Protocol
 - › **UDP**: User Datagram Protocol
 - › **UDPLITE**: Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - › **ICMP (ICMPV4)**: Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - › **IGMP**: Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - › **ESP**: Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - › **AH**: Authentication Header protocol, which is used to authenticate SNMP.
 - › **SCTP**: Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
 - Specify the source address in the **Source** field. You can either specify a range (a network address and a subnet mask) or you can specify a source IP address. Also, specify a port number or a range of ports (for example, 22-34) for the source.
 - Specify the destination address in the **Destination** field. You can either specify a range (a network address and a subnet mask) or you can specify a destination IP address. Also, specify a port number or a range of ports (for example, 22-34) for the destination.

NOTE

If you choose ICMP (ICMPv4), the option to specify source and destination ports is not available.

11. Click **Create**. The rule that you created is displayed in the **Traffic Policy** dialog box.

NOTE

The rule that you create initially is displayed in a row with the priority set to 1 by default. When you create a second rule, it is displayed with the priority set to 1, and the previous rule is displayed in the second row with the priority set to 2. When you have created multiple rules, you can use the up and down arrows to move rows up or down to set the desired priority of the rules. The edit and delete links options at the end of each row enables you to edit or delete rules. When you click the edit button, the **Add Traffic Access Rule** dialog box is displayed where you can edit any of the rule properties.

12. Click **OK** in the **Traffic Policy** dialog box, added all the required rules.

You return to the **Advanced Network Settings** dialog box, where you can set the **Traffic Policy** button to **ON** or **OFF**, activating or deactivating the traffic policy that you created. The **Edit** option allows you to navigate to the **Traffic Policy** dialog box, where you can edit the policy that you created. The **Clear** button allows you to delete the traffic policy.

13. Toggle the **Wi-Fi Calling** option to **ON** and click **Select Profiles** to select a Wi-Fi calling profile.

By default, the **Wi-Fi Calling** is set to **OFF**

14. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.

15. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.

16. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.

17. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.

18. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.

19. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.

20. In **Mgt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.

21. **Enable 802.11k neighbor reports**: Enhances roaming by providing a list of neighbor APs to the client device.

22. **Enable 802.11r Fast BSS Transition**: 802.11r Fast BSS Transition fast roaming protocol.

23. **Client Inactivity Timeout**: Client will be disconnected from the network if it is inactive for more than the time interval specified. The timeout period can range from 60 through 1000 seconds.

24. **Directed MC/BC Threshold**: Directed multicast/broadcast threshold.

25. Click **OK** in the **Advanced Network Setting** dialog box and you return to the **Add Network** dialog box. Click the **Create** button to create the Wi-Fi network. The newly created Wi-Fi network is displayed in the **Networks** window, with the **Overview** tab displaying an overview diagram of the Wi-Fi network with various network properties. To view and edit all the network settings that you entered while creating the network, click the **Edit Network** link on the top-right corner of the **Network** page. You can make the required changes and click the **Save** button to enable the edits.

Configuring Advanced Network Settings

Advanced Network Settings include additional options for configuring the network.

After selecting other network options, this is an optional section before the network is actually created. Not all options appear for all types of network. Exceptions are highlighted. Configure the following advanced network settings:

1. In **VLAN ID**: Type the VLAN ID number (default is 1) that you want to assign to this network.
2. In **Max. Number of Devices**: (Only for Captive Portal Host Approval and Self Sign In networks) Select the maximum number of devices that can connect to the network.
The list allows up to 10 devices.
3. In **User Connection Settings (Default)**: (Only for Captive Portal networks except Click-Through)
 - **Allow the user to stay connected for**: Select Minutes or Hours from the drop-down arrow box and then use the up/down arrows to select the number of minutes or hours of connection time after which the client is disconnected.
 - **Do not redirect to the portal when reconnecting within**: You can set the grace period which sets the number of minutes during which previously authenticated clients that disconnect from the network can rejoin the network without going through the authentication process again. The default grace period is 60 minutes, but this time cannot be longer than the allowed user connection period.
4. In **User Connection Settings (Time Limited)**: (Only for Captive Portal Click-Through networks) If you have clicked the **Change to Time limited connection** option.
 - **Allow users to connect for**: Enter an aggregated time period after which the user is disconnected. The default is 24 hours.
 - **After that time, don't allow to reconnect for**: Sets a lock-out time during which users are not allowed to sign-in again. The default is 2 hours.
5. In the **Load Control** section:
 - **Max rate**: There are three options:
 - Unlimited—no limits on bandwidth allocation.
 - Per AP—The maximum bandwidth allocation limit of all connections to that specific network on the AP. If selected, two other options appear, Upload Limit and Download Limit. If either (or both) check boxes are selected, a sliding scale appears and you can drag your cursor along the line to choose the Mbps limits.
 - Per Client—The maximum bandwidth allocated for a device connected to this network. If selected, two other options appear, Upload Limit and Download Limit. If either (or both) check boxes are selected, a sliding scale appears against each option and you can drag your cursor along the line to choose the Mbps limits.
 - **Max clients per radio**: Limit the number of clients that can associate with this network per AP radio (default is 100).
 - **Enable load balancing between 2.4GHz & 5GHz radios**: Select this check box to enable load balancing between the 2.4GHz and 5GHz radios. Load balancing helps improve network performance by helping to spread the client load between the two radios on the AP.
 - **Enable load balancing between APs**: Select this check box to spread the client load between nearby access points, so that one AP does not get overloaded while another sits idle.
6. In **Access Control** section: you can define a user traffic policy by clicking the **Set up a Policy** link. The **Traffic Control Policy** dialog appears. By default, the **Allow Traffic** option (green) is enabled. You can choose to change this to **Deny Traffic** by clicking the option (red) provided.

7. To create a new traffic rule, click the **Add Rule** link. The **Add Traffic Access Rule** dialog appears. You can create rules only for up-stream traffic.

NOTE

L3/L4 traffic policy rules will not be applied to traffic between clients attached to the same WLAN on the same AP.

- Enter a description for the rule in the text field provided.
- You can create a rule to allow or block up-stream traffic by clicking and selecting the **Allow Traffic** or **Block Traffic** option, respectively.
- Select the protocol which you wish to use for the new traffic rule, from the **Protocol** drop down list. Following are the list of protocols available for use.
 - **TCP**—Transmission Control Protocol
 - **UDP**—User Datagram Protocol
 - **UDPLITE**—Lightweight User Datagram Protocol, which is a connectionless protocol that allows even a damaged data payload to be delivered rather than being discarded.
 - **ICMP (ICMPV4)**—Internet Control Message Protocol, which is an error-reporting protocol used by network devices to generate error messages to the source IP address, when issues in the network prevent delivery of IP packets.
 - **IGMP**—Internet Group Management Protocol, which is a communications protocol used by hosts on IPv4 networks to establish multicast group memberships.
 - **ESP**—Encapsulating Security Payload is a protocol which provides the authentication, integrity, and confidentiality of network packets in IPv4 and IPv6 networks.
 - **AH**—Authentication Header protocol, which is used to authenticate SNMP.
 - **SCTP**—Stream Control Transmission Protocol is a communications protocol which operates at the transport layer.
- Specify the source address in the **Source** field. You can either specify a range (a network address and a Subnet Mask, in the field provided) or you can specify a source IP address in the field provided. Also, specify a port number or a range of ports (e.g: 22-34) for the source, in the field provided.
- Specify the destination address in the **Destination** field. You can either specify a range (a network address and a Subnet Mask, in the field provided) or you can specify a source IP address in the field provided. Also, specify a port number or a range of ports (e.g: 22-34) for the destination, in the field provided.

NOTE

If you choose the ICMP protocol in the previous step, you do not need to specify ports for the source and the destination. Hence, the option to select ports will not be presented to you.

8. Click **Create**. The rule which you created appears in the **Traffic Control Policy** dialog.

NOTE

The rule which you initially create appears in a row with priority set a "1", by default. When you create a second rule, it appears in the row with priority "1" and the previous rule which you created appears as second in the row, with priority "2". When you have multiple rules created, you can use the "up" and "down" arrows available at the end of each row, to shift respective rows up or down in the order, to set the desired priority.

The edit and delete links available at the end of each row allow you to edit and delete respective rules. Each time you click the edit button, the **Add Traffic Access Rule** dialog appears where you can edit any of the rule properties.

9. Click **OK** in the **Traffic Control Policy** dialog, once you have all the required rules added.

You are navigated back to the **Advanced Network Settings** dialog, where you can click the **Traffic Policy** toggle button to "ON" or "OFF", activating or de-activating the traffic policy which you created, respectively. The **Edit** option allows you to navigate to the **Traffic Control Policy** dialog, where you can edit the policy which you created. The **Clear** button allows you to delete the traffic policy.

10. In **Enable Client Isolation**: Select this check box to prevent clients on the same network from communicating with each other.
11. In **Force DHCP**: Select this check box to force clients to obtain a valid IP address from a DHCP server. This prevents clients configured with a static IP address from connecting to the network.

If a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
12. In **Hide SSID**: Select this check box if you do not want the ID of this network advertised at any time. This will not affect performance or force the network user to perform any unnecessary tasks.
13. In **Enable OFDM only (Disables 802.11b)**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.
14. In **Enable logging client data to external syslog**: Select this check box to allow client data to be logged in all venues that have the external syslog server enabled. The box is unchecked by default. Refer to the [#unique_110](#) page for details about configuring the external syslog server for a venue.
15. In **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the network. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.
16. In **Mgt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 6 Mbps.
17. Click **Reset to Defaults** in the lower left side of the screen to reset all the advanced settings back to their defaults.
18. Click **OK** to save your settings.

You have completed configuring the advanced network settings.

Viewing APs That Are Advertising a Network

From the **APs** tab on the **Networks** page, you can view information about APs that are advertising a particular network.

To view a list of APs that are providing a particular network, follow these steps.

1. From the navigation pane, click **Networks**.

The **Networks** page is displayed.
2. From the list of networks, click the name of the network that you want to view.

The network information page displays the **Overview** tab.

3. Click the **APs** tab.

The page refreshes and then **APs** tab displays a list of APs that are currently advertising the network service, including the following information:

- **AP:** Displays the name of the AP.
- **Status:** Displays the status of AP. If everything is operating normally, the **Status** column shows **Operational**.
- **Model:** Displays the hardware model of the AP.
- **IP:** Displays the IP address or the serial number of the AP.
- **MAC address:** Displays the MAC address of the AP.
- **Venue:** Displays the name of the venue in which is this AP is physically deployed.
- **Clients:** Displays the length of time that the wireless client has been associated with the network.
- **AP Group:** Displays the name of the AP Group.
- **RF Channel:** The RF 2.4 GHz channel and 5 GHz channel
- **Tags:** Displays the tags that have been assigned to this network.

Editing a Network

Edit a network if you need to update any its current settings. For example, if you want to change the network name, description, network type settings, advanced network settings, or even the venue at which it is advertised.

Follow these steps to edit a network.

1. From the navigation pane, click **Networks**.

The **Networks** page appears.

2. From the network list, click the name of the network that you want to edit.

The network information page appears.

3. In the upper-right corner of the page, click **Edit Network**.

The **Edit Network** dialog box displays three tabs where settings can be changed:

- **Network Details:** For help with the different network details, refer to [Creating Networks Overview](#) on page 96, and click the network type.
- *network-type* **Settings:** For example, Pre-shared key Settings. For help with the different authentication options and settings for each option, refer to [Creating Networks Overview](#) on page 96, and click on the link for the network type.
- **Venues**
- **Advanced**

4. Update the network settings as required. To edit a different set of settings, click the tab for the settings.

5. Click **Save**.

Viewing LTE Clients

- [Viewing Associated LTE Clients..... 143](#)
- [Filtering Associated Clients..... 143](#)

Viewing Associated LTE Clients

Use the **Users** page to view LTE clients that are associated with your managed APs.

The **Users** page has two tabs, the default **LTE** tab, and the **WiFi** tab. The number of connected clients is shown in the tab under the tab title.

1. On the Dashboard, click **Users**.
By default, the **Users** page appears and displays the **LTE** tab, which displays LTE clients that are currently associated with your managed APs.
2. View information about your LTE clients under the following columns.
 - Venue
 - AP
 - Network
 - Clients
3. Click the name of the column to sort clients by the column name, (for example, **Venue**).
If a large number of associated clients appears on the page, sorting them by the column names is recommended.
4. Click **Refresh** in the top right of the client section to refresh the display,.

Filtering Associated Clients

Use a filter on the **Users** tab to view specific LTE clients. The filter option helpful when a large number of LTE clients are associated with APs at your venues.

Displaying Clients That Belong to a Particular Venue

By default, the **Users** page displays all LTE clients that belong to all managed venues. To display only LTE clients that belong to a particular venue, click the down arrow after **All Venues**, and then select a **venue** to view the associated LTE clients.

Displaying Clients That Are Associated with a Particular AP

By default, the **Users** page displays all LTE clients that belong to all managed APs. To display only LTE clients that are associated with a particular AP, click the down arrow after **All APs**, and then select an **AP** to view the associated LTE clients.

Managing Wi-Fi Clients and Guests

- [Viewing Associated Clients.....](#) 145
- [Viewing Client Details.....](#) 146
- [Managing Guests.....](#) 151

Viewing Associated Clients

Use the **Users** page to view wireless clients that are associated with your managed APs.

From the navigation pane, click **Users**. The **Users** page displays the **Clients** tab by default, which displays wireless clients that are currently associated with your managed APs and their details, including:

- **Device Type:** Device type
- **OS Vendor:** Device operating system
- **Model Name:** Device model name
- **IP Address:** Internet Protocol address
- **MAC Address:** MAC address of the device
- **WLAN:** Wireless Local Area Network
- **AP Name:** Access point name
- **AP MAC:** MAC address of the access point
- **Traffic:** Traffic session
- **Traffic (Uplink):** Uplink traffic
- **Traffic (downlink):** Uplink traffic
- **RSSI:** Received Signal Strength Indicator
- **SNR:** Signal-to-Noise Ratio
- **Radio Type:** Radio type
- **CPE MAC Address:** CPE MAC address
- **MCS Rate (Tx):** MCS rate (tx)
- **Effective Data Rate:** Effective data rate
- **Auth Method:** Authentication method
- **Auth Status:** Authentication status
- **Encryption:** Encryption
- **Control Plane:** Control plane
- **Packets to:** Packets sent to
- **Packets From:** Packets received from
- **Packets Dropped:** Packets dropped
- **Session Start Tim:** Session start time

If a large number of associated clients are displayed on the page, you can sort them by the column names. To sort clients by the column name, click the name of the column (for example, Venue).

Filtering Associated Clients

Use the filtering options on the **Clients** tab to display wireless clients based on the criteria you specify. These filtering options are especially useful when a large number of wireless clients are associated with APs in your venues.

Searching for Connected and Historical Clients

The **Clients** tab can display both connected and disconnected (historical) wireless clients. To search for connected clients, enter the partial or full user name or host name, MAC address, IP address, OS type, AP name, or VLAN ID in the search field, and then click the search (magnifying glass) button. The page displays any matching clients.

Search criteria for historical clients is restricted to partial or full user name, host name, or MAC address.

Connected and historical clients display in two separate lists. To view client details, click any row in the tables.

NOTE

The user name and MAC address are not case-sensitive.

ATTENTION

IP address-based searches are performed on each octet in the IP address as a number (not as a string). This means that a search match only occurs if the search string matches exactly one of the four octets in the IP address. For example, if you entered "78" in the search box, "10.104.2.78" will be a match, but "10.104.2.178" will not be a match.

Displaying Clients That Belong to a Particular Venue

By default, the **Clients** page displays all wireless clients that belong to all managed venues. To display only wireless clients that belong to a particular venue, click the down arrow after **All Venues**, and then select the venue for which you want to view associated wireless clients.

Displaying Clients That Are Associated with a Particular AP

By default, the **Clients** page displays all wireless clients that belong to all managed APs. To display only wireless clients that are associated with a particular AP, click the down arrow after **All APs**, and then select the AP for which you want to view associated wireless clients.

Viewing Client Details

You can view details about a wireless client to determine its properties, including its MAC address, IP address, and the user name used to associate it with the AP or switch. You can also view information about its connection, venue, AP or switch, network, and VLAN ID.

Follow these steps to view details about a wireless client that is currently associated with a managed AP or switch or a disconnected (historical) AP or switch clients.

NOTE

References to the name of an object managed by the Ruckus Cloud portal (Venue, AP or switch, Network, Client) display in blue to represent a link to the detail page of the object. For example, the AP name in the Connection section table, links to the AP page.

1. From menu, click **Users**.

By default, the **Wi-Fi** tab is selected.

The **Users** page loads and displays the two tabs **Wi-Fi** and **Switch**. The screen displays both connected and disconnected (historical) wireless clients with search options. When searching for disconnected (historical) clients, you can only search by MAC address, hostname or username.

NOTE

If a large number of clients appears on the **Clients** page, use the filtering options to narrow down the client list. Refer to [Filtering Associated Clients](#) on page 146 for more information.

2. From the list of currently associated clients, locate the wireless client (connected or disconnected) for which you want to view details, and then click its MAC address.

The **Client MAC Address** page appears and displays three sections across two panes followed by five report-type sections.

3. In the **Client Properties** section, information about the wireless client's network properties information displays.

The following table lists the client property details for connected and disconnected clients:

TABLE 7 Client Property Details

MAC Address	MAC address of the wireless client
Device OS	Operating System icon and name
Host Name	Product name
User Name	User name used to associate with wireless client with the managed AP
Status	Current status of the wireless client

4. In the **Connection** section, information about the wireless client's connection information displays.

The following table lists the client's current connection details:

TABLE 8 Client's Current Connection Details

Connected Time	Length of time that has elapsed since the wireless client associated with the managed AP
IP Address	IP address assigned to the wireless client
AP Name	Name of the AP with which the wireless client is associated
Venue	Venue name where the client is located
Network	Network name
Connected to SSID	SSID on the managed AP to which the wireless client is associated
VLAN ID	ID number of the VLAN
Connected to BSSID	BSSID on the managed AP to which the wireless client is associated

For disconnected clients, the connection information displays as a **Last Session** section with the following details for the disconnected client's last session:

TABLE 9 Disconnected Client's Last Session

Start and End Time	Start and end time of the last session of the disconnected wireless client associated with the managed AP
Session Duration	Duration of the last connected session
Last IP Address	Last IP address assigned to the wireless client

TABLE 9 Disconnected Client's Last Session (continued)

Last AP Connected to	Name of the last AP with which the wireless client is associated
Last Venue	Name of last venue where the client is located
Last SSID	SSID on the managed AP to which the wireless client is associated

5. In the **Operational Data for Current Session** section, information about the wireless client's operational data displays.

The following table lists the operational data details for current connected clients (this information is not available for disconnected clients):

TABLE 10 Operational Data Details

RF Channel	Radio Frequency (RF) channel number
Transmitted Bytes	Number of bytes, in kilobytes, sent during this current session
Transmitted Packets	Number of packets in total, sent during this current session
Received Bytes	Number of bytes received during this current session
Received Packets	Number of packets in total, received during this current session
Frames Dropped	Number of frames dropped during this current session
RSSI	The received signal strength indicator, expressed in dBm. The value may be expressed in three colors - green, orange or red. Green represents good signal strength, orange represents moderate signal strength, and red represents poor signal strength.
SNR	The signal-to-noise ratio, expressed in decibels (dB). The signal power indicator adjacent to the value indicates signal strength. Higher value indicates more power.

6. In the **Client Information for Last 7 Days (Date-start-to-date-finish)** section you can choose to display the information for 24 hours or 7 days using the drop-down arrow on the right of the screen.

The following report information in table or graphical format is displayed:

- Historical Stats—the following information is displayed for both connected and disconnected clients:
 - Number of APs that are connected
 - Average rate in Bytes
 - User traffic in MB
 - Number of applications being used
 - Average session length in minutes and seconds
 - Number of sessions
 - Slider graphic showing use of the radio bands 2.4GHz and 5GHz in Bytes, GB, or MB
- Traffic Trend
- Top 10 Applications by Traffic Volume
- Events History
- Session History

Review the information for any patterns or trends.

Viewing Switch Clients

7. From menu, click **Users**.

The **Users** page loads and displays.

8. Select the **Switch** tab.

The switch clients page appears displaying the list of clients with the following information.

- **MAC Address:** MAC address of the switch client.
- **Description:** Description about the switch client.
- **Device Type:** the device type.
- **Venue:** The name of the venue.
- **Switch:** the name of the switch.
- **Port:** The port number of the switch.
- **VLAN:** The VLAN ID.

9. Click on a switch client to view its properties.

FIGURE 32 Switch Client Properties

The screenshot displays the 'Client Properties' page for a switch client. At the top, the breadcrumb 'Clients >' and the MAC address 'CC:4E:24:89:BC:87' are visible, along with an 'Export' link. The page is divided into two main sections: 'Device' and 'Connection'. The 'Device' section lists the following properties: MAC Address (CC:4E:24:89:BC:87), Device Type (Router), Description (N/A), and Status (Connected). The 'Connection' section lists: Switch (ICX7150-48ZP-C14U20), Port (1/1/16), Venue (Lab-East), and VLAN (VLAN-ID: 1).

The switch **Client Properties** page displays the following information.

Device

- **MAC Address:** MAC address of the switch client.
- **Device Type:** the device type.
- **Description:** Description about the switch client.
- **Status:** The status of the connection.

Connection

- **Venue:** The name of the venue.
- **Switch:** the name of the switch.
- **Port:** The port number of the switch.
- **VLAN:** The VLAN ID.

Managing Guests

You can learn to generate and manage guest passes, which allow temporary users to connect to your Ruckus Cloud wireless networks.

Creating a Guest Pass

If you have a user that requires temporary access to the network (for example, a company visitor or a temporary worker), you can create a guest pass for that person.

NOTE

If you need to create guest passes for multiple users, you can create them in bulk. For more information, see [#unique_126](#).

Complete the following steps to create a single guest pass.

1. From the navigation pane, click **Users**.
The **Users** page is displayed.
2. Select the **Guest Pass Credentials** tab.
3. If you see the message “Guest cannot be added since there are no guest networks,” click the **Add a Captive Portal network with Guest Pass** option.

A modified version of the network wizard window appears with the Guest pass as the network type. Complete the rest of the steps in [Creating a Network That Uses a Captive Portal with a Guest Pass](#) on page 131 to add a guest network.

4. In the upper-right corner of the **Guest Pass Credentials** tab, click **Add Guest**.

The **Add Guest Pass** form appears

FIGURE 33 Adding a Guest Pass

Add Guest Pass

* Guest Name:

* Mobile Phone:

Email:

Notes:

* Allowed Network:

* Pass is Valid For:

Pass is Valid From: Now First Log-In

Number of devices:

Send to Phone

Send to Email

Print guest pass

* Required field

5. Complete the following fields to identify the user of this guest pass:

- **Guest Name:** Type the name of guest.
- **Mobile Phone:** Type the mobile phone number of the guest. The mobile phone number must follow the format: + {country code}-{area code}-{phone number}. For example, you can type +1-408-888-8888.

NOTE

Based on the browser locale, the default country is displayed for the **Mobile Phone** field.

- **Email:** Type the email address of the guest.
- **Notes:** Type any notes or additional information about the guest.
- **Allowed Networks:** Select a network to which you want this guest to have access. Only managed guest networks appear on this list. If you have not created a managed guest network, this list will be empty.
- **Pass is Valid For:** Select the number of hours or days for which the guest pass will be valid.
- **Pass is Valid From:** Check either **Now** or **First Log-in**.
- **Number of Devices:** Select the number of devices on which the guest pass can be used simultaneously. In addition to the option of adding a definite number of clients ranging from 1 to 5, you have the option of adding unlimited number clients under the guest.

6. Specify how you want the guest user to receive the instructions for activating the guest pass. Options include:

- **Send to Phone:** Click to send the guest pass information to the guest's phone via SMS.
- **Send by Email:** Click to send the guest pass information to the guest's email address.
- **Print guest pass:** Click to print a hard copy of the guest pass, which you can give to the guest user.

NOTE

If you are printing the guest pass, remember to temporarily disable your web browser's pop-up blocker (if enabled).

You can select multiple guest pass delivery methods.

7. Click **Create Guest**.

Ruckus Cloud sends the guest pass information to the guest using the delivery methods you selected. The **Guest Pass Credential** page refreshes, and then an entry for the guest pass that you have created appears.

Viewing Guest Passes

Complete the following steps to view a summary of all the guest passes that have been created in your Ruckus Cloud account.

1. From the navigation pane, click **Users**.

The **Users** page is displayed.


2. Select the **Guest Pass Credentials** tab.

The **Guests** page displays a table that summarizes all *existing* guest passes. Available information on each guest pass includes:

- **Created:** Date and time when the guest pass was created.
- **Name:** Name of the guest user.
- **Phone:** Phone number of the guest user.
- **Email:** Email address of the guest user.
- **Type:** Type of user account.
- **Allowed SSID:** SSID of the network to which the guest user has access.
- **Expires:** Date and time when the guest pass will expire.
- **Status:** Current connection status of the guest user.

NOTE

A status shown as **N/A** implies that there may be an unlimited number of clients connected to the guest. Unlimited guests can have three statuses: N/A, Disabled, and Expired, unlike the normal guest which can have two additional statuses: Online and Offline.

-  : Click to view the guest pass details, which displays all the preceding information in the **Guest Details** dialog box. For more information, refer to [Viewing Guest User Details](#) on page 153.
3. To view details of previously created guest passes that have already expired, click the **Show expired guests** check box in the upper-right corner of the page.
 4. If you have a large number of guest passes, use the filtering options in the upper-left corner of the page to display guest passes based on the criteria you specify. For example, if you know the name, phone number, or email address of the guest user, enter it in the first field. If you want to filter the results further, click the **Creation Time** check box, and then select the date from the calendar on which the guest pass was created.

Viewing Guest User Details

You can view guest user details to review the SSID to which the guest user is assigned or to determine when the guest user account will expire.

Complete the following steps to view the details of a guest user.


1. From the navigation pane, click **Users**.

The **Users** page is displayed.

2. Click the **Guest Pass Credentials** tab.

A table that displays a summary of all guest users that have been created appears.

3. Locate the guest user for which you want to view the details.

4. Click  (Manage Guest icon) that is in the same row as the guest user name.

The **Guest Details** page displays the following information:

- Guest Type
- Guest Name
- Mobile Phone
- Email
- Notes
- Allowed Network
- Guest Created
- Access Expires
- Max number of clients (that can use the same guest user account)
- Status, which shows the status of the connected client, along with the number of clients connected. If the client is online, it is called out as Online in green. If the client is not online, it is called out as offline, in gray.

NOTE

A status shown as **N/A** implies that there are an unlimited number of clients connected to the guest. Unlimited guests can have three statuses: N/A, Disabled, and Expired, unlike the normal guest which can have two additional status: Online and Offline.

FIGURE 34 Guest Details

You can download the GDPR record of the client as a CSV file, by clicking the **Download Private Guest Information** link available in the **Status** field. You are prompted to save the CSV file with the file name containing guest name and the time stamp. Click **Save** to download the file. Open the file to view the details such as guest name, mobile number (along with relevant country code), guest creation and expiry date.

NOTE

The **Download Private Guest Information** link is available for all users except Guests Manager.

In addition, a static table at the bottom of the report displays a list of accessible information, who can access each information, and why they are allowed to access.

You can also find the following links in the upper-right corner of the Guest Details screen:

- **Generate New Password:** Click to generate a new password for this guest user account. For more information, refer to [Generating a New Guest User Password](#) on page 156.
- **Download Private Guest Information:** Click to download guest information. For more information, refer to [#unique_130](#).
- **Disable Guest:** Click to disable this guest user account. For more information, refer to [Disabling a Guest User](#) on page 156.
- **Delete Guest:** Click to delete this guest user account. For more information, refer to [Deleting a Guest User](#) on page 157.

Disabling a Guest User

If you want to prevent a guest user from accessing the network temporarily, you can disable the guest user account.

NOTE

If you want to permanently delete the guest user account, refer to [Deleting a Guest User](#) on page 157.

Follow these steps to disable a guest user.

1. On the navigation pane, click **Users**.
The **Users** page appears.
2. Select the **Guest Pass Credentials** tab.
A table that displays a summary of all guest users that have been created appears.
3. Click name of the guest user name.
The **Guest Details** dialog appears.
4. In the upper-right corner of the screen, click **Actions** and click **Disable Guest**.
The guest information is downloaded in a .csv file.
5. Click **Close**.

You have completed disabling the guest user account. To enable the guest user account again, go to the **Guest Details** screen, and then click **Enable Guest**.

Generating a New Guest User Password

If you want a guest user to use a different password (for example, if the password has been compromised) to access the network, you can generate a new guest user password.

Complete the following steps to generate a new guest user password.


1. From the navigation pane, click **Users**.
The **Users** page is displayed.
2. Select the **Guest Pass Credentials** tab.
A table that displays a summary of all guest users that have been created appears.
3. Click name of the guest user name for whom you want to generate a new password.
The **Guest Details** dialog appears.
4. In the upper-right corner of the screen, click **Actions** and click **Generate New Password**.


- Specify how you want to send the new password to the guest user by selecting one or more of the following check boxes:
 - Send to phone
 - Send by email
 - Print guest pass


FIGURE 35 Generating New Password

Generate New Password

How would you like to give the new password to the guest:

 Send to phone

 Send by Email

 Print guest pass

Cancel Generate

- Click **Generate**.

Ruckus Cloud generates the new password and sends it to the guest user using the delivery method or methods that you selected in the previous step.

Deleting a Guest User

If a user no longer needs the guest account you can delete the account from Ruckus Cloud.

NOTE

If you want to temporarily disable the guest user account, refer to [Disabling a Guest User](#) on page 156.

Complete the following steps to delete a guest user.

- From the navigation pane, click **Users**.
The **Users** page is displayed.
- Select the **Guest Pass Credentials** tab.
A table that displays a summary of all guest users that have been created appears.
- Select the name of the guest user that you want to delete and click **Delete**
- Alternatively, click name of the guest user name.
The **Guest Details** dialog appears.

Managing Wi-Fi Clients and Guests

Managing Guests

5. In the upper-right corner of the screen, click **Actions** and click **Delete Guest**.

A confirmation message appears.

6. Click **Delete Guest**.

The guest user account that you deleted is removed from the **Guest Pass Credentials** tab.

Monitoring Events

- [Event Monitoring Overview.....](#) 159
- [Event Severity Levels.....](#) 159
- [Event Types.....](#) 159
- [Event List.....](#) 160
- [Viewing Events.....](#) 162
- [Exporting Events to a CSV File.....](#) 163

Event Monitoring Overview

An event is an occurrence or the detection of certain conditions in and around the network. An AP being rebooted, an AP changing its IP address, and a user connecting to a WLAN are all examples of events.

Ruckus recommends that you regularly monitor events to stay current on any network conditions that can potentially affect your wireless networks and wireless users.

NOTE

Events that require your attention are called *alarms*.

Events are assigned different severity levels and types.

Event Severity Levels

A severity level is assigned to every event generated in the Ruckus LTE AP Management Service.

Events are assigned the following severity levels:

- **Critical**—Indicates a serious issue that requires your immediate attention.
- **Indeterminate**—Indicates a notification about an event or condition.
- **Informational**—Indicates simple informational notification.
- **Major**—Indicates the occurrence of an issue that may cause a device or service to fail.
- **Minor**— Indicates a minor error in the system.
- **Warning**—Indicates about an event that might led to a critical or major issue.

Event Types

Events in the Ruckus LTE AP Management Service are classified into the following types: Admin, AP, Client, and Notification.

- **Admin:** Events that occur within the AP Management Service, including the web interface.
- **AP:** Events that occurs on managed APs. For example, when the configuration settings of an AP are updated and when an IP address of an AP changes.
- **Client:** Events that occur on LTE clients that are associated with any of your managed APs.

Monitoring Events

Event List

- Notification:** Informational notifications such as an upcoming license expiration, disconnection of an AP from the AP Management Service, Ruckus partner accepting customer invitation and so on. Ruckus LTE AP Management Service notifies administrative users about important events via email and SMS.

Event List

View a complete list of events that may appear on the Ruckus LTE AP Management portal, including their event IDs and recommended actions (if any).

For more details about the events, refer to the latest *Ruckus LTE Alarms and Events Guide* for the Ruckus Small Cell product family.

TABLE 11 Ruckus LTE AP Management Events

Event ID	Event Message	Severity	Recommended Action
101	The RSC temperature is too high and therefore the LTE radio has been disabled	Major	
102	RSC temperature is higher than expected	Minor	
105	LTE Radio OpState is disabled	Minor	No action is required.
108	Sync Lost: All Sync sources lost: Alarm is triggered when all sync sources are lost	Warning	LTE AP is expected to reboot after half an hour of sync loss based on configuration.
109	Sync holdover expired: Holdover timeout: Alarm is triggered	Minor	LTE AP reboots.
111	EPC SeGW connection lost. Link down for a peer with which EPC IPsec tunnel is established	Major	LTE AP retries IPsec tunnel reestablishment until reboot.
112	S1AP connection lost. RRC/SCTP association failure alarm	Minor	Cell transmission is disabled.
115	File upload failure - Failure in streaming KPIs to MQTT Broker, Failed to upload KPIS to File Server/MQTT broker	Major	No action is required.
117	Firmware image download failure. Software Activation/Download failure	Major	No action is required.
119	Configuration image download failure: Download Failure: SwMgr failed to download the configuration image	Major	No action is required.
120	File persistence error: No vendor config file present: File is no longer present or has been corrupted	Major	No action is required.
122	Server authentication failure	Major	
123	Server certificate revoked	Major	
124	Server revocation check failure	Major	LTE AP retries OCSP procedure until reboot timer expires.
125	OCSP/CRL Server not reachable	Major	
126	Server Root CA certificate missing or expired	Major	
127	NTP Sync cannot be established. NTP synchronization is not achieved.	Minor	No action is required.
128	Ruckus PKI RA/CA is not reachable.	Major	
129	LTE AP disconnected from management cloud	Major	
130	Enrollment failure for NHN PKI	Major	
133	CBSD Registration error	Minor	Retry if SAS was not reachable, else wait for user action.
134	CBSD Grant Error - SAS grant unsuccessful	Minor	

TABLE 11 Ruckus LTE AP Management Events (continued)

Event ID	Event Message	Severity	Recommended Action
135	CBSD Grant Suspended - GRANT SUSPENDED due to Transmit Timer Expiry, SAS-CBSD Procedure Failure.	Major	Attempt re-registration procedure or grant on different channel/issue spectrum inquiry.
136	SAS Certificate expired: Certificate Outdated.	Critical	Retry procedure with SAS.
137	SAS Certificate invalid: Security procedure failure with SAS.	Major	Retry
138	SAS is not reachable	Major	Retry to connect to SAS.
139	CBSD installation error.	Minor	No action is required.
141	CBSD location is modified without CPI.	Critical	Report the alarm.
142	CBSD location might be modified without CPI	Major	No action is required.
304	RSC disconnected from management cloud SeGW	Informational	
307	RSC IKESA IP address renewal was initiated	Informational	
308	RSC IKESA establishment timeout	Informational	
309	RSC is not authorized	Informational	
310	RSC authentication failure — RSC client certificate has been revoked	Informational	
314	RSC Integrity/Confidentiality algorithm could not be successfully negotiated	Informational	
501	RSC authentication successful	Informational	
502	CBSD registration is successful	Informational	
503	CBSD grant is successful	Informational	
505	CBSD HB with operational param	Informational	
507	CBSD grant relinquished	Informational	
508	CBSD deregistered	Informational	
901	GPS Session could not be established or maintained - Location source is missing or lost	Major	No action is required.

Viewing Events

An event in the Ruckus LTE AP Management is any significant occurrence on managed APs, associated clients, or in the system that requires tenants to be notified, whether for an immediate action or information purposes.

1. On the Dashboard, click **Events**.

The **Events** page appears and displays the 50 most recent events that have occurred in your AP Management account. If the AP Management has recorded more than 50 events, the right-bottom area of the page displays left (<) and right (>) arrows that you can click to view older events.

Event details that are displayed on the page include:

- **Date:** Date and time when the event occurred.
- **Severity:** Severity level assigned to the event. For more information, refer to [Event Severity Levels](#) on page 159.
- **Event Type:** Indicates where the event occurred (managed AP, associated client, or administrative). For more information, refer to [Event Types](#) on page 159.
- **Source:** Name of the AP, client, or administrative component on which the event occurred.
- **Identifier:** MAC address or the serial number of the LTE AP or SecGW.
- **Model:** The model number of the LTE AP.
- **Description:** The Alarm ID and description of the event .

2. (Optional) Click the **View Event** icon to view the event details.
3. To view the next page, click the right arrow (>). To jump to the last page of events, click the >| arrow.

You can also filter the events that are displayed on the page by using the filtering options at the top of the page.

- **All Severities**—Click the drop-down arrow to select the severity level by which the list of events is sorted.
- **All Event Types**—Click the drop-down arrow to select the event type (Admin, AP, Client, or Notification) by which the list of events is sorted.
- **Jump To**—Click **Time** to select a date by which the list of events is sorted.
- Use the **Search in description** box, type a keyword that you want to use for any matching events. Click the magnifying glass icon to start the search.

4. (Optional) Click **Export to CSV** to export the list of events to a .csv file.

The **Exporting Events** dialog appears and the list of events are downloaded as a .csv file (for example, Events_25_11_2019_13-40.csv) in the default download directory of your systems. You can open and review the .csv file using Microsoft Excel.

NOTE

You can view and export a maximum number of 10,000 records from the current page on the portal. The portal displays the events ordered by the event date and time. If the number of records exceed 10,000, contact the Ruckus Support team.

You have completed viewing events in your Ruckus LTE AP Management account.

Exporting Events to a CSV File

Beginning with the Ruckus LTE 2019.02 release, you can export the list of events in your account to a .csv file.

1. From the side bar menu, click **Events**.

The **Events** page appears and displays the 50 most recent events that have occurred in your AP Management account. If the AP Management has recorded more than 50 events, the right-bottom area of the page displays left (<) and right (>) arrows that you can click to view older events.

The **Export to CSV** option is available in all **Events** pages such as tenant, venue, network, and AP levels.

2. In the upper-right corner, click **Export to CSV**.

The **Exporting Events** dialog appears and the list of events are downloaded as a .csv file (for example, Events_25_11_2019_13-40.csv) in the default download directory of your systems. You can open and review the .csv file using Microsoft Excel.

NOTE

You can view and export a maximum number of 10,000 records from the current page on the portal. The portal displays the events ordered by the event date and time. If the number of records exceed 10,000, contact the Ruckus Support team.

You have completed exporting events in your Ruckus LTE AP Management account.

Viewing Analytics

- [Analytics Overview](#)..... 165
- [Available LTE Analytics Report](#)..... 165
- [Available Analytics Reports](#)..... 172
- [Viewing and Filtering Wi-Fi Analytics Data](#)..... 174

Analytics Overview

Ruckus LTE AP Management Service has a set of analytics that gives you a deeper insight into your network statistics. Using a wide variety of common use cases, you can analyze the network capacity, traffic trends, client statistics, and device inventories.

Using the reports, you assess the followings:

- Network capacity, carried traffic, and utilization
- User experience (getting on the network, connection speed - simple high/low/ average and CDF views)
- User activity (devices, applications, sessions, and bandwidth)
- AP behavior (channel changes, meshing, band steering, and load balancing)
- Network operating conditions (interference sources)
- Usual network mechanics (uptime, alarms, and so on)
- Capability to view statistics at multiple layers (AP, radio, SSID) and session

Ruckus LTE AP Management Service offers a number of analytics reports that you can generate to analyze your Wi-Fi and LTE network, grouped separately under two tables, **WiFi** and **LTE**. The LTE KPIs are available in both the report and plots format.

Available LTE Analytics Report

From The LTE analytics tab, you can access the KPI (Key performance indices) reports.

Ruckus LTE AP Management Service has the following KPI reports:

- [Accessing LTE KPIs](#) on page 170—provides summary of a variety of KPIs for a specific time period, which helps you monitor the Venues and AP performance.
- [Plots](#) on page 171—enables you to plot the relevant LTE KPIs as visual representation of metrics against time to monitor LTE venues and performances of APs.

Statistics Supported in LTE AP

The following table provides information about statistics supported by an LTE AP.

TABLE 12 Ruckus LTE Statistics

Statistics	Description
networkTenantId	This counter is used for reporting the identification number of network tenant.
networkName	This counter is used for reporting the name of the network.
networkClientsCount	This counter is used for reporting the total number of network clients.
radioFreq	This counter is used for reporting the radio band indicator.

Viewing Analytics

Available LTE Analytics Report

TABLE 12 Ruckus LTE Statistics (continued)

Statistics	Description
radioFreqId	This counter is used for reporting the identity of an LTE AP.
plmnid	This counter is used for reporting the PLMN identity of RSC.
Number of Dropped Calls (erabRelEnbNbrSum)	This counter is used for reporting the total number of dropped calls. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
RRC Connection Establishment Attempts (rrcConnEstabAttSum)	This counter is used for reporting the total number of RRC connection establishment attempts. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
RRC Connection Establishment Successes (rrcConnEstabSuccSum)	This counter is used for reporting the number of successful RRC connections. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
RRC Connection Reestablishment Attempts (rrcConnReEstabAttSum)	This counter is used for reporting the number of reestablishment attempts for RRC connection. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
RRC Connection Reestablishment Successes (rrcConnReEstabSuccSum)	This counter is used for reporting the number of reestablishment successes for RRC connection. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Initial E-RABs Setup Attempts (erabEstabInitAttNbrSum)	This counter is used for reporting the number of initial E-RABs establishment attempts. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Initial E-RABs Setup Successes (erabEstabInitSuccNbrSum)	This counter is used for reporting the number of initial E-RABs establishment successes. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Additional E-RAB Setup Attempts (erabEstabAddAttNbrSum)	This counter is used for reporting the number of additional E-RABs establishment attempts. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Additional E-RAB Setup Successes (erabEstabAddSuccNbrSum)	This counter is used for reporting the number of additional E-RABs establishment successes. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Handover Attempts(eutranToEutranHoOutAttTargetSum)	This counter is used for reporting the number of HO attempts. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Handover Successes (eutranToEutranHoOutSuccTargetSum)	This counter is used for reporting the number of successful HO. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Cell Unavailable Time (cellUnavailableTime)	This counter is used for reporting the time for which RSC is unavailable.
Average Number of Active UEs (numOfActiveUE)	This counter gives the instantaneous number of active UEs.
SAS Unavailability (sasUnavailableTime)	This counter is used for reporting the time for which SAS is unavailable.
GPS Unavailability (gpsUnavailableTime)	This counter is used for reporting the number of seconds elapsed between the last GPS/GNSS unavailability until the GPS availability.
Phase Sync Loss Time (phaseSyncLossTime)	This counter is used for reporting the number of seconds elapsed between the last PTP phase sync loss until the PTP phase sync lock.
Average DL Throughput (Mbps) (txKbps)	This counter is used for reporting the average downlink throughput. This counter is used to calculate per venue or system KPI using $(\sum \text{ of all RSC})/\# \text{ of RSC}$.
Average UL Throughput (Mbps) (rxKbps)	This counter is used for reporting the average uplink throughput. This counter is used to calculate per venue or system KPI using $(\sum \text{ of all RSC})/\# \text{ of RSC}$.
DL Traffic Volume (GBytes) (dlTrafficVolume)	This counter is used for reporting the volume of downlink traffic in bytes. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
UL Traffic volume (GBytes) (ulTrafficVolume)	This counter is used for reporting the volume of uplink traffic in bytes. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Frequency Sync Loss Time (frequencySyncLossTime)	This counter is used for reporting the duration for which frequency synchronization is lost, including PTP ACQUIRING state. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
Percentage Phase Locked (percentagePhaseLocked)	This counter is used for reporting the percentage of the duration for which PTP phase is locked. The sum of this counter from all RSCs can be used to calculate per venue/system KPI.
configuredSyncSource	This counter is used for reporting the configured sync source of RSC.
holdoverTime	This counter is used for reporting the Holdover time.
numOfTfcsStateTransToGpsLocked	This counter is used for reporting the number of times GPS is locked in the TFCS state.

TABLE 12 Ruckus LTE Statistics (continued)

Statistics	Description
numOfTfcsStateTransToHoldover	This counter is used for reporting the number of holdover in the TFCS state.
numOfTrackedSatellites	This counter is used for reporting the number of tracked satellites.
numOfPtpSlaves	This counter is used for reporting the number of PTP slaves.
numOfTfcsStateTransToPhaseLocked	This counter is used for reporting the number of time PTP is phase locked.
syncRecoveryTime	This counter is used for reporting the sync recovery time.

KPIs Supported in LTE AP

The following table provide information about KPIs supported by LTE APs.

TABLE 13 System KPIs

KPI	Description
DCR (Dropped Call Rate)	To calculate Dropped Call rate, use the following formula: $(100 * A) / (B + C)$ <p>A = Number of dropped calls B = Number of additional E-RABs successful to setup C = Number of initial E-RABs successful to setup</p> To calculate per venue/system, use \sum of all RSCs.
RRC Connection Establishment Success rate	To calculate RRC Connection Establishment Success rate, use the following formula: $(\sum A / \sum B) * 100$ <p>where A = Number of RRC connection establishment successes B = Number of RRC connection establishment attempts</p> To calculate per venue/system, use \sum of all RSCs.
RRC Connection Re-establishment Success rate	To calculate RRC Connection Re-establishment Success rate, use the following formula: $(\sum A / \sum B) * 100$ <p>where A = Number of RRC connection re-establishment successes B = Number of RRC connection re-establishment attempts</p> To calculate per venue/system, use \sum of all RSCs.
Initial E-RAB Setup Success rate	To calculate initial E-RAB Setup Success rate, use the following formula: $(\sum A / \sum B) * 100$ <p>where A = Number of initial E-RABs successful to setup B = Number of initial E-RABs attempted to setup</p>
Additional E-RAB Setup Success rate	To calculate additional E-RAB Setup Success rate, use the following formula: $(\sum A / \sum B) * 100$ <p>where A = Number of additional E-RABs successful to setup B = Number of additional E-RABs attempted to setup</p>

TABLE 13 System KPIs (continued)

KPI	Description
Initial Bearer Setup Success Rate	To calculate Initial Bearer Setup Success rate, use the following formula: $(A*100)/B$ where A = Number of initial E-RABs successful to setup B = Number of initial E-RABs attempted to setup
Additional Bearer Setup Success Rate	To calculate Initial Bearer Setup Success rate, use the following formula: $(A*100)/B$ where A = Number of additional E-RABs successful to setup B = Number of additional E-RABs attempted to setup
Handover Success rate	To calculate Handover Success rate, use the following formula: $(\sum A/\sum B)*100$ where A= Number HO successes B = Number HO attempts
SAS Availability	To calculate SAS Availability, use the following formula: $[(A-B)/A]*100$ where A = Measurement Period B = SAS unavailable time
Cell Availability	To calculate cell availability, use the following formula: $[(A-B)/A]*100$ where <ul style="list-style-type: none"> • A = measurement_period • B = sum of cell unavailable time
Average Cell Availability	To calculate average cell availability per venue/system, use the following formula: $\{ 1 - (U/T) \} * 100 = \%$ where <ul style="list-style-type: none"> • U = average cell unavailability in seconds = (S/R) <ul style="list-style-type: none"> – S = sum of all Cell Unavailable time from all RSCs – R = total number of RSCs • Reporting interval in seconds To calculate average cell availability for plots, compute and display cell availability on the charts/plots (if possible) or the reported Cell unavailability time.
Average number of Active UEs	To calculate average number of active UEs per venue/system, use sum of all UEs for RSCs.
Total DL Traffic Volume (GBytes)	To calculate total DL traffic volume per RSC, use the following formula: \sum of all dlTrafficVolume reported for the RSC in a given interval of reporting time.
Total UL Traffic Volume (GBytes)	To calculate total UL traffic volume per RSC, use the following formula: \sum of all ulTrafficVolume reported for the RSC in given a interval of reporting time.

TABLE 13 System KPIs (continued)

KPI	Description
Frequency Synchronized	<p>Frequency synchronized is reported as A or calculated in percentage value as $\text{Frequency Synchronization} = (1-A/T)*100$ where $A = \sum \text{ of all frequencySyncLossTime reports for all RSC with GPS} / \# \text{ no. of RSC with GPS}$ $T = \text{Reporting Time interval}$</p>

TABLE 14 System Throughput KPIs

KPI	Description
Average DL Throughput (Mbps)	To calculate per venue/system, use $(\sum \text{ of all RSCs})/\# \text{ of RSCs}$.
Average UL Throughput (Mbps)	To calculate per venue/system, use $\sum \text{ of all RSCs}$.
DL Traffic Volume (GBytes)	To calculate per venue/system, use $\sum \text{ of all RSCs}$.
UL Traffic Volume (GBytes)	To calculate per venue/system, use $\sum \text{ of all RSCs}$.

TABLE 15 System GPS KPIs

KPI	Description
GPS Availability	<p>The GPS availability is reported as A or calculated in percentage value as $\text{GPS Availability} = (1-A/T)*100$ where $A = (\sum \text{ of all gpsUnavailableTime reports for each RSC with GPS as timing source} / \# \text{ no of RSC with GPS}) - \text{Reporting Time}$ $T = \text{Reporting Time interval}$</p>
Phase Locked	<p>To calculate Phase Locked, use the following formula: $[(A-B)/A]*100$ where $A = \text{measurement_period}$ $B = \text{Phase sync loss time}$ For per venue KPI, use the following formula: $\text{Phase sync loss time} = \sum \text{ of all GPS RSC} / \# \text{ no of RSC with GPS}$</p>
Holdover	<p>To calculate Holdover, use the following formula: $100-A$ where $A = \text{Percentage of time in Phase Locked}$ To calculate per venue KPI, use the following formula: $\text{percentagePhaseLocked} = \sum \text{ of all percentageHoldover from RSC with GPS} / \# \text{ no of RSC with GPS}$</p>
Frequency Phase Recovery	<p>To calculate Frequency Phase Recovery, use the following formula: $(A/B)*100$ where $A = \text{Frequency Sync Loss Time}$ $B = \text{meaurement_period}$ To calculate per venue KPI, use the following formula: $\text{frequencySyncLossTime} = \sum \text{ of all GPS RSC} / \# \text{ no of RSC with GPS}$</p>

Accessing LTE KPIs

KPIs are the important performance parameters that are required to troubleshoot and optimize the LTE network and check the performance of the most essential network functions.

- **Summary Report:** Select the time range, venue and APs from the respective drop-down and click **Apply** to view the following System KPI reports:
 - **RRC Connection Establishment Success Rate:** The Radio Resource Control (RRC) protocol connects UE/Clients (CBRS compliant LTE device such as a dongle or a phone) with LTE AP. A RRC connection is successful when an UE performs the call establishment procedure, and get resources from the LTE AP. The connection success rate is displayed as a percentage, computing the successful connections against total connection attempts. An acceptable success rate percentage is displayed in green color and a poor success rate is displayed in red.
 - **RRC Connection Reestablishment Success Rate:** The re-establishment procedure is required in order to re-establish the lost RRC connection. This procedure is successful only when LTE AP has a valid UE context. A re-establishment is initiated upon detecting radio link failure, handover failure, mobility failure, integrity check failure and when there is a RRC connection reconfiguration failure. The connection re-establishment success rate is displayed as a percentage, computing the successful re-connections against total re-connection attempts. An acceptable success rate percentage is displayed in green color and a poor success rate is displayed in red.
 - **Initial E-RAB Setup Success Rate:** After the UE sends the RRC setup complete message to the LTE AP, the LTE AP sends an initial UE message to the MME indicating that the purpose of the UE and its credentials. When the MME receives this message and it decides that a bearer is required, it sends an initial Context setup request to the LTE AP. This message is considered as the initial EPS Radio Access Bearer (E-RAB) attempt, as it contains the bearers to be added.

The initial connection setup success rate is displayed as a percentage, computing the successful connections against total connection attempts. An acceptable success rate percentage is displayed in green color and a poor success rate is displayed in red.
 - **Additional E-RAB Setup Success Rate :** The additional E-RAB success rate is displayed as a percentage, computing the successful additional connections against total connections.
 - **Handover Success Rate:** This KPI is used to measure the performance of network when handling the movement of users and still retain the service for the user. When the source LTE AP sends RRC connection reconfiguration message to the UE, an inter LTE AP hand over is done. The number of the attempted handover is calculated at the source cell. The hand over success rate is displayed as a percentage, computing the successful handover against total handover attempts. An acceptable success rate percentage is displayed in green and a poor success rate is displayed in red.
 - **Dropped Call Rate (DCR):** DCR in LTE network is a scenario when a user's ongoing session is dropped, terminated abruptly, and unintentionally, requiring the user to initiate a new connection to resume services. At the LTE AP level, this is considered as an abnormal release which can be verified from the error code inside the Context Release message. The DCR is displayed as a percentage, computing the number of dropped calls against total calls handled. An acceptable DCR percentage is displayed in green color and a poor rate is displayed in red.
 - **SAS Availability:** For LTE APs to remain in the transmitting state, a valid grant from SAS is mandatory. Each AP is constantly communicating with SAS via the heartbeat mechanism. Therefore, it is critical that the SAS connection with LTE AP is always available. For any SAS outages, a counter is maintained to record the percentage of time for which SAS is available to track LTE AP service availability.
 - **Cell Availability:** Each LTE AP is referred to a Cell as per LTE protocol terminology. Each Cell is considered as available when an LTE AP can provide the E-RAB service in the cell. This KPI is calculated as the percentage of time that the cell is considered available against the total measurement time. A healthy percentage is displayed in green, and a poor percentage is displayed in red.
- **Throughput statistics:** The following KPIs measures various data traffic statistics in terms of throughput (Mbps) and volume (GBytes) for the Down Link (DL) and the Up Link (UP) direction.
 - **Average DL throughput (Mbps):**This KPI measures the average rate at which data is transferred from the LTE AP to the UE, within a selected reporting interval.
 - **Average UL throughput (Mbps):** This KPI measures the average rate at which data is transferred from the UE to LTE AP, within a selected reporting interval.

- **DL traffic volume (GBytes):** This KPI measures the total amount of data transferred from LTE AP to the UE
- **UL traffic volume (GBytes):** This PKI measures the total amount of data transferred from the UE to LTE AP.
- **GPS statistics:**
 - **GPS Availability:** This KPI measures the availability GPS measurements only for LTE APs within a venue that are configured to sync up with GPS satellites. The GPS availability is measured in percentage of time within the selected reporting interval.
 - **Phase Locked:** This KPI indicates the average percentage of time LTE APs within a Venue remained in the phase-locked state with timing source. This KPI is measured in percentage of time within the selected reporting interval.
 - **Holdover:** This KPI indicates the average percentage of time LTE APs within a Venue were degraded to holdover phase because of unavailability of a reliable timing information from their timing source. This KPI is measured in percentage of time within the selected reporting interval.
 - **Frequency Phase Recovery:** This KPI indicates the average percentage of time all GPS capable LTE APs within a Venue were in frequency recovery phase. This KPI is measured in percentage of time within the selected reporting interval.
- **Stats per LTE AP:** Click the **Stats per LTE AP** to view the KPIs pertaining to each configured LTE AP, in a tabular format. The data is presented per Access Point.

All of the per Venue KPIs are also available for each LTE AP.

Plots

You can plot the relevant LTE KPIs as line graphs.

Follow these steps to display the plot.

1. Form the drop down, select the time period for which you need to generate the plot. The time period can be for the last month, last 7 days, last 24 hours or a custom range.

NOTE

If you select a custom range, specify the start date and end date.

2. Select the venue for which you want to display the plot. You can select All Venues or select the preferred venue from the list.
3. Select the AP for which you want to display the plot. You have the option to select all APs or choose a preferred AP from the drop down.
4. Click the **Manage Report Components** link to select the components which you want to display in the list. The dialog box displays all the available components in the left pane. You can choose to add all of them in the report by moving them to the right page in the dialog box, by clicking the ">>" button. You can also select particular components by selecting them and clicking the ">" button.
5. Click **Apply** to load the graph.

The line graph displays the following components based on your selection in the **Manage Report Components** dialog box.

- The Radio Resource Control (RRC) connection establishment successes number in percentage, along the Y axis, against the date and time range displayed in the X axis.
- The Uplink and downlink traffic volume is displayed in Gigabits along the Y axis, against the date and time range displayed in the X axis.
- Handover attempts, handover success, and rate and success rate is displayed as percentage in the Y axis against date and time in the X axis. Success in plotted in green color and attempt is plotted in orange color.
- Availability fo the Spectrum Allocation Server (SAS) is displayed as percentage along the Y axis against date and time range in the X axis.
- Availability of GPS services is displayed as percentage along the Y axis against date and time range in the X axis.
- The throughput is represented as the average down link throughput (Mbps) and average uplink throughput (Mbps) along the Y axis, against date and time range in the X axis. The number of active UEs plot are available to compare with throughput, on the same plot
- Cell availability is displayed as percentage availability along the Y axis, against date and time range along the X axis.

Viewing Analytics

Available Analytics Reports

- Phase locked is represented as percentage long the Y axis, against date and time range along the X axis.

NOTE

A phase-locked loop (PLL) is in a locked state when the phase error signal produced by the phase detector settles to a constant value.

- The Frequency Synchronization percentage displayed along the Y axis, against the date and time range in X axis.

Choose the **Custom Combination** option to represent any two components listed previously in a single line graph. To select the components, select the respective check box and click **Save**. Click **Export to file** and choose to export the **Custom combination** graph as a CSV or PDF file.

Available Analytics Reports

Ruckus Cloud offers a number of analytics reports that you can generate to analyze your networks.

Client Traffic

The client traffic analytics report shows the top N wireless clients that have the greatest cumulative unicast traffic volume transmitted to or received from an AP during a specific time interval. The data is represented as a cumulative distribution function (CDF).

When to Generate This Analytics Report

Generate this report if you want to:

- Track high-volume users, identify their subscriptions and potentially target for throttling or band steering
- Discover natural “break points” in usage patterns. Make consequent future subscription price adjustments or set data caps.

Unique Clients

The unique clients report displays the total number of unique client devices during a specific time interval and the radio to which they are connected.

Use this report to analyze the number of unique client devices using Wi-Fi. It can also be used in conjunction with other reports to determine the average number of devices/subscription.

NOTE

A single wireless device can associate to the network during different time intervals and thus have multiple sessions. The device’s MAC address is used to bind these multiple sessions together.

By applying a variety of filters, the chart(s) can display more specific information. For more details on the filtering options, refer to [Viewing and Filtering Wi-Fi Analytics Data](#) on page 174.

Number of Sessions

The number of sessions report displays sessions per radio over time, authorized versus unauthorized clients, and session distribution per radio (2.4 GHz versus 5 GHz).

Use this report to analyze the number of devices on the network at any given time. It can be applied to network dimensioning, looking at possible revenue (for example, advertising), and so on.

When using this report, note that:

- A user may have multiple devices on the network, for example, an iPhone and iPad. In this case, the number of sessions would be reported as 2 (devices), not 1 (user).
- A user may have one device on the network at two different times (e.g., from 1:03pm to 1:08pm and 2:25pm to 2:45pm). In this case, the number of sessions would be reported as 2 (sessions), not 1 (user).

By applying a variety of filters, the charts can display the information for a specific period of time, by venue, by AP, by network type, and by radio settings. For more details on the filtering options, refer to [Viewing and Filtering Wi-Fi Analytics Data](#) on page 174.

Session Inventory

The session inventory report displays as a table that provides a session log for a set of wireless devices during a given time interval.

Use this report to analyze usage statistics using SP defined method; method takes CSV file as input.

By applying a variety of filters, the charts can display the information for a specific period of time, by venue, by AP, by network type, and by radio settings. For more details on the filtering options, refer to [Viewing and Filtering Wi-Fi Analytics Data](#) on page 174. You can also filter the session inventory table using the search box and searching for clients by MAC address.

Apply filters as required and click the **Export button** available on top right corner of the page to export the session inventory data from the tenant portal into a CSV file.

For instance, select the report date range as **Custom Range** and then pick the report start date and report end date. Select a Venue for which you wish to run the report and then click the **Export** button. The report for the selected date range, for the selected Venue is downloaded as a CSV file. In the report, you will find that the first row displays the date range, and the second row mentions the Venue which you selected.

NOTE

In the above instance, as you did not apply filter for APs, Networks and WiFi Radios, the report is generated for all configured APS, Networks and WiFi radios.

When interpreting this report, note that:

- Each row in the table contains the MAC address of the wireless devices, device type, OS type, authentication time, association time, session end time, downstream / upstream bytes transferred and serving AP.
- Wireless devices are selected based on being joined to a particular controller, AP, AP group, SSID or radio.

Session Duration

The session duration report is a cumulative distribution function (CDF) of the wireless devices' session durations that exceed a user-specified duration, which occurred during a given time interval. The session duration length is defined by the user.

Use this report to analyze how long users are on the network. Service delivery can then be optimized accordingly.

By applying a variety of filters, the charts can display the information for a specific period of time, by venue, by AP, by network type, and by radio settings. For more details on the filtering options, refer to [Viewing and Filtering Wi-Fi Analytics Data](#) on page 174.

Viewing Analytics

Viewing and Filtering Wi-Fi Analytics Data

AP Traffic

This report provides the cumulative volume of unicast traffic transmitted to or received from wireless clients associated with any network on a managed AP for a specific time interval.

The reported traffic is actually traffic density (traffic/time); the value of the traffic reported is scaled to the time dimension on the x-axis of the graph (for example, traffic/15-min, traffic/hour, traffic/day). The graph displays three types of AP traffic:

- AP to user traffic
- User to AP traffic
- Client traffic

Data used to create the report includes STA session statistics from all VAPs configured on a [physical] AP and includes both 2.4- and 5-GHz radios (if present) on an AP. Data on the following traffic types is also included:

- IP datagrams carrying client traffic
- Non IP, layer-3 packets
- Network-layer management traffic a STA needs to access network resources
- Data link layer traffic above the 802.11 MAC

By applying a variety of filters, the charts can display the information for a specific period of time, by venue, by AP, by network type, and by radio settings. For more details on the filtering options, refer to [Viewing and Filtering Wi-Fi Analytics Data](#) on page 174.

When to Generate This Report

Generate this report if you want to:

- Learn how busy the AP is with traffic to/from users (includes unicast/multicast packets)
- Learn how much traffic is uploaded versus downloaded
- Find network locations which are the busy areas
- View the relative proportion of total traffic (user + management) to management traffic.

Viewing and Filtering Wi-Fi Analytics Data

Analytics data in Ruckus Cloud can help you gain an insight into the status of your Wi-Fi networks, APs, and wireless clients.

Follow these steps to view and filter data in Ruckus Cloud.

1. On the menu, click **Analytics**.

The **Analytics** page appears with four categories:

- Clients
- Sessions
- Access Points
- Applications

2. On the **Analytics** menu, click the report that you want to view in any category.
To filter the data displayed, various filters are available at the top of the screen.

NOTE

Not all filter options are displayed for each data chart. The Data Summary and the next five options appear on most of the report screens. After selecting one or more filter options, click **Apply** to refresh the data charts.

3. Under the filter options, the Data Summary: appears with a date range and other information applicable to each report. Click the clock icon to select a different time period. Check other options as applicable.

After making your selection, the data charts refresh.

4. To filter the data for a time period other than the default 24 hours, click the down arrow in the **Last 24 Hours** option.

Select one of the following:

- **Last 24 Hours**—This is the default choice.
- **Last 7 Days**—Data for the last week is displayed.
- **Last Month**—Data for the last month is displayed.
- **Custom Range**—Use the calendar icon to select your custom time period.

After you select a time period, select other options or click **Apply** to refresh the data charts.

5. To filter the data by Venue click the down arrow in the **All Venues** option.

Select one of the following:

- **All Venues**—This is the default choice.
- **<Venue-name>**—Click the venue name to display data for the specific venue.

After you select a venue option, select other options or click **Apply** to refresh the data charts.

6. To filter the data by Access Point (AP) click the down arrow in the **All APs** option.

Select one of the following:

- **All APs**—This is the default choice.
- **<AP-name>**—Click the AP name to display data for the specific AP.

After you select an AP option, select other options or click **Apply** to refresh the data charts.

7. To filter the data by network click the down arrow in the **All Networks** option.

Select one of the following:

- **All Networks**—This is the default choice.
- **<Network-name>**—Click the network name to display data for the specific network.

After you select a network option, select other options or click **Apply** to refresh the data charts.

8. To filter the data by radio bandwidth click the down arrow in the **All Radios** option.

Select one of the following:

- **All Radios**—This is the default choice.
- **2.4Ghz**—Data for the 2.4Ghz radio bandwidth is displayed.
- **5 Ghz**—Data for the 5Ghz radio bandwidth is displayed.

After you select a radio option, select other options or click **Apply** to refresh the data charts.

Viewing Analytics

Viewing and Filtering Wi-Fi Analytics Data

9. To filter the data by the Top N% click the down arrow in the **Top 10%** option.

Select one of the following:

- **Top 10%**—This is the default choice.
- **Top N%**—Various % options appear from 1 through 5, 10 through 100. Depending on your selection, data can be displayed for the top N percent.

After you select a top N percentage option, select other options or click **Apply** to refresh the data charts.

10. To filter the data and group the data by a specific time period, click the down arrow in the **Per 1 Hour** option.

Select one of the following:

- **Per 1 Minute**—Data is grouped by minute.
- **Per 15 Minutes**—Data is grouped by 15-minute intervals.
- **Per 30 Minutes**—Data is grouped by 30-minute intervals.
- **Per 1 Hour**—This is the default choice. Data is grouped by 1-hour intervals.
- **Per 1 Day**—Data is grouped by day.

After you select a group time period, select other options or click **Apply** to refresh the data charts.

11. To filter the data by the most AP reboots, click the down arrow in the **Top 10 APs** option.

Select one of the following:

- **Top 5 APs**—Data is displayed for the top 5 APs by number of reboots.
- **Top 10 APs**—This is the default choice. Data is displayed for the top 10 APs by number of reboots.
- **Top 15 APs**—Data is displayed for the top 15 APs by number of reboots.

After you select a Top N APs option, select other options or click **Apply** to refresh the data charts.

Performing Administrative Tasks

- Performing Administrative Tasks..... 177
- Viewing Your Account Details..... 177
- Viewing Administrators..... 178
- Configuring Notification Settings..... 181
- Using the Support Options on the Web Interface..... 183
- Viewing Your License Information..... 183
- Adding a SAS Account..... 184
- Editing a SAS Account..... 186
- Viewing Your SAS Account..... 188
- Deleting a SAS Account..... 189
- Enabling or Disabling Access Restriction 191
- Sending Feedback..... 191
- Reporting an Issue..... 192

Performing Administrative Tasks

Use the **Administration** menu to manage user accounts, administrators, system notifications, and your Ruckus LTE AP Management Service license. If you need technical support from Ruckus, you can also use the **Administration** menu to grant temporary administrator-level access to your account to the Ruckus Support team.

Viewing Your Account Details

Your RUCKUS Cloud account information includes your organization's name, address, and phone number.

Follow these steps to view your account details.

1. On the Dashboard, click **Administration**.

The **Administration** page appears and displays the following tabs:

- **Account Details**
- **Administrators**
- **Notifications**
- **Support**
- **License**
- **Cloud Version**

2. Click the **Account Details** tab to review your account information. The **Account Details** tab displays the following information:
 - **Organization:** Name of the organization that you represent.
 - **Address:** Street address of your organization.
 - **City:** City in which your organization is located.
 - **State/Province:** State or province in which your organization is located.
 - **ZIP:** ZIP or postal code of your organization's location.
 - **Country:** Country where your organization is located.

NOTE

To update your name and email address, edit your profile on the RUCKUS Support website.

When you enable MFA, RUCKUS Cloud asks for a verification code via your chosen security method (Email, SMS or authentication app). By default, MFA is disabled. The Prime-Admin controls the MFA feature and applies to all admin accounts. When the MFA is enabled all users of the account are required to set and use MFA. Managing the personal authentication settings is done via the **User Profile** menu.

To enable MFA, follow these steps.

3. Toggle the **Multi-Factor Authentication (MFA)** switch to **ON**.
4. Click **Enable MFA** when the **Enable Multi-Factor Authentication** dialog box appears.

RUCKUS Cloud generate recovery codes for that can be used as a backup method to access the account if the admins have trouble receiving the security code. Make sure that you copy the codes and store them in a safely.

Viewing Administrators

Your Ruckus Cloud account supports multiple administrators to allow you to delegate management tasks to other people.

Follow these steps to view a list of administrators who have management access to your Ruckus Cloud account.

1. On the **Dashboard**, click **Administration**.
2. On the **Administration** page, click the **Administrators** tab.

The page refreshes, and the **Administrators** screen appears. The Local Administrators list displays the following information for each administrator:

 - Email address
 - Name
 - Role
3. (Optional) Select an administrator and click **Edit** to modify the role. Click **Delete** to remove the administrator.
4. If Ruckus partners have management access to your account, a second list of 3rd Party administrators displays.

The following information displays for each administrator:

- Name
 - Status
 - Action
5. (Optional) Click **Revoke access** to revoke the 3rd-party administrator access.

You have completed viewing a list of existing administrators. To add another administrator, see the [Adding an Administrator](#) on page 179.

Understanding Administrator Roles

An administrator role defines the types of tasks that an administrator can perform to manage venues, APs, networks, guest users, and authentication services, to monitor wireless clients and events, and to view analytics reports.

The following table describes the administrator roles that Ruckus Cloud supports.

NOTE

You can assign the same administrator roles to multiple users.

TABLE 16 User Roles in Ruckus Cloud

Administrator Role	Description
Prime Admin	The highest-level administrator role in Ruckus Cloud. This role allows administrators to perform <i>all</i> configuration, monitoring, and administration tasks in your Ruckus Cloud account.
Administrator	This role allows administrators to fully control tenant accounts and to manage delegated tenants, if permitted by the Prime Admin.
Guest Manager	This role allows administrators to manage guest user accounts. The tasks that administrators assigned the guest manager role can perform include: <ul style="list-style-type: none"> • Adding a new guest user • Managing existing guest users, including disabling or deleting guest users and generating a new guest password • Viewing guest user information
Read Only	This role allows administrators to view venues, APs, networks, guest accounts, events, and reports. However, an administrator that is assigned this role cannot perform any configuration tasks, including creating or editing venues, APs, networks, and guest accounts.

If a third-party administrator (an authorized Ruckus partner, also known as a value-added reseller or VAR) is assigned as a prime administrator, additional VAR administrators automatically get read-only access to the VAR portal. Any further permissions must be explicitly granted by the prime administrator.

Adding an Administrator

If you want to delegate the management of APs in your venues to another person, you can create an administrator account for that person.

NOTE

Trial accounts are limited to one administrator account. If you have a trial account with a TEMP license, you will be unable to create an additional administrator account.

Complete the following steps to add an administrator in your Ruckus Cloud account.

1. From the navigation pane, click **Administration**.
2. On the **Administration** page, click the **Administrators** tab.
3. Click **Add Administrator** in the upper-right corner of the Local Administrators list.
The **Add New Administrator** page is displayed.
4. Add the email of the person that you want to add as an administrator.
 - If the person that you want to add as an administrator has an existing Ruckus Support account, click **Add a registered user**, and then select the registered user that you want to add as an administrator.
 - If the person that you want to add as an administrator does not have an existing Ruckus Wireless Support account, click **Invite new user**, and then type the person's email address. Ruckus Cloud will set up an account and send an email request to the email address supplied for the administrator.

Performing Administrative Tasks

Viewing Administrators

5. In the **Role** list, select the role that you want to assign to this user.

Available administrator roles include:

- Prime Admin
- Administrator
- Guest Manager
- Read Only

For more information about the roles, refer to [Understanding Administrator Roles](#) on page 179.

6. Finish adding or inviting the administrator.
 - If you clicked **Add a registered user** in Step 4, click **Add Administrator**.
 - If you clicked **Invite new user** in Step 4, click **Send invitation**.

The page refreshes, and then the **Administrators** tab lists the new administrator that you added or invited, along with the existing accounts. If you do not see the new administrator, click **Refresh**.

If you invited a new user to be an administrator, Ruckus Wireless will send an email message with the subject *Ruckus Wireless Support Account Invitation* to this user. Ask the user to check his or her email inbox (and junk mail) and to click the link to complete the registration process.

Editing or Deleting an Administrator

You can change the role of a local administrator that you created or delete the administrator from your Ruckus Cloud account.

Complete the following steps to edit or delete an administrator. To complete these actions, you must have prime administrator permissions.

1. From the navigation pane, click **Administration**.
2. Click the **Administrators** tab.
3. Locate the local administrator that you want to edit or delete.
4. Click the pencil (Edit) icon that is in the same row as the administrator account that you want to edit or delete.

The **Edit Administrator** page appears.

5. To change the role assigned to the administrator, select a new administrator role from the **Role** list. To delete the administrator, click **DELETE ADMINISTRATOR**, and then click **Delete Administrator** to confirm.
6. Click **OK**.

Inviting a Ruckus Partner to Manage Your Account

You can choose an authorized Ruckus partner also known as a value-added reseller (VAR) to manage your Ruckus LTE AP Management account.

You require the email address of the authorized Ruckus Partner administrator to send an invitation from the Ruckus LTE AP Management web interface. For assistance, contact Ruckus Support.

Follow these steps to invite a third-party administrator to manage your Ruckus LTE AP Management account.

1. On the Dashboard, click **Administration**.

The **Administration** page appears.
2. Click the **Administrators** tab.

The **Administrators** page appears and displays a list of local administrators and 3rd Party administrators (Ruckus Partners).
3. Scroll down to the **3rd Party Administrators** section, and then click **Invite 3rd Party Administration**.

The **Invite 3rd Party Administration** dialog box appears.

4. In the **Invite an administrator** dialog box, enter the email address of the Ruckus partner.
5. Click **OK**.

The AP Management sends an invitation to the email address. The LTE AP Management verifies its support account database for the email address that you entered.

- If a Ruckus partner is mapped to the email address that you entered, an invitation is sent to the partner. If the Ruckus partner accepts your invitation, the partner is granted administrative access to your account, and you are notified about it. If the Ruckus partner does not have a Ruckus LTE AP Management account, a Prime Admin account is created using the email address that you entered.
- If a Ruckus partner is not registered using the email address that you entered, an error message is displayed: `No 3rd party administration found with the specified email address. Try using different email address.`

You have completed inviting a 3rd party administrator to manage your Ruckus LTE AP Management account.

Configuring Notification Settings

To ensure that you and other administrators in your organization stay updated on what is going on in your network (including issues that need immediate attention), configure the notification settings on Ruckus Cloud.

Ruckus Cloud supports two types of notification methods:

- **Email:** Send system notifications to multiple email address. Refer to [Adding an Email Address for System Notifications](#) on page 181.
- **SMS:** Send text or short message service (SMS) messages to multiple mobile numbers. Refer to [Adding an SMS Address](#) on page 182.

Notification are sent for three main issues:

- **AP disconnection (Alarm issued)**—After a period of 15 minutes has elapsed since an Access Point (AP) is disconnected from Ruckus Cloud, a notification is sent to the administrator. The information in the notification includes the time the AP was disconnected, the venue, the AP name, MAC address and serial number.
- **AP reconnection (Alarm cleared)**—After the AP is reconnected to Ruckus Cloud, a notification is sent to the administrator. The information in the notification includes the time the AP was disconnected, the venue, the AP name, MAC address and serial number.
- **License expiration**—Notifications are sent when a license is about to expire starting from 30 days prior to expiration, and on a weekly basis until expiration. After a Ruckus Cloud subscription expires, any affected APs are disconnected from Ruckus Cloud and a notification is sent with a reminder to renew the subscriptions. The information in the notification includes AP name, model, venue, serial number, MAC address, Internal IP address and tags. While these APs are removed from Ruckus Cloud management, they are still operational.

Adding an Email Address for System Notifications

The RUCKUS LTE AP Management sends notifications for system-related events to the email addresses configured in the system.

Follow these steps to add an email address to which to send system notifications.

1. On the menu, click **Administration**.
2. In the **Notifications** tab, click **Add Email Address**.
The **Add New Email Address** dialog box appears.
3. In the **Add New Email Address** dialog box, enter the email address that you want to add.

4. Click **Add**.

The message `Creating email notification` appears. After the AP Management successfully adds the email address, the **Notifications** tab refreshes and then email address you added appears in the **Email** section. By default, the notifications options is enabled.

You have completed adding an email address to which the AP Management will send system notifications.

Editing, or Deleting an Email Address for System Notifications

The RUCKUS LTE AP Management sends notifications for system-related events to the email addresses configured in the system.

Follow these steps to add an email address to which to send system notifications.

1. On the menu, click **Administration**.
2. In the **Notifications** tab, click the pencil icon in the **Add Email Address** section.
The **Edit Email Address** dialog box appears.
3. In the **Email Address** field, enter the new email address.
4. Click **Save**.
5. (Optional) After Step 2, click **Delete Address** to delete the email address.

You have completed editing an email address to which the AP Management will send system notifications.

Adding an SMS Address

Ruckus Cloud can send system notifications via SMS to multiple mobile numbers.

Complete the following steps to add a mobile number to which to send SMS notifications.

1. From the navigation pane, click **Administration**.
2. Click the **Notifications** tab.
3. In the **SMS** section, click **Add Mobile Number**.
The **Add New Mobile Number** screen appears.
4. In **Mobile Number**, type the mobile number to which you want to send SMS notifications. The mobile number must follow the format: + (country code) - (area code) - (mobile number) For example, you can type +1-408-888-888.
5. Click **Add**.

The message `Creating SMS notification` appears. After Ruckus Cloud adds the mobile number successfully, the **Notifications** tab refreshes, and the mobile number you have added appears under the **SMS** section.

Editing or Deleting a Mobile Number

Complete the following steps to edit a mobile number to which to send notifications vis SMS.

1. From the navigation pane, click **Administration**.
2. Click the **Notifications** tab.
3. In the **Mobile Number** section, click the pencil icon to edit the mobile number.
The **Edit Mobile Number** dialog box appears.
4. In the **Mobile Number** field, enter the mobile number to which you want to send SMS notifications.

5. Click **Save**.

After RUCKUS Cloud adds the mobile number successfully, the **Notifications** tab refreshes, and the mobile number you have added appears under the **SMS** section.

6. (Optional) After Step 3, click **Delete Number** to delete the mobile number.

Using the Support Options on the Web Interface

The Support tab on the web interface helps you recover an AP when it loses connection with Ruckus LTE AP Management Service, and also allows Ruckus Support to access your account for troubleshooting, when required.

Recovery Network Passphrase

If an AP loses its connection to the AP Management Service, you cannot manage it from the AP Management Service web interface.

To regain access to the AP, you must connect the SSID of the network, which is named "Recover.Me". You must also enter a 16-digit passphrase to connect to the recovery network.

To view the current recovery network passphrase, click the eye icon. The passphrase appears in plain text.

To change the recovery network passphrase, click **Change**. When the **Change Recovery Network Passphrase** page appears, enter a new 16-digit passphrase, and then click **Save**.

Allow Access to Ruckus Support

If you request assistance from the Ruckus Support Team, you may be asked to enable the **Allow Access to Ruckus Support** feature to grant Ruckus Support temporary administrator-level access to your account. The temporary access is automatically revoked after seven days.

To allow Ruckus Support temporary access to your account, toggle the switch to the **ON** position.



CAUTION

You must enable the **Allow Access to Ruckus Support** feature only when requested by Ruckus Support.

Viewing Your License Information

Your Ruckus LTE AP Management license information shows the type of license that you have purchased, the number of APs that your account can support, and additional details about your license subscriptions.

Follow these steps to view your license information.

NOTE

The temporary (TEMP) licenses are valid only for 60 days; there is no grace period. If new licenses are not obtained, expiration of TEMP license will result in deletion of APs

1. On the Dashboard, click **Administration**.

The **Administration** page appears.

2. Click the **License** tab to review your licenses.

The **License** window displays.

- If any of your licenses are about to expire, or have expired, a banner displays at the top of the screen.
- The paid licenses have a 60-day grace period. An alarm is raised thirty days prior to the subscription expiration, and the administrator receives an email notification on a weekly basis until the date of the expiration. The text in the license expiration banner changes depending on the status of the license, the number of days before it expires, or the numbers of days left in the grace period.
- After the grace period expires, you cannot manage the APs using AP Management. A notification is sent with details of the expired APs to allow you to identify and renew the licenses of the impacted APs. After the expiry of a thirty-day grace period, the APs are removed from your Ruckus LTE AP Management account.
- TEMP licenses are valid only for 60 days; there is no grace period.
- The progress bars show the percentage of the APs deployed in both text and a graphic format, for the Wi-Fi and LTE network. The fraction at the end of the progress bar indicates the number of current APs deployed/the maximum number of APs that you can deploy. For example, if you see 12/20, this indicates that you have deployed 12 APs and the maximum number of APs you can deploy is 20.
- The **Total usage** information is displayed next to the progress bars and displays the total usage summery value.

Under the **License Subscriptions** header the following fields are displayed.

- **License for:** Indicates the maximum number of APs allowed for your license subscription.
- **Type :** Type of AP Management license that your organization purchased. License type includes Wi-Fi Basic, LTE trial, and LTE basic.
- **Activated On:** Indicates the date and time when your organization activated the license subscription.
- **Expires on:** Indicates the date and time when your license subscription expires.
- **Time left:** Indicates the length of time, in days, left before your license subscription expires.
- **Act Now:** If the license has expired, the **Act Now** link appears at the end of the row. Click **Act Now** to view the instructions on how to re-activate a license. You can contact the reseller, go to the license management website, or contact the Ruckus support team.

You can have multiple license subscriptions.

You have completed viewing your license information.

Adding a SAS Account

Review the SAS configuration in your Ruckus LTE AP Management account and update it or create a new SAS account.

To add a SAS account, follow these steps.

NOTE

Any addition, deletion, or modification to the SAS account results in service disruption.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, click the **SAS Accounts** tab.

3. Click **Add SAS Account** on the top-right corner of the page.

The **Add SAS Account** dialog box appears.

FIGURE 36 Adding a SAS Account

Add SAS Account

* SAS Account Name: Custom

* Provider: Federated Wireless

* URL: https://developer-sc-02.federatedwireless.com

* Version: v1.2

* CBSD User ID: Ruckus_IDC

* Registration Mode: Using STA

Set as default SAS account

* Required field Cancel Save

4. Choose a service provider from the **Operator** list.

Currently, the following options are available:

- Custom
- CommScope
- Google
- Federated

The selected service provider appears in the **Operator** field. The **URL** and **Version** fields get automatically populated. For a custom service provider, you must manually enter the URL and its version in the respective fields.

5. Enter a valid CBSD ID to create a tenant account with the service provider in the **CBSD User ID** field.

A CBSD user ID is provided by the SAS vendor and is unique per tenant account.

6. In the **Registration Mode** field, you can choose **Using STA** or the **Single-Step Registration**.

NOTE

CPI information is mandatory if STA is not available.

Performing Administrative Tasks

Editing a SAS Account

7. Check the **Set as default SAS account** check box to add this account as the default SAS account.
8. Click **Save**.

A progress bar appears displaying **Updating SAS Account**.

NOTE

Saving changes will revoke CPI certification from all certified APs and require recertification.

You have completed adding a SAS account.

For a list of **Events** pertaining to a SAS account of a tenant, refer to [Event List](#) on page 160.

Editing a SAS Account

Review the SAS configuration in your Ruckus LTE AP Management account and update it or create a new SAS account.

To edit a SAS account, follow these steps.

NOTE

Any addition, deletion, or modification to the SAS account results in service disruption and any changes will revoke CPI Certification from all certified APs. You must certify all APs again.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, click the **SAS Accounts** tab.

3. Click **Edit** on the top-right corner of the page.
The **Edit SAS Account** dialog box appears.

FIGURE 37 Edit SAS Account

Edit SAS Account ⓘ ✕

* SAS Account Name:

* Provider:

* URL:

* Version: ⓘ

* CBSD User ID:

* Registration Mode: ⓘ

Set as default SAS account ⓘ

* Required field Cancel Save

4. Choose a service provider from the **Operator** list.
 - CommScope
 - Google
 - Federated
 - Custom

The selected service provider appears in the **Operator** field. The **URL** and **Version** fields get automatically populated. For a custom service provider, you must manually enter the URL and its version in the respective fields.

5. Enter the URL or update an existing URL of the service provider in the **URL** field.
6. Enter the version or update the existing version of the service provider in the **Version** field.
The version number must be in this format: v.[version number], for example, **v1.2**
7. Enter a valid CBSID ID to create a tenant account with the service provider in the **CBSD User ID** field.
A CBSID user ID is provided by the SAS vendor and is unique per tenant account.
8. In the **Registration Mode** field, you can choose **Using STA** or the **Single-Step Registration**.

NOTE

CPI information is mandatory if STA is not available.

9. Check the **Set as default SAS account** check box to add this account as the default SAS account.

Performing Administrative Tasks

Viewing Your SAS Account

10. Click **Save**.

A warning message appears stating: Saving changes will revoke CPI Certification from all certified APs. All APs will need to be recertified again..

You have completed editing a SAS account.

For a list of **Events** pertaining to a SAS account of a tenant, refer to [Event List](#) on page 160.

Viewing Your SAS Account

The **SAS Account** tab displays details about your SAS account.

- **Provider:** The service provider for your SAS account (for example, **Custom**).
- **URL:** The URL to access the service provider's services.

NOTE

When the SAS URL is updated by the provider, a notification appears on the **SAS Accounts** page. In addition, an alarm is also triggered when the SAS URL is updated by the provider.

Click **Apply Update** to apply the changes to the affected SAS account.

- **Version:** The current version.
- **CBSD User ID:** The user ID for a tenant account with the SAS provider.
- **STA Available:** Special Temporary Authority

FIGURE 38 Viewing SAS Accounts

SAS Account Name	Provider	URL	Version	CBSD Use...	Registratio...	Venues	Default SAS Account ?		
1	Custom	https://www.ww...	v234	98798	Using STA	0	Set As Default		
1 a	CommScope	https://developer-...	v1.2	111111	Using STA	0	Set As Default		
1b	Federated ...	https://developer-...	v1.2	67g6ut77u	Using STA	0	Set As Default		
adil@#\$\$%^&*()*(&^%...	CommScope	https://prod.sasc...	v1.2	adi98kkkjh...	Single Step	4			
FW_adi	Federated ...	https://developer-...	v1.2	e54tvert5g...	Using STA	0	Set As Default		
ssa one	Google	https://test.sas.go...	v1.2	546468	Using STA	0	Set As Default		

The SAS Accounts page displays the following columns.

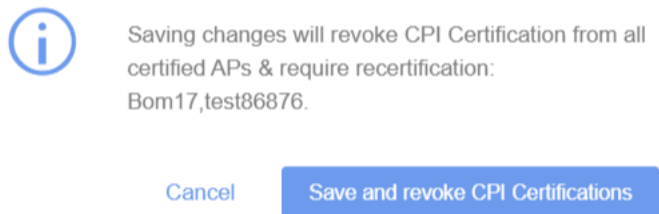
- **SAS Account Name:** Name of the SAS account.

- **Provider:** Name of the SAS account provider.
- **URL:** URL of the SAS account provider.
- **Version:** Version number.
- **CBSD User ID:** CBSD user ID for the SAS account.
- **Registration Mode:** Registration mode selected for the SAS account
- **Venues:** Venues where the SAS account is used.
- **Default SAS Account :** Option to select the SAS account as the default SAS account.

NOTE

When you modify the default SAS account, it will revoke CPI Certification from all certified APs and require recertification.

FIGURE 39 Save and Revoke CPI Certification



To update existing SAS account, click the pencil icon.

For more information, refer to [Adding a SAS Account](#) on page 184.

To delete the existing SAS account, click the delete icon . Deleting the SAS account deactivates the LTE service in all RSCs.

Deleting a SAS Account

To delete a SAS account, follow these steps.

NOTE

Any addition, deletion, or modification to the SAS account results in service disruption.

1. On the Dashboard, click **Administration**.

Performing Administrative Tasks

Deleting a SAS Account

2. On the **Administration** page, click the **SAS Accounts** tab.

The list of existing SAS accounts are displayed.

FIGURE 40 Deleting a SAS Account

Administration

Account Details Administrators Notifications Support License **SAS Accounts** ECGI Records CPI Details

SAS Accounts [Add SAS Account](#)

SAS Account Name	Provider	URL	Version	CBSD Use...	Registratio...	Venues	Default SAS Account
1	Custom	https://www.ww...	v234	98798	Using STA	0	Set As Default
1 a	CommScope	https://developer-...	v1.2	111111	Using STA	0	Set As Default
1b	Federated ...	https://developer-...	v1.2	67g6ut77u	Using STA	0	Set As Default
adi1@#\$%^&*()*&^%...	CommScope	https://prod.sasc...	v1.2	adi98kkkjh...	Single Step	4	✓
FW_adi	Federated ...	https://developer-...	v1.2	e54tvert5g...	Using STA	0	Set As Default
ssa one	Google	https://test.sas.go...	v1.2	546468	Using STA	0	Set As Default

3. Click the delete icon against the SAS account that you want to delete.

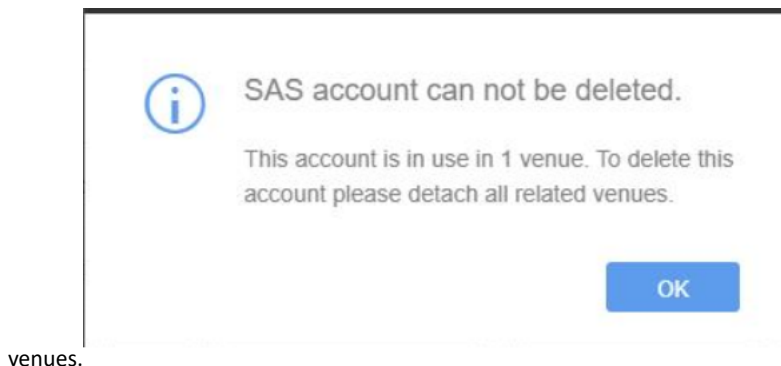
A progress bar is displayed

Deleting SAS Account

after clicking on **Delete SAS Account** button in confirmation pop up message.

NOTE

You cannot delete a SAS account that is associated with a venue. Before deleting a SAS account, you must detach it from the



venues.

You have completed deleting a SAS account.

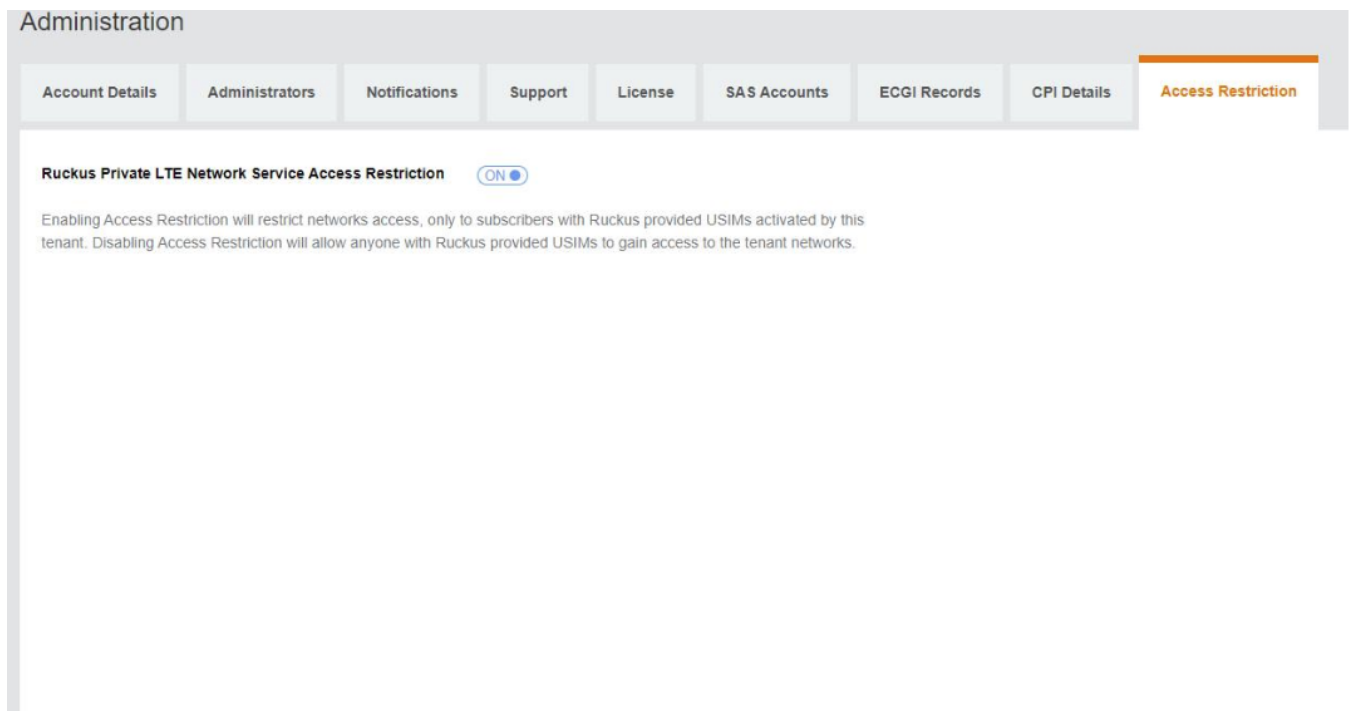
Enabling or Disabling Access Restriction

Enabling Access Restriction will restrict networks access, only to subscribers with Ruckus provided USIMs activated by you. Disabling Access Restriction will allow anyone with Ruckus provided USIMs to gain access to your networks.

To enable, access restriction, follow these steps.

1. On the Dashboard, click **Administration**.
2. On the **Administration** page, select the **Access Restriction** tab.

FIGURE 41 Access Restriction



3. Toggle the **Ruckus Private LTE Network Service Access Restriction** button to **ON** to enable access restriction or **OFF** to disable access restriction.

By default, the **Access Restriction** feature is **OFF**. If the **Access Restriction** is disabled at the tenant level, access restriction will be disabled for all related venues, and it will not be possible to change the **Access Restriction** setting at the a venue level.

Sending Feedback

You can send your feedback to the Ruckus LTE AP Management Service team from the web interface.

Follow these steps to send feedback to Ruckus.

1. Log in to the web interface.
2. Click the **Send Feedback** button in the lower-left corner of the page.

The **Send Feedback** window appears.

Performing Administrative Tasks

Reporting an Issue

3. Type your message in the text box.
4. Click **Send**.

A message appears stating: Thank you for sending us your feedback.

You have completed sending feedback to Ruckus.

Reporting an Issue

If you have a valid support contract, you can submit a support ticket request to Technical Support through the Ruckus Support portal at:

<https://support.ruckuswireless.com/contact-us>

The following section provides information on how to open a how to open cases for Ruckus LTE (CBRS).

1. Using your Ruckus Wireless Support credentials, log in to: <https://support.ruckuswireless.com>.
2. Click **Submit A Case**.
3. Check the type of case in the **Case Type** check box.
4. Check the the priority of the case in the **Priority** check box.
5. Select **LTE** as the **Product Name** box.

Step 1 - Case Type

Case Type ⓘ

- Administration
- Ruckus Cloud
- Software
- Hardware
- vSCG/vSPOT

Priority ⓘ

- P1 - Critical. Please [contact us](#) by phone or chat. P1 cases cannot be submitted through the web form.
- P2 - High
- P3 - Medium
- P4 - Low

Step 2 - Case Description

Product Name ⓘ

Select an Option

lte

Cloud Services

LTE

Software Version ⓘ

Description - Please provide as much detail as possible ⓘ

6. Enter the Ruckus LTE Management software verison in the **Software Version** box.
7. Provide details of the issue in the description box.
8. Check **Email** or **Phone** in the **Best way to contact me** section.
9. Click Submit to open a new case.

A new screen appears displaying the case cumber which will be used as the reference for all communications regarding the reported issue. Also, an email is sent to the originator of the case.

When reporting an issue, provide the following information:

- The AP model

- Description of the client device that has issues connecting or accessing the AP model
- Specific steps that led to the situation

In the majority of cases, the Master AP's Debug information (saved from **Administer > Diagnostics**) is helpful for the analysis of a problem.

Troubleshooting Basic Issues

- Login Issues..... 195
- AP Is Unable to Connect to Ruckus LTE AP Management.....195
- Firewall Ports to Open for Ruckus LTE AP Management..... 195
- Troubleshooting LTE Issues..... 196

Login Issues

If you are unable to log in to the Ruckus LTE AP Management Service portal, review the following.

- If you already have a Ruckus LTE AP Management Service account but forgot password, reset your account password.
- If an error occurs (or nothing happens) when you attempt to log in to the AP Management Service portal, make sure that you have a valid Ruckus LTE AP Management Service account. A Ruckus LTE AP Management Service account is different from a Ruckus Support account. To request for a Ruckus LTE AP Management Service trial account, contact your local Ruckus sales representative.

AP Is Unable to Connect to Ruckus LTE AP Management

If an AP is unable to connect to the Management platform, check the following

- Power source (802.3AT/ PoE+)
- DHCP IP allocation
- Internet connectivity for the network deployed. For other helpful tips, refer to the following sections in this chapter.

Firewall Ports to Open for Ruckus LTE AP Management

The following table lists the ports that must be opened in the network firewall to ensure that managed APs, guest users, DNS servers that can communicate successfully with Ruckus LTE AP Management.

TABLE 17 Ports Required for Ruckus LTE AP Management Communication

From (Sender)	To (Listener)	Port	Purpose	Symptoms When Blocked
Admin	Any	TCP:443	Login and access tenant account for managing tenant APs	The AP Management portal is inaccessible.
AP	LTE AP Management	UDP:4500	Used for NAT traversal	Connection to the management fails.
AP	LTE AP Management	UDP:500	Used for IKE and management	Connection to the management fails.
AP	LTE AP Management	IP: 50	ESP	Connection to the management fails.
AP	LTE AP Management	TCP:22	SSH tunnel between the AP and Ruckus Cloud for management and control traffic	<ul style="list-style-type: none"> • The AP is unable to connect to the AP Management, DIR LED is off. • Tenant account shows that AP is disconnected.
AP	LTE AP Management	TCP:443	Discovery of vSZ	This port is only used when an AP is first added to a tenant account. If this port is blocked, an AP cannot connect to the AP Management after a factory-reset.

TABLE 17 Ports Required for Ruckus LTE AP Management Communication (continued)

From (Sender)	To (Listener)	Port	Purpose	Symptoms When Blocked
AP	Ruckus AP Registrar	TCP:443	Query vSZ associated with registered AP	This port is only used when an AP is first added to a tenant account. If this port is blocked, any factory-reset AP cannot connect to the AP Management after a factory-reset.
AP	Ruckus NTP Server (ntp.ruckuswireless.com)	UDP:123	Synchronization of the AP clock with the NTP server	The LTE AP may not become operational.
AP	DNS server (provided by local DHCP)	TCP/UDP:53	Query to resolve Ruckus AP Registrar's FQDN	This port is only used when an AP is first added to a tenant account. If this port is blocked, an AP cannot connect to the AP Management after a factory-reset.

Troubleshooting LTE Issues

This section provides troubleshooting tips for resolving common issues while working with Ruckus LTE Access Point (AP). All Ruckus LTE AP models have common software modules that can be used interchangeably. The document is valid for all the Ruckus LTE AP models.

After successful setup and commissioning, Ruckus LTE APs are capable of transmitting 20 MHz bandwidth TDD-LTE and providing wireless coverage to relevant LTE devices.

Use this document to debug any setup or performance issues that are encountered during routine operation of the Ruckus LTE AP. Each LTE AP is powered by a managed PoE+ switch or a PoE injector (PoE+ desirable), or DC power adaptor (for Q710 AP) whichever is available.

After booting up, LTE APs send DHCP requests. The LTE APs rely on an external DHCP server to provide each AP, a routable IP address that enables it to route and send connection requests to EMS (Ruckus LTE AP Management Service), Network (EPC), Timing Master, and SAS.

You can configure an LTE AP to complete the following actions:

- Obtain its timing information from the GPS satellites, and assume the role of a Master PTP source for other LTE APs in the network.
- Assume a PTP slave role and obtain its timing information from another AP that is the designated Master (that is reachable by IP address) for that venue.

In the current system implementation, each venue can only have one LTE AP assuming the Timing Master source role. There can be a maximum of up to 32 devices acting as timing slaves per master. In addition, there can be multiple LTE APs with timing source set as GPS satellites and can obtain their timing information directly via GPS satellites (if capable).

For an LTE AP to obtain timing via GPS and/or function as Master timing source, place the AP such that it has direct line-of-sight view with open sky or as close to the outside facing windows or doors.

Initial Setup Issues

Q: I have installed my LTE AP, how do I configure the AP on RUCKUS LTE AP Management environment?

The Management switch powers on the AP via PoE/power adaptor and the AP obtains an IP address from the DHCP server. You must ensure that a DHCP server is configured to provide an IP address to the AP, and is reachable by the AP.

After powering on, Ruckus LTE AP seeks management platform environment connectivity. Ensure that this AP is added to the specific Venue and Network is applied to it on the management platform. For information on how to add an AP to a venue, refer to [Adding an AP](#) on page 53.

By default, LTE AP Management initiates the following actions after an LTE AP connects:

- Checks the LTE AP software build version, and upgrade to most current version.

- Applies basic configuration (venue and network configuration, SAS Provider, and synchronization) to the LTE AP.
- Reports any alarms or events that occurred on the LTE AP.

Q: What is the sequence of AP bootup and various states of LTE AP indicated by LED illumination?

The following is the setup sequence for each AP:

PWR > EMS > SYNC > EPC > LTE

Review the following table to understand the different LTE AP states indicated by LED illumination and its approximate duration in each state along with any recommended corrective actions based on LED patterns observed during the initial AP/venue setup stage.

TABLE 18 LED Labels

LED Label	Time Duration	LED Color/Behavior	Corrective Action
PWR	Until corrective action is executed.	OFF: AP is not powered on.	Check the AP power source.
	Less than 5 minutes.	RED: Boot up in process. The LED remains red if AP does not successfully boot and begin operation.	If longer than 5 minutes, check adequate power is supplied (PoE+/ 802.3at), toggle the power source connection, check cables. If the LED is still RED, contact Ruckus support.
	Until corrective action is executed	AMBER: AP does not have sufficient Power levels	Check adequate power is provided through appropriate PoE cables.
	Few minutes. Until corrective action is executed.	Slow-flashing GREEN: AP does not have a routable IP address (IP address has not been allocated from a DHCP server).	If slow-flashing green is non-stop, check the DHCP settings as the LTE AP is unable to obtain an IP address.
	Perpetual (until default)	SOLID GREEN: AP has booted successfully and obtained a routable IP address.	No action is required.
EMS	Until PWR LED turns Solid Green.	OFF: AP is not being managed by an EMS (Ruckus LTE AP Management).	After PWR LED is in solid green, the EMS LED either starts fast-flashing green autonomously, or solid green immediately. If not, check the reachability of the LTE AP IP to the AP Management.
	Until IP reachability is resolved for LTE AP IP.	Slow-flashing GREEN: AP is unable to communicate with LTE AP Management/ EMS' SecGW.	Check the IP reachability to the Internet and LTE AP Management. Make sure that the AP is accurately created and added to a venue on LTE AP Management.
	Usually less than ~ 10-15 minutes.	Fast-flashing GREEN: AP is being managed by the EMS and is receiving a configuration or a firmware update.	Until the time required to download firmware or configuration. Depends on internet connection speed, do NOT unplug or change anything as this might corrupt the Ruckus Cloud LTE software and needs factory reset.
	Perpetual.	SOLID GREEN: AP is being managed by the EMS. For example, AP successfully connected to AP management.	EMS-AP connection should be always ON.

TABLE 18 LED Labels (continued)

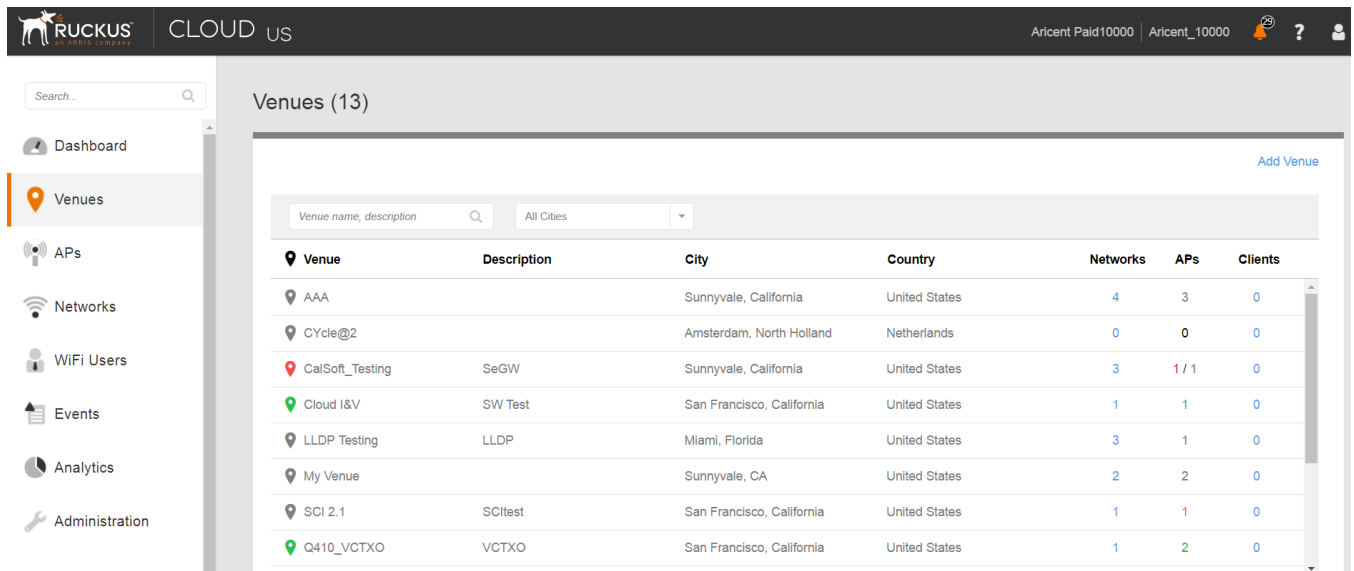
LED Label	Time Duration	LED Color/Behavior	Corrective Action
EPC	May be up to 60 minutes.	OFF: AP is not configured with the Network (EPC) connectivity information.	Make sure that the network configuration is accurate and a Network is turned ON for the AP Venue . Also, check the PTP status under AP Details . If unknown/link lost EPC connection is not attempted, wait until the PTP sync is acquired which takes up to 60 minutes.
	~ few moments after ptp sync obtained AND S1 parameters match else see Corrective Action.	Slow-flashing GREEN: AP is unable to connect to the EPC.	Check if SecGW configuration is accurate (if enabled). Attempting S1 connection to MME but unable connect. Check the reachability or even if reachable, S1 is failing to establish. Check the S1 parameters on network settings. Note that the MME IP, PLMNID, TAC, and Cell ID have to be unique per venue.
	Perpetual	SOLID GREEN: AP is connected to the EPC.	
SYNC	Perpetual	OFF: Timing source is VCTXO/standalone.	Stand-alone mode: Removes Timing dependency for operation. No action needed.
	Until Corrective Action is executed.	Slow-flashing GREEN: Not Timing synced and the AP is not receiving a GPS signal, a macro cell signal (NL) or a PTP signal.	Timing Master: Check the line-of-sight visibility to Timing satellites. Place the AP closer to a window or open sky. Timing Slave: Check the IP reachability between the Timing Slave and the Timing Master.
	May be up to ~ 2 hrs. or more; depends on weather conditions and AP placement.	Fast-flashing GREEN: AP is in the process of acquiring sync, but has not yet acquired sync lock. AP is receiving a GPS signal or a PTP signal.	The sync process is dependent on the GPS signal strength and precision so it takes up to 2 hours. Avoid changing anything during this phase.
	Perpetual until sync is lost.	GREEN: Time synchronization achieved.	If sync synchronization lost, debug the IP connectivity or any other local issues.
LTE	Perpetual or until corrective action is executed.	OFF: LTE transmitter is disabled.	AP service is set to OFF on LTE AP Management or a Grant is not received from SAS to transmit. If the later is true, check the SAS availability, CBSD Registration parameters (SAS URL, CBSD User ID, and so on) under AP Properties > More.
	Perpetual until at least one UE registers with AP.	AMBER: LTE transmission is ON, no UEs are attached.	No UE is registered, check UE settings.
	Perpetual until all UEs de-register from AP.	SOLID GREEN: LTE transmission is ON and one or more UEs are attached to the cell.	—

Venue Status Check using Alarms

Q: How can I check status of a venue using alarms?

- From the Ruckus Cloud LTE dashboard, click **Venues**.
 The **Venue** page appears displaying the list of venues.

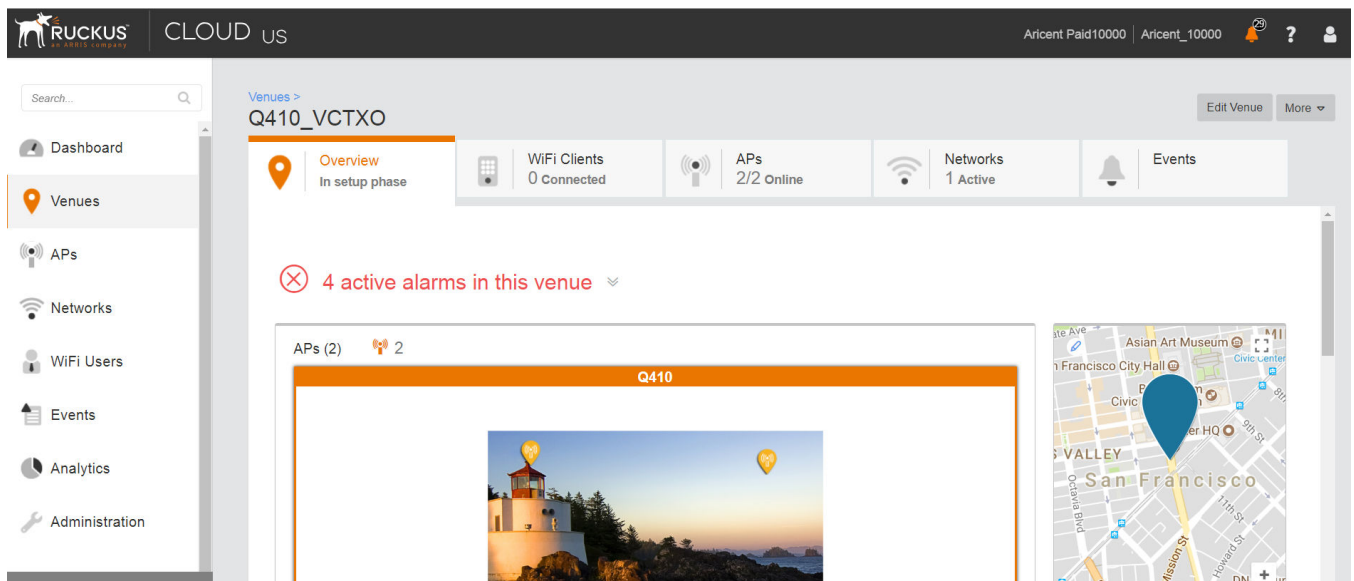
FIGURE 42 Venue Page



2. Click the desired venue to view its status.

The Overview screen appears displaying an informational message about the active alarms.

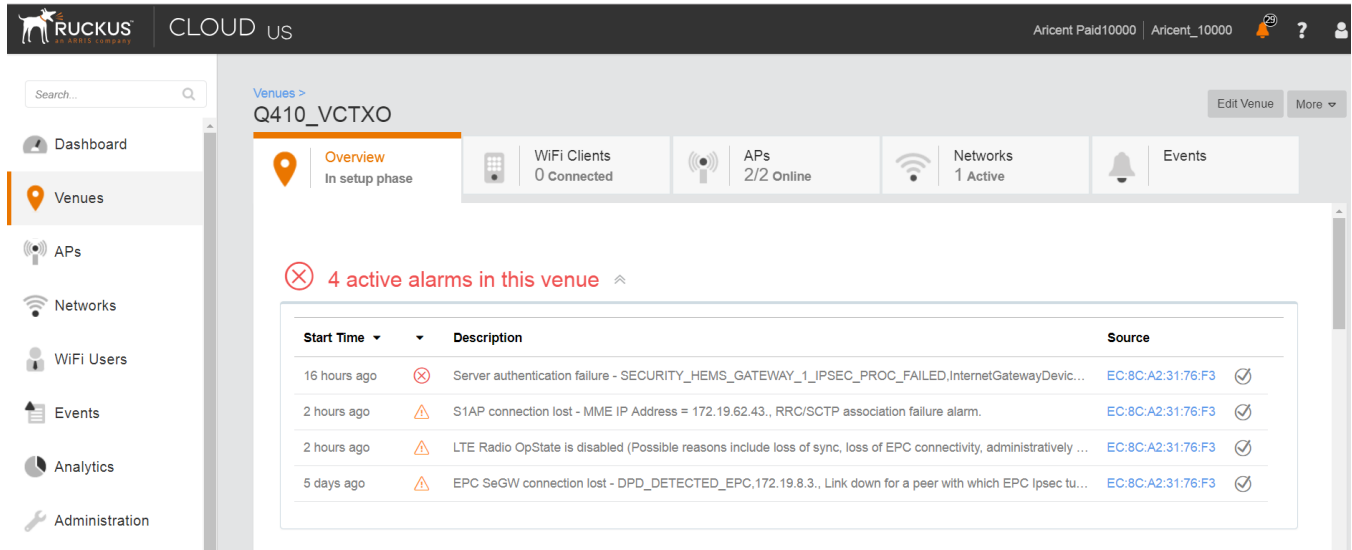
FIGURE 43 Venue Page Showing Number of Active Alarms



3. Click .

The screen displays details of all the active alarms in the venue.

FIGURE 44 Venue Page Showing Active Alarms



NOTE

If there are alarms that have occurred in the past or are not critical to be addressed for normal AP functions (as indicated by Operational status), "All good" is indicated under Overview. In such a case, you can ignore the alarms or clear them from the drop-down menu option against each AP on the leftmost column.

- Check all the alarms for each AP to identify any critical alarms that need to be addressed.
- Typical alarms indicates the component.
- When a specific connectivity issue occurs, it will impact the corresponding functionality and this may also be indicated on the AP LEDs. If EPC IP is unreachable or the S1 connection fails to establish, the EPC LED keeps blinking (For more information, refer to [Initial Setup Issues](#) on page 196).
- You must take appropriate action items to rectify the error as mentioned in the alarms.

Collecting LTE AP Logs via LTE AP Management

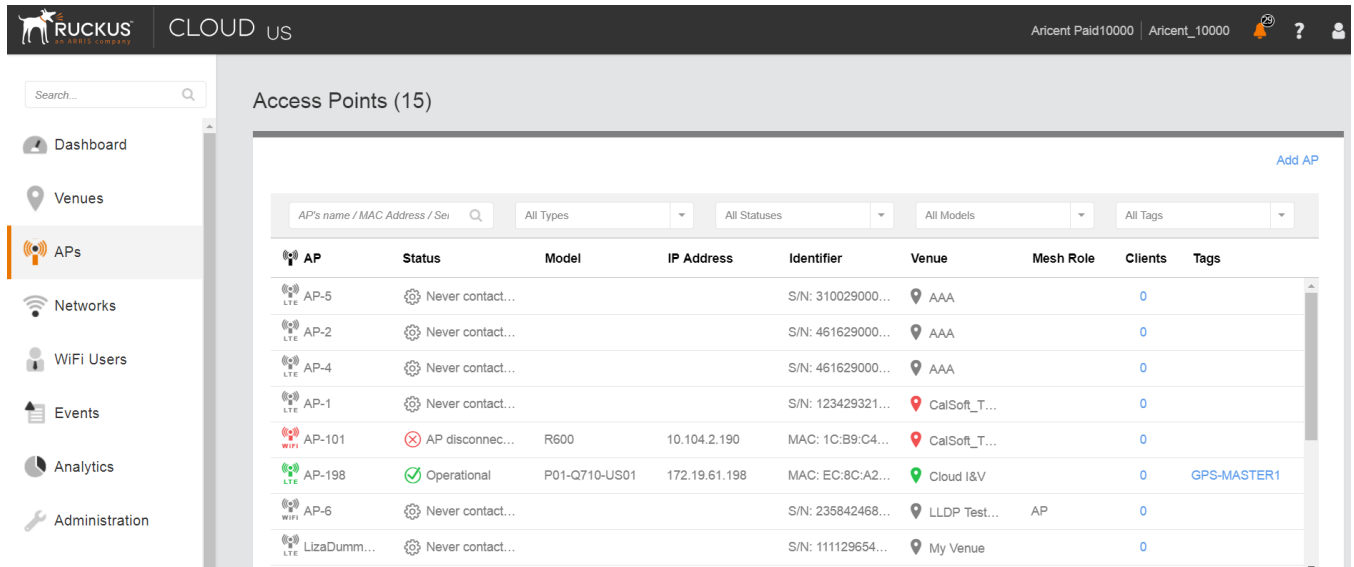
Q: How can I collect LTE AP logs through LTE AP Management?

To collect LTE AP logs through LTE AP Management, perform the following steps:

1. Log in to LTE AP Management and click **APs** on the left side of the screen.

The **Access Points** page appears showing the list of all APs.

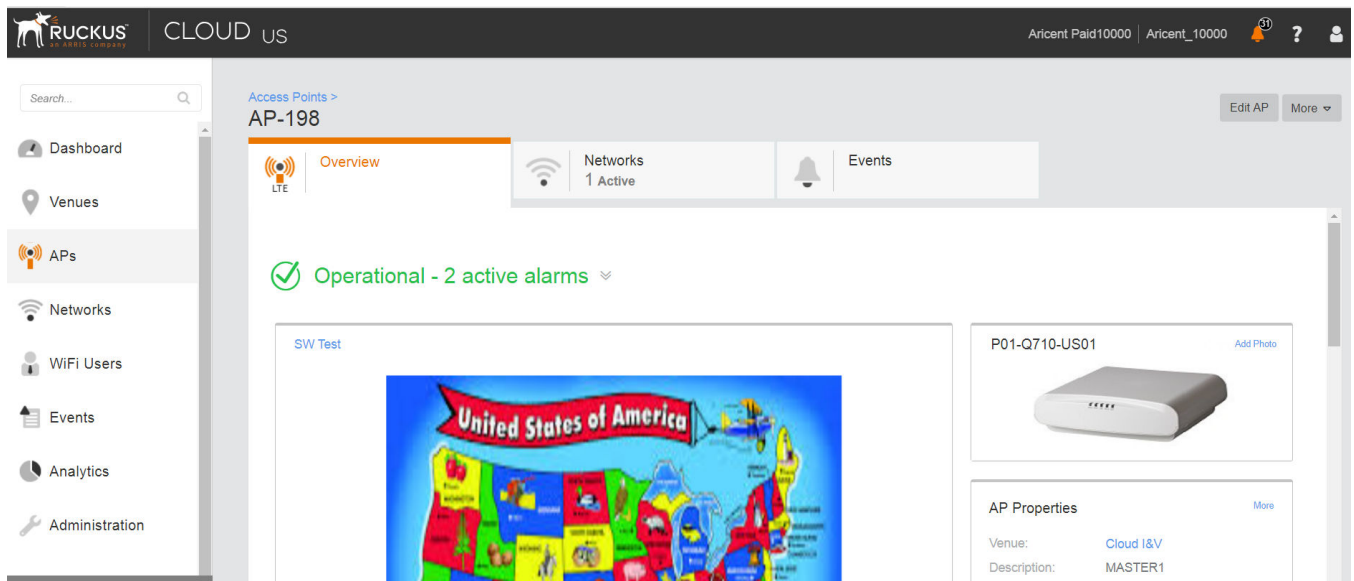
FIGURE 45 Access Points Page



2. Click an AP from which you want to collect the logs.

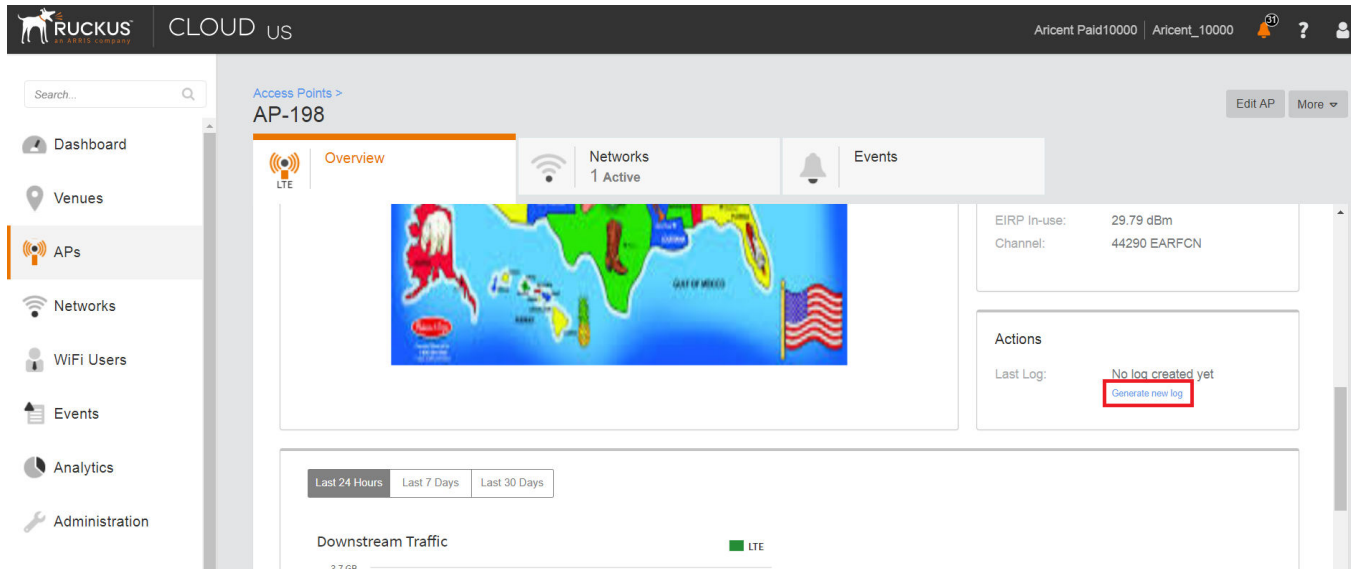
The details of the selected AP appears.


FIGURE 46 Access Point Details



3. Scroll down and click **Generate new log** under **Actions** right side, as shown in the following figure.

FIGURE 47 Generate AP Log



- Click  that is located next to **Last Log**: to download the .tar file to the local Downloads directory with all the relevant logs.

Debugging Performance Issues

Q: What are the commonly reported issues?

After provisioning LTE AP and enabling transmission, there may be rare scenarios that can cause performance issues.

The following table is a list of typical performance issues and suggested corrective actions.

TABLE 19 Performance Issues and Corrective Actions

ID	Issue	Details	Corrective Action
1	Poor data rate	Poor data rate measured in DL/UL or both directions compared to expected throughput.	<ol style="list-style-type: none"> 1. Check the backhaul capacity/throughput rating. 2. Obtain the RF logs and check sources of interference (RSRP/RSRQ values). 3. Check for UE handing off multiple times (also known as ping-pong effect) between more than one LTE AP.
2	UE disconnects frequently from network.	UE connection is dropped frequently and reconnects after unplugging.	If using a USB dongle/Wi-Fi Device over USB, check the dongle USB connection.
3	EPC connection down.	S1 connection disconnected after successful connection during initial setup.	<ol style="list-style-type: none"> 1. Check the S1 status via get S1APConfigParam command to match EPC parameters. 2. Check the IP reachability (try pinging the MME IP address from the AP). 3. Capture the Wireshark trace (or tcpdump) on the switch via port mirroring. 4. Open the "S1AP" messages and follow the sequence to learn the reason for rejection or setup failure.

TABLE 19 Performance Issues and Corrective Actions (continued)

ID	Issue	Details	Corrective Action
4	AP not transmitting although all connection are successful.	All LEDs are solid Green but LTE is dark - transmission stopped.	<ol style="list-style-type: none"> 1. Check whether the AP service button is ON. 2. Check alarms to detect if there are any issues reported with SAS availability/ response. 3. Check the statistics to obtain the CurrentGrant status. 4. Check the logs for SAS-CBSD communication and check for any error codes that have been reported.
5	Timing sync lost/ SYNC LED starts to blink.	In general, when a timing sync is lost, the SYNC LED is dark/ blinking indicating it is trying to regain connection with timing master/GPS.	<ol style="list-style-type: none"> 1. When in PTP-slave mode: Check connection with the Timing Master AP using the IP address. 2. When in PTP-Master mode: Check visibility to satellites/ line of sight to open sky, and relocate to a new position closer to the window or door.

Case 1: LTE AP is in sync but has disconnected from the ACS and/or Mgmt SecGW

Review the following information.

1. An AP reboots 24 hours after disconnection with the AP management platform when it is unable to reach LTE AP Management.
2. After reboot, an AP connects to the SC-R.
3. The SC-R sets relevant IP address of the SecGW and LTE AP management (ACS) on an LTE AP.
4. The LTE AP attempts to connect to the LTE AP Management
5. If an LTE AP is unable to connect, it keeps on retrying for 24 hours. On completion of 24 hours, steps 1, 2, and 3 mentioned above are repeated.
6. An AP repeats the above steps for a total of 3 times, one each reboot after 24 hours.
7. After a total of 96 hours from the first disconnection, AP reverts to the factory reset. In this case, any configuration that was set from ACS or using the CLI, get reset and in this case the earlier AP configuration is erased.

NOTE

The above-mentioned behavior is for the disconnection/not reachable case only. SC-R: sc-registrar - A database/ service in the management platform that provides each AP important connectivity information upon power up.

Case 2: LTE AP is in not in sync and has disconnected from the ACS and/or Mgmt SecGW:

Review the following information.

1. If after startup, the PTP hard sync does not occur, the behavior for network disconnection mentioned in case I above should be used.
2. If an external PTP device is configured (not using a Ruckus AP as the Timing Master) to provide timing information to the network, ensure that the following settings are set on the PTP source:
 - a. Ensure that the PTP source and rest of the APs are on the same Layer 2 network and the PTP traffic is allowed on any firewalls in between.
 - b. Select the 8275.2 profile on your timing source administration/ configuration page.
 - c. Set Domain to 44.

3. If GPS synchronization is does not occur from startup or the PTP phase sync is not achieved (but the PTP hard sync has been achieved), RSC reboots every hour till the synchronization is achieved. The timers mentioned in case I above does not apply in this case that is the LTE AP does not go to SC-R or perform a factory reset.
4. If AP was already synchronized when the network disconnected, and if it loses synchronization that is goes into holdover.
 - a. LTE AP reboots after 1 hour in the case of the PTP master assuming that 24 hours of the network disconnection have not occurred
 - b. LTE AP reboots after 2 hours in the case of the PTP slave assuming that 24 hours of the network disconnection have not occurred
5. If after reboot, AP achieves synchronization, but is still disconnected from the network, in that case behavior for network disconnection mentioned in case I above shall be used. Note that the disconnect reboot timer is applicable from the reboot in such a case.
6. If after a reboot, AP does not achieve synchronization, the behavior mentioned in this case II is applicable.

AP States in LTE AP Management

Q: What are the AP states in LTE AP Management?

The following are the AP states in the LTE AP Management:

- Never Contacted
- Contacted
- Connected
- Operational
- Disconnected

Q: Why does the AP state show Never Contacted in LTE AP Management?

The following are reasons for AP state to be Never Contacted:

- AP cannot connect to the internet.
 - Ensure that the AP connected IP network has access to the Internet and also has DNS server setup to resolve domain names such as www.google.com or www.yahoo.com.
 - Try connecting a laptop to the same network as the AP and use a browser to go to <https://sc-registrar.ruckuswireless.com>.
- Check if the requested ports are allowed on the network (firewall ports 4500...etc.)
- The AP is not in the factory reset state.

If an AP is not in the factory default (reset) state, it may not connect to the AP Management due to an incorrect resident configuration. Reset the AP to its factory defaults using the button located near the RJ45 port. A long press on this button for over 20 seconds will cause the AP restore to its factory default firmware and configuration. Power LED will be RED. AP will resume its boot-up procedures upon release of the reset button.

Q: Why AP state is Contacted but not Connected or Operational?

Check the following:

- Whether the AP to Management SecGW connection is flapping.
- Whether there are AP alarms or events on the AP and check that the IPsec tunnel is up.

Q: Why does AP state show Connected but not Operational?

The possible reasons for this issue could be one of the following.

- The AP admin state is disabled.

Check whether the AP Management has been administratively disabled from the UI by clicking **AP > More > Operation status Disable/Enable**

- The AP lost synchronisation.
 - If the AP is GPS source, AP may have lost connection to the GPS satellite.
 - If the AP is PTP source, AP may have lost connection to the PTP master.
- The AP to Network (EPC) connection is lost.
 - The SCTP connection timeout to EPC occurred.
 - The AP-EPC connection is lost.
 - The EPC is not reachable.
 - If a SecGW is configured for the EPC connection, the AP to SecGW connection may be lost. (All Ruckus-offered networks/ EPC services have a SecGW)
- The AP lost the grant.
 - The AP relinquished the Grant because of a timing sync failure or lost connection to EPC.
 - The AP-SAS heartbeat failed or communication failed.
 - An AP-SAS grant conflict occurred.
 - An AP-SAS registration error occurred.
 - SAS revoked the grant.

Ruckus LTE Alarms

- Temperature Critical Alarm..... 208
- Temperature Warning Alarm..... 208
- LTE Radio OpState Disabled Alarm..... 209
- RSC at max capacity..... 209
- Loss of Sync Sources Alarm..... 209
- HoldOver Timeout Alarm..... 210
- Dead Peer Detection Alarm..... 210
- SCTP Association Failure Alarm..... 211
- File Upload Failure Alarm..... 211
- Software Activation Failure Alarm..... 211
- Configuration Image Download Failure Alarm..... 212
- Server Authentication Failure Alarm..... 213
- Server Certificate Revoked Alarm..... 216
- Server Revocation Check Failure Alarm..... 218
- Server Root CA Certificate Missing or Expired Alarm..... 219
- OCSP Server not Reachable Alarm..... 220
- NTP TOD Sync Failure Alarm..... 222
- RA/CA not reachable Alarm..... 223
- Ruckus LTE AP Disconnected from Management Cloud SeGW..... 224
- Enrolment Failure Alarm..... 224
- CBSD Registration Error Alarm..... 225
- CBSD Grant Error Alarm..... 226
- CBSD Grant Suspended Alarm..... 226
- SAS Certificate Expired Alarm..... 227
- SAS Certificate Invalid Alarm..... 227
- SAS not Reachable Alarm..... 227
- CBSD Installation Error Alarm..... 228
- Conclusive CBSD Location Change Detection Alarm..... 228
- Probable CBSD Location Change Detection Alarm..... 229
- RSC Startup Failure Alarm..... 229
- tx LO Sync Loss Alarm..... 229
- rx LO Sync Loss Alarm..... 230
- txPowerExceededMax Alarm..... 230
- txPowerOutOfBounds Alarm..... 230
- rxDiversity Alarm..... 231
- GPS Lost Alarm..... 231
- LTE SecGW Alarms..... 232
- LTE Controller Alarms..... 232
- LTE RSM Alarms 233

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).

TABLE 20 LTE AP Alarm IDs

101 on page 208	Temperature Warning Alarm on page 208	105 on page 209	RSC at max capacity on page 209	Loss of Sync Sources Alarm on page 209	HoldOver Timeout Alarm on page 210	Dead Peer Detection Alarm on page 210	SCTP Association Failure Alarm on page 211
-----------------	---------------------------------------	-----------------	---------------------------------	--	------------------------------------	---------------------------------------	--

TABLE 20 LTE AP Alarm IDs (continued)

115	116	117	119	120	122	123	124
125	126	127	129	130	133	134	136
136	137	138	139	141	143	511	801
802	803	804	805	901	914		

TABLE 21 SecGW AlarmsIDs

304	307	308	309	310	314
-----	-----	-----	-----	-----	-----

TABLE 22 LTE Controller Alarms IDs

LTC-011	LTC-012	LTC-013	LTC-21
---------	---------	---------	--------

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	<ol style="list-style-type: none"> Switch off LTE AP and reboot it. 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	<ol style="list-style-type: none"> Switch off LTE AP and reboot it. 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.			

RSC at max capacity

TABLE 23 RSC at max capacity alarm

Alarm Identifier	106
Description	The LTE radio is at full capacity and cannot accept additional UE attachment requests.
Default Severity	
Entered Event	
Exit Event	Sent whenever the number of attached UEs is back to nominal range. NOTE This event clears the max capacity alarm.
Managed Objects	—
System Actions	—
Event Type	—
Probable Cause	—
Specific Problem	—
Corrective Action	—

Loss of Sync Sources Alarm

Alarm Identifier	108
Description	Sync Lost: All Sync sources lost: Alarm is triggered when all sync sources are lost.

Ruckus LTE Alarms

HoldOver Timeout Alarm

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	<ol style="list-style-type: none"> Link down for a peer with which EPC IPsec tunnel is established. 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	<ul style="list-style-type: none"> 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 when 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.			

Ruckus LTE Alarms

Configuration Image Download Failure Alarm

Perceived Severity	Minor			
Action to clear alarm	<ol style="list-style-type: none"> 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				<ol style="list-style-type: none"> 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

Server Authentication Failure Alarm

Alarm Identifier	122
Description	Server authentication failure - <Additional Text>, <Additional Info>.
Details	
Additional Information	<ol style="list-style-type: none"> 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

Ruckus LTE Alarms

Server Authentication Failure Alarm

<p>Action to clear alarm</p>	<ol style="list-style-type: none"> 1. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.
2. IhemsDiscoveryFailure	When iHeMS becomes reachable.	iHeMS Reachability failure.	LTE AP retries to check reachability of initial server until reboot.	iHeMS discovery failure.
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.

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.
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.
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.
7. IpcsecProcedureFailedForHemsSecurityGateway1	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.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer1.
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.
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.
10. IpcsecProcedureFailedForHemsSecurityGateway2	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.
11. HemsSecurityGateway3FqdnResolutionFailure	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.
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.
13. IpcsecProcedureFailedForHemsSecurityGateway3	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.
14. EPCSecurityGateway1FqdnResolutionFailure	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.
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,InternetGatewayDevice.X_001392_FAPMgmtSecGW.SecGWServer1.

Ruckus LTE Alarms

Server Certificate Revoked Alarm

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.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer1.
17. EPCSecurityGateway2FqdnResolutionFailure	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.
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.
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.
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.
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.

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		<ol style="list-style-type: none"> 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. HEMSecGw1CertificateRevoked	No exit event.	HeMS Security Gateway 1 certificate is revoked.	Security module halts until reboot timer expires*.	HeMS gateway 1 Certificate revoked.
2. HEMSecGw1CACertificateRevoked	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. HEMSecGw2CertificateRevoked	No exit event.	HeMS Security Gateway 2 certificate is revoked.	Security module halts until reboot timer expires*.	HeMS gateway 2 Certificate revoked.
4. HEMSecGw2CACertificateRevoked	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. HEMSecGw3CertificateRevoked	No exit event.	HeMS Security Gateway 3 certificate is revoked.	Security module halts until reboot timer expires*.	HeMS gateway 3 Certificate revoked.
6. HEMSecGw3CACertificateRevoked	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.

Ruckus LTE Alarms

Server Revocation Check Failure Alarm

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. IheMSCertificateRevoked	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	<ol style="list-style-type: none"> Sent when OCSP/CRL procedure failed for EPCSecurityGateway2. Sent when OCSP/CRL procedure failed for EPCSecurityGateway3. Sent when iHeMS OCSP/CRL procedure failed. Sent when Ruckus LTE AP OCSP/CRL procedure failed. 			
Specific Problem	Server revocation check failure.			
Perceived Severity	Major			
Action to clear alarm	<ol style="list-style-type: none"> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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.Se cGWServer2,<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.Se cGWServer1,<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.

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	<ol style="list-style-type: none"> 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

Ruckus LTE Alarms

OCSF Server not Reachable Alarm

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.

OCSF Server not Reachable Alarm

Alarm Identifier	125
Description	OCSF/CRL Server not reachable: <Additional text>, <Additional Info>
Details	
Additional Information	<ol style="list-style-type: none"> 1. Sent when Ruckus LTE AP is unable to resolve FQDN of HeMS SecGw1 OCSF/CRL server 2. Sent when Ruckus LTE AP is unable to ping HeMS SecGw1 OCSF/CRL server. 3. Sent when Ruckus LTE AP is unable to resolve fqdn of HeMS SecGw2 OCSF/CRL server. 4. Sent when Ruckus LTE AP is unable to ping HeMS SecGw2 OCSF/CRL server. 5. Sent when Ruckus LTE AP is unable to resolve FQDN of HeMS SecGw3 OCSF/CRL server. 6. sent when Ruckus LTE AP is unable to ping HEMS SecGw3 OCSF/CRL server. 7. Sent when Ruckus LTE AP is unable to resolve fqdn of EPC SecGw1 OCSF/CRL server. 8. Sent when Ruckus LTE AP is unable to ping EPC SecGw1 OCSF/CRL server. 9. Sent when Ruckus LTE AP is unable to ping EPC SecGw2 OCSF/CRL server. 10. Sent when Ruckus LTE AP is unable to resolve fqdn of EPC SecGw3 OCSF/CRL server. 11. Sent when Ruckus LTE AP is unable to ping EPC SecGw3 OCSF/CRL server.
Specific Problem	OCSF/CRL Server not reachable.
Perceived Severity	Major

Action to clear alarm	<ol style="list-style-type: none"> 1. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.
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.
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.
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.
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.
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.

Ruckus LTE Alarms

NTP TOD Sync Failure Alarm

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.
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 not reachable,InternetGatewayDevice.Services.FAPService. 1.FAPControl.LTE.Gateway.SecGWServer2.
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.
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.
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.

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	<ol style="list-style-type: none"> 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 when Ruckus LTE AP is unable to ping to CMP Server for CBRS PKI. 			
Specific Problem	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.
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.
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.
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.

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	<ol style="list-style-type: none"> Link down for a peer with which HeMS IPsec tunnel is established. 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	<ol style="list-style-type: none"> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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.
2. IpcProcedureFailedForHemsSecurityGateway1	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.

Enrolment Failure Alarm

Alarm Identifier	130			
Description	<Specific Problem>, <Additional text>, <Additional Information>			
Details				
Additional Information	<ol style="list-style-type: none"> Sent when CMP server is Not responding for NHN PKI. Sent when CMP procedure failed for CBRS PKI. Sent when CMP server is Not responding for CBRS PKI. Sent when CMP procedure failed for NHN PKI. 			
Specific Problem	<ol style="list-style-type: none"> NHN PKI RA/CA not responding. Enrolment failure for CBRS PKI. CBRS PKI RA/CA not responding. Enrolment failure for NHN PKI. 			
Perceived Severity	Major			

Action to clear alarm	<ol style="list-style-type: none"> 1. Check for CMP procedure service running on CMP Server and configured properly. 2. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.
2. CMPPProcedureFailedPkiNhnway1	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.
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.
4. CMPPProcedureFailedPkiCbrs	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.

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	<ul style="list-style-type: none"> • 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

Ruckus LTE Alarms

CBSD Grant Error Alarm

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	<ul style="list-style-type: none"> 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 (cbstdId).	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	<ul style="list-style-type: none"> 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.		

Ruckus LTE Alarms

CBSD Installation Error Alarm

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

RSC Startup Failure Alarm

TABLE 24 RSC Startup Failure alarm

Alarm Identifier	511
Description	Failure occurring during system startup.
Default Severity	Major
Entered Event	Startup fails due to some reason. For example: Sync not achieved.
Exit Event	Sync achieved.
Managed Objects	SOM
System Actions	RSC goes for reboot.
Event Type	Equipment Alarm
Probable Cause	Configuration or customizing error.
Specific Problem	System startup failure due to failure in submodule.
Corrective Action	Check for the reason of startup failure and the proper configurations.

tx LO Sync Loss Alarm

TABLE 25 tx LO Sync Loss alarm

Alarm Identifier	801
Description	Alarm triggered when Tx Local Oscillator goes out of sync.
Default Severity	Major
Entered Event	Local Oscillator for one of the carrier's transmit paths has lost synchronization.
Exit Event	Local Oscillator for one of the carrier's transmit paths is in sync.
Managed Objects	SOM
System Actions	Critical alarm is raised and carrier is disabled and enable carrier request is rejected.

TABLE 25 tx LO Sync Loss alarm (continued)

Event Type	Equipment Alarm
Probable Cause	Transmitter Failure
Specific Problem	Hardware failure
Corrective Action	Clear alarm via RF OAM action and enable carrier.

rx LO Sync Loss Alarm

TABLE 26 rx LO Sync Loss alarm

Alarm Identifier	802
Description	Alarm triggered when Rx Local Oscillator goes out of sync.
Default Severity	Major
Entered Event	Alarm set when Local Oscillator for one of the Carrier's Rx Paths has lost synchronization.
Exit Event	Alarm cleared if the Local Oscillator regains synchronization.
Managed Objects	SOM
System Actions	Warning alarm is raised.
Event Type	Equipment Alarm
Probable Cause	Receiver Failure
Specific Problem	Hardware failure
Corrective Action	No OEM action required.

txPowerExceededMax Alarm

TABLE 27 txPowerExceededMax alarm

Alarm Identifier	803
Description	Alarm triggered when Tx Power exceeds maximum expected value.
Default Severity	Major
Entered Event	Alarm triggered when Tx Power exceeds maximum expected value.
Exit Event	Alarm cleared when Tx power falls in expected range.
Managed Objects	SOM
System Actions	Carrier will be disabled when alarm is detected and a critical alarm is raised.
Event Type	Equipment Alarm
Probable Cause	Transmitter Failure
Specific Problem	Hardware failure
Corrective Action	Clear alarm via RF OAM Action and Enable carrier.

txPowerOutOfBounds Alarm

TABLE 28 txPowerOutOfBounds alarm

Alarm Identifier	804
Description	Alarm triggered when Tx Power is outside the expected range.

TABLE 28 txPowerOutOfBounds alarm (continued)

Default Severity	Major
Entered Event	Alarm triggered when Tx Power exceeds expected range and cleared once back within the expected range.
Exit Event	This alarm will be cleared if Tx Power returns to the proper range.
Managed Objects	SOM
System Actions	A warning alarm is raised.
Event Type	Equipment Alarm
Probable Cause	Transmitter Failure
Specific Problem	Hardware failure
Corrective Action	No OEM action required.

rxDiversity Alarm

TABLE 29 rxDiversity alarm

Alarm Identifier	805
Description	Alarm triggered when difference of maxRssidB and minRssidB exceeds threshold of 6.0 dB.
Default Severity	Major
Entered Event	Alarm set if one of the Carrier's Rx Paths is in a failed state.
Exit Event	This alarm will be cleared if a signal is detected again on all Rx paths.
Managed Objects	SOM
System Actions	A warning alarm is raised.
Event Type	Equipment Alarm
Probable Cause	Receiver Failure
Specific Problem	Hardware failure
Corrective Action	No OEM action required.

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.

LTE SecGW Alarms

This section provides information about alarms generated by the SecGW.

TABLE 30 LTE Security Gateway Alarms

Alarm Number	Description
304	RSC disconnected from management cloud SeGW
307	RSC IKESA IP address renewal was initiated
308	RSC IKESA establishment timeout
309	RSC is not authorized
310	RSC authentication failure - RSC client certificate has been revoked
314	RSC Integrity/Confidentiality algorithm could not be successfully negotiated

LTE Controller Alarms

This section provides information about alarms the generated by management cloud , LTE controller service.

Configuration Failure Alarm

Alarm Identifier	LTC-011			
Description	Configuration failed. Reboot the AP or factory reset for a system initiated retry. Failed parameters: <%Parameter Name%>			
Details				
Additional Information	Alarm is triggered when AP does not accept a configuration that is created on the tenant portal.			
Specific Problem	—			
Perceived Severity	Critical			
Action to clear alarm	Switch off the LTE AP and switch it on.			
Entered Event	Exit Event	Probable Cause	System Action	Additional Text
When a configuration fails on an AP.	When a configuration is sent to an AP again. It may be due to AP reboot, factory reset or a configuration change on the tenant portal.	Internal conflict of configuration parameters.	Configuration change, a reboot or factory reset of AP is required. Any of these actions will trigger configuration re-try.	—

Synchronization Error Alarm

Alarm Identifier	LTC-011			
Description	The AP cannot be configured due to a synchronization error. Reboot or Factory Reset AP for a system initiated retry			
Details				
Additional Information	Alarm is triggered when the Cloud is unable to get the information about current configuration of the AP.			
Specific Problem	—			
Perceived Severity	Critical			
Action to clear alarm	Switch off the LTE AP and switch it on.			
Entered Event	Exit Event	Probable Cause	System Action	Additional Text

When AP does not accept the request from the Cloud.	When a configuration is changed on the tenant portal or a reboot or factory reset is triggered on AP.	Internal error on AP side or an invalid firmware version.	A reboot or factory reset of AP is required. Any of these actions will trigger synchronization re-try.	—
---	---	---	--	---

Configuration Pending Alarm

Alarm Identifier	LTC-013			
Description	Configuration is pending. Make sure that the AP is in connected to the Cloud.			
Details				
Additional Information	Alarm is triggered when cloud is unable to send configuration to the AP for some time (more than 10 minutes).			
Specific Problem	—			
Perceived Severity	Major			
Action to clear alarm	Switch off the LTE AP and switch it on.			
Entered Event	Exit Event	Probable Cause	System Action	Additional Text
When AP does not respond to a request from the Cloud.	When AP starts responding or a configuration is re-triggered due to a configuration change on the tenant portal, reboot or factory reset.	The AP is not connected or it is occupied by other requests such as firmware download.	If the AP is connected and a configuration is still pending for more than 20 to 30 minutes, a factory reset is required.	—

TDD Configuration Failure Alarm

Alarm Identifier	LTC-021			
Description	Configuration failed: TDD value of AP is unknown. Reboot or Factory Reset is required.			
Details				
Additional Information	Alarm is triggered when the Cloud is unable to get the current TDD (time division duplex) configuration from the AP. An invalid TDD configuration on one AP may affect other APs located in the same venue.			
Specific Problem	—			
Perceived Severity	Critical			
Action to clear alarm	Switch off the LTE AP and switch it on.			
Entered Event	Exit Event	Probable Cause	System Action	Additional Text
When AP does not respond to the TDD request from the Cloud.	When reboot or factory reset on AP is executed.	An internal AP error.	A reboot or factory reset may be required. A reboot or factory reset triggers a new TDD check.	—

LTE RSM Alarms

This section provides information about alarms generated by the RSM.

Configuration Failure Alarm

Alarm Identifier	CBRS-001
------------------	----------

Ruckus LTE Alarms
 LTE RSM Alarms

Description	Less than <available ECGIs> unique ECGIs are now available for your networks with PLMN ID <PLMNID>. Please configure additional records for this PLMNID.			
Details				
Additional Information	<p>Alarm is triggered when a specific PLMN ID has ECGI records, and total availability for it (by summing all the related ECGI records) is below one of the thresholds (100/50/10) - trigger an Alarm to the tenant, notifying the status for this PLMN ID.</p> <p>An alarm should be sent out when a certain <number> of the unique ECGIs are left available for allocation on a per PLMN ID level. This is to ensure that tenants are aware of the need to submit a request to procure additional Identifiers from the CBRS-A authorities.</p>			
Specific Problem	—			
Perceived Severity	Major (if 'available ECGIs' is 100 or 50) / Critical (if 'available ECGIs' is 10)			
Action to clear alarm	Increase ECGI availability for the given PLMN ID (by adding a new ECGI record for this PLMN ID)			
Entered Event	Exit Event	Probable Cause	System Action	Additional Text
When a PLMN ID has ECGI records defined, and a threshold (100/50/10) is exceeded (and alarm for this threshold was not yet triggered).	When ECGI availability for the given PLMN ID is increased and is above the threshold used for the alarm.	<p>New APs were added to a venue on which the network with the given PLMN ID is activated.</p> <p>Another option is that a network with the given PLMN ID was activated on venue that has APs on it.</p>	<p>User (tenant) has to purchase additional Macros from CBRS-A and add a new ECGI record for the given PLMN ID with the new Macro purchased.</p> <p>This will increase availability by 128</p>	—

COMMScope®
RUCKUS®

© 2020 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>