



Ruckus CBRS/Private LTE

Deployment Guide

Table of Contents

<i>Intended Audience</i>	3
<i>Overview</i>	4
Citizens Broadband Radio Service (CBRS)	4
Ruckus CBRS.....	4
<i>Private LTE</i>	5
Ruckus CBRS Private LTE	5
<i>Network Topology</i>	6
Components of a Private LTE Network	6
<i>Configuration</i>	8
Adding a Venue	8
Adding an LTE Network	11
Configuring SAS	13
Adding LTE AP and verifying operation	13
SIM Management Service (SMS)	19
<i>Summary</i>	21

Intended Audience

This document provides an overview of how to configure Ruckus products to support a Private LTE solution. Step-by-step procedures for configuration and testing are demonstrated. Some knowledge of the Ruckus Cloud and access points is recommended. This document is written for and intended for use by technical engineers with background in Wi-Fi design and 802.11/wireless engineering principles.

For more information on how to configure Ruckus products, please refer to the appropriate Ruckus user guide available on the Ruckus support site, <http://support.ruckuswireless.com>.

Overview

This document describes how to configure the Ruckus products to support the Ruckus Citizens Broadband Radio Service (CBRS) solution. The document is broken into the following main categories

- CBRS
- Private LTE
- Topology
- Configuration

Citizens Broadband Radio Service (CBRS)

If an enterprise wants to build a private wireless network using current technologies, it must do so using unlicensed spectrum in the 2.4GHz or 5.8 GHz bands. The de-facto standard for this wireless connectivity is Wi-Fi. While it is relatively simple to deploy an initial Wi-Fi network, it cannot always provide predictable latency, quality of service (QoS) or bandwidth. This is particularly true when access points (APs) are heavily loaded or operating in challenging environments with high RF interference.

Long-Term Evolution (LTE) wireless networks were developed to operate with the highest level of predictability and QoS and are designed to minimize RF interference. LTE is deployed in the 3.5 GHz band by mobile operators in many countries worldwide where it is available as licensed spectrum. Until now, LTE deployments have been limited primarily to service providers and mobile operators due to the level of complexity, cost, and regulatory licensing requirements. This is changing in the U.S. as the FCC makes spectrum in the 3.5 GHz band (CBRS) available to enterprises for private LTE networks. This band was previously not licensed to mobile operators in the U.S. because it already had incumbent users, such as the U.S. Navy, that are difficult to relocate. However, the typical utilization is very low, offering opportunities to use the band without endangering incumbent traffic if managed correctly.

The FCC is now making this spectrum available under a new set of licensing rules that protects the incumbents while making the spectrum broadly available for a wide set of users.

Ruckus CBRS

Ruckus' proven performance and ease of use combines with LTE to tackle the hardest connectivity challenges that Wi-Fi alone cannot address. This includes:

- **Distance:** The range of coverage for Ruckus CBRS deployments is as much as 4 times the range of a typical 5GHz cell. This is advantageous for things like inventory management, automation, and general network connectivity for employees.
- **Better network time coordination:** Advantageous for automation and robotics applications
- **Network security:** With the emergence of "zero trust networking", Wi-Fi and wired networks have become much more complex to maintain and deploy under this model. Ruckus CBRS private LTE brings a zero-trust level of security with the ease of a typical Wi-Fi deployment.
- **Better roaming:** Decisions concerning roaming are handled at the network level instead of the client as they are in Wi-Fi deployments.

Private LTE

Private LTE is a network restricted to one enterprise (thus the private designation). By taking advantage of the benefits of low latency and high predictability, a private LTE network is ideal as a method of efficiently connecting people and things and securing data. A key differentiator between a private LTE network and that of a service provider LTE network is the elimination of the LTE device connection to a core network of public mobile operators. This allows an enterprise freedom in how it deploys and manages the wireless network.

A private LTE network, furthermore, eradicates the restrictions associated with a conventional network system, such as Ethernet or Wi-Fi, by supporting both client and machine communication on a single network.

Ruckus CBRS Private LTE

As a co-founder of the CBRS Alliance, Ruckus Networks has been at the forefront advocating for CBRS and was the first vendor to ship an FCC-approved CBRS access point/base station. Ruckus CBRS is 100% LTE. All the benefits of Ruckus CBRS— improved security, latency, superior client management and roaming decisions (handled at the network level instead of the client), and so on—apply to a Ruckus wireless network.

Ruckus CBRS allows the deployment of private LTE networks in all aspects of enterprise deployments.

Cloud Managed: private LTE networks are managed in the cloud by the Ruckus Enhance Management Service (EMS). This negates the need for building out a virtual controller or the installation of additional management hardware. The system can be managed from anywhere at any time.

Dedicated Equipment: By using dedicated equipment, the private LTE network and its performance is independent from other users, and free from issues such as sudden traffic surges that can happen in a shared network. This benefit is essential for industrial and enterprise applications where productivity must be maintained at high and predictable levels. Having a local and dedicated network also enables full control of the data. For example, a company can ensure that sensitive data does not leave the premises.

- **Optimized:** By serving the needs of a single company, the private LTE network can be tailored for that company's specific Internet of Things (IoT) applications. Examples of such optimization are QoS and mobility settings. With customized QoS, consistent service can be provided for the critical applications irrespective of the network load. With customized mobility settings, the behavior can be optimized for local applications; for example, to perform a faster reconnection in the unlikely event of a link failure.
- **Readily deployed:** With semi-licensed CBRS spectrum available for anyone to use for private LTE networks, deployment of private LTE networks is easy, which enables new entities to enjoy the benefits of LTE without the cumbersome complexity normally associated with LTE. The ease of use and adoption will only fuel an increasing number of UEs (clients). In addition, the ability to leverage the LTE standard allows access to features such as self-organizing networks and to network architectures with both self-contained or virtual/hosted core networks.

Ruckus CBRS provides private LTE networks that deploy with the ease of a typical Wi-Fi network while maintaining the exceptional characteristics of LTE. Ruckus CBRS is a cloud-managed system that is accessible from anywhere. The security provided by a private LTE network meets and exceeds zero trust network requirements as well as industry safety and privacy standards. The list of CBRS-ready devices continues to expand day by day and will soon offer everything from embeddable chips, IoT, phones, and many other devices-- opening a wide array of possible deployments.

Network Topology

Components of a Private LTE Network

The structure of a private network is like that of a public mobile operator. The key differences are in how it is licensed, deployed and operated. There is no need for any roaming agreements and, once the site for deployment is approved by the FCC, the operator owns that space for their allotted frequency slice. The Private LTE operator has control over their Evolved Packet Core (EPC) and can control all device traffic on their private network.

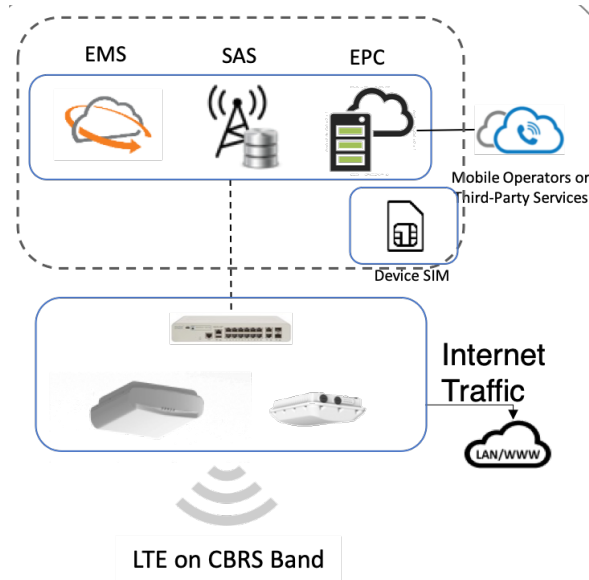


FIGURE 1: PRIVATE LTE NETWORK TOPOLOGY

Spectrum Access Server (SAS) is responsible for protecting incumbents (other operators transmitting on the spectrum) from harmful interference from new deployments. A Citizens Band Radio Service Device (CBSD) is a base station that must connect to a SAS when the CBSD is powered on. The base station provides its coordinates (latitude, longitude, altitude) and globally unique CBSD identifier to the SAS. Based on this information, the SAS provides the base station with the channels not already in use within the CBRS spectrum. Multiple entities operate SAS systems and there is a standard interface between the SAS and base station that allows them to interoperate. Technically, CBRS rules allow the SAS to change the channels available to a base station at any time to protect higher tier users. For example, if a navy radar in a given location starts to use a specific portion of the CBRS spectrum, the SAS becomes aware of this. The SAS will then reassign all lower priority base stations operating in that area and using that specific part of the CBRS spectrum to other channels within the CBRS spectrum within 5 minutes.

The SAS is vital for keeping interference between LTE networks low—a requirement for low latency and high predictability.

Evolved Packet Core (EPC) is the logical backbone for providing voice and data on LTE networks. This is where the 3GPP functions and routing are managed as well as maintenance of 3GPP-specific database contents. Much of the complexity of an LTE network resides within the EPC. Once an EPC is in place, the private LTE network becomes just another way to gain IP connectivity for the enterprise IP network and services, exactly in the same way as Ethernet or Wi-Fi are used.

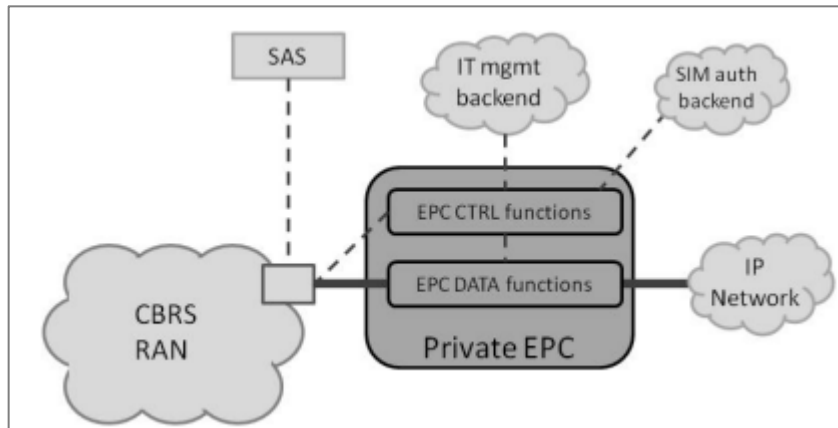


FIGURE 2: EVOLVED PACKET CORE (EPC)

Client devices, also called User Equipment (UE), connect to the LTE network. Enterprises can use any UEs that support the new 3GPP band for CBRS, called Band 48, on their private LTE network. Since mobile operators plan to use Band 48 as well, there will be a wide range of off-the-shelf CBRS UEs for private LTE networks, ranging from smart phones to Internet of Things (IoT) modules.

Public Land Mobile Network Identifier (PLMN-ID) is how an LTE network is identified to the UE device. Each mobile operator has a unique PLMN-ID. The 3GPP specification allows each mobile operator to create Closed Subscriber Groups (CSG) to offer separate access authorization and differentiated services to specific groups of its subscribers. An LTE Radio Access Network (RAN) broadcasts the supported PLMN-IDs as well as the CSG-ID served by the specific local LTE deployment.

International Mobile Subscriber Identifier (IMSI) is used for LTE subscriber identification and authentication. A subscriber's IMSI is stored on a SIM card and is tied to the PLMN-ID of the mobile operator that issued the SIM card.

Configuration

Preliminary Cloud configuration can be done via a web browser using a PC or laptop (details listed below). Ruckus Cloud Mobile App from your phone or iPad can also be used to add or change network and AP configurations. Once powered up completely, the default behavior of the AP is to seek Cloud environment connectivity, and by virtue of previously added configuration on cloud as well as default AP config, it will connect to the appropriate instance of Ruckus Cloud.

Cloud initiates the following default actions (no user intervention required) once an AP connects:

- Check AP software build version and upgrades to latest approved version.
- Apply basic configuration (venue & network configuration) to the AP.
- Report any alarms/ events identified on AP.

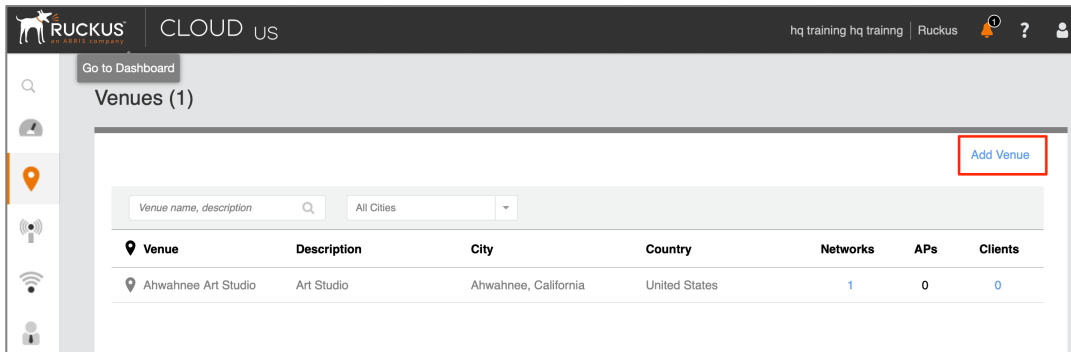
Turn AP Service ON to get the LTE Service.

The config steps can be summarized into the following steps:

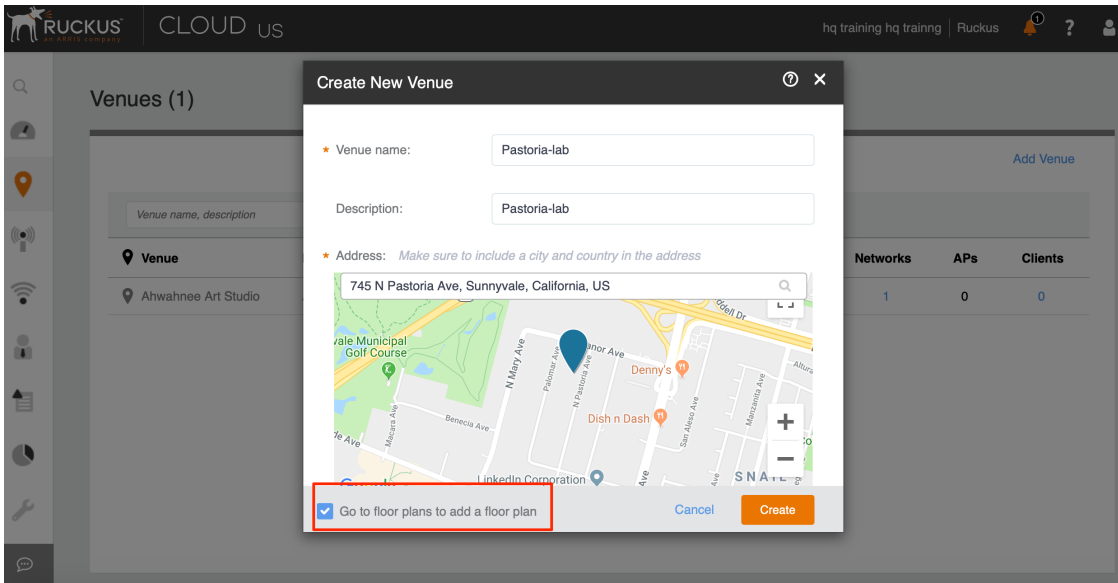
1. Adding a venue
2. Adding an LTE Network
3. Configuring SAS
4. Adding an LTE AP and verifying operation
5. Accessing SIM Management Service (SMS)

Adding a Venue

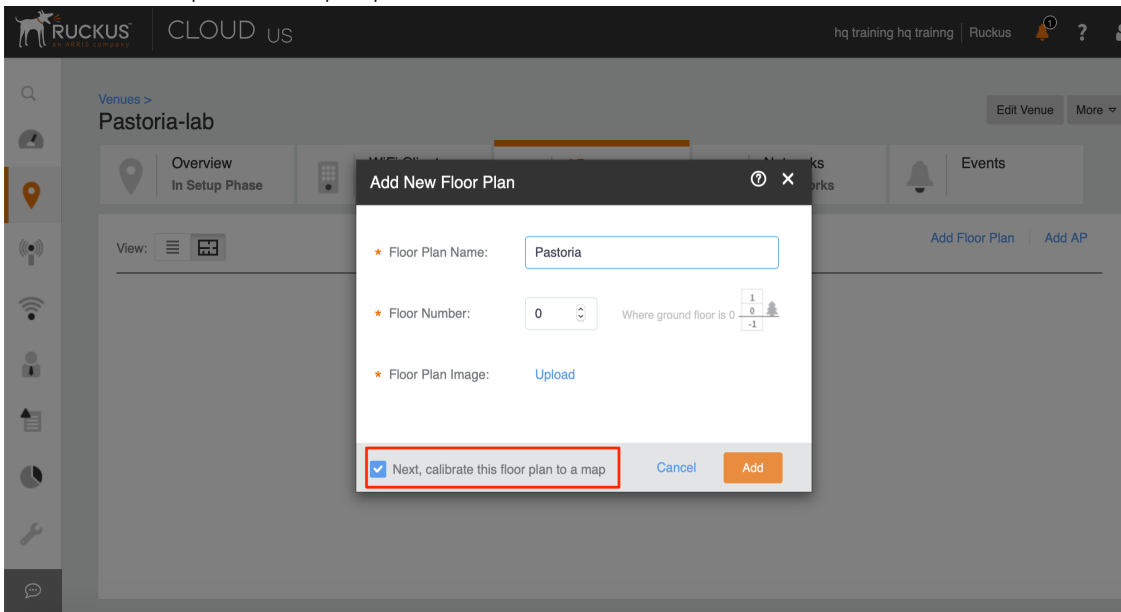
1. Click the “Add Venue” button on the Venues page.



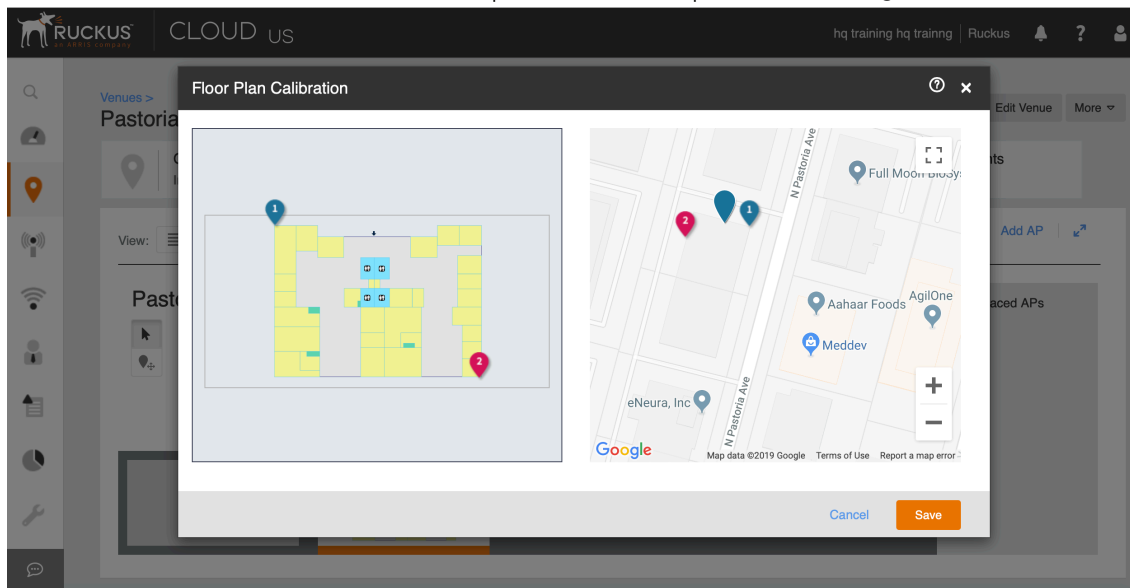
2. Enter a venue name, address and make sure the "Go to floor plans to add a floor plan" option checked. Click Create.



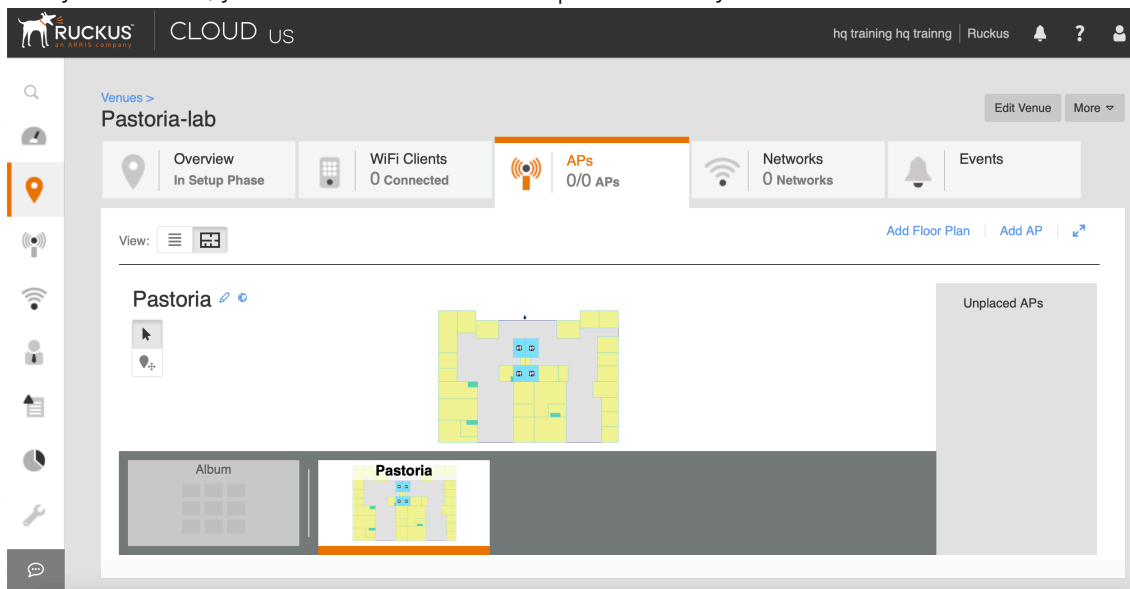
3. The "Add a new floor plan" dialog box is displayed. Enter the floor plan details and upload the floor plan. Make sure the "Next, calibrate this floor plan to a map" option checked. Click Add.



- For the Floor Plan Calibration, ensure that the points 1 and 2 are placed on the diagonal far corners of the building for best results.

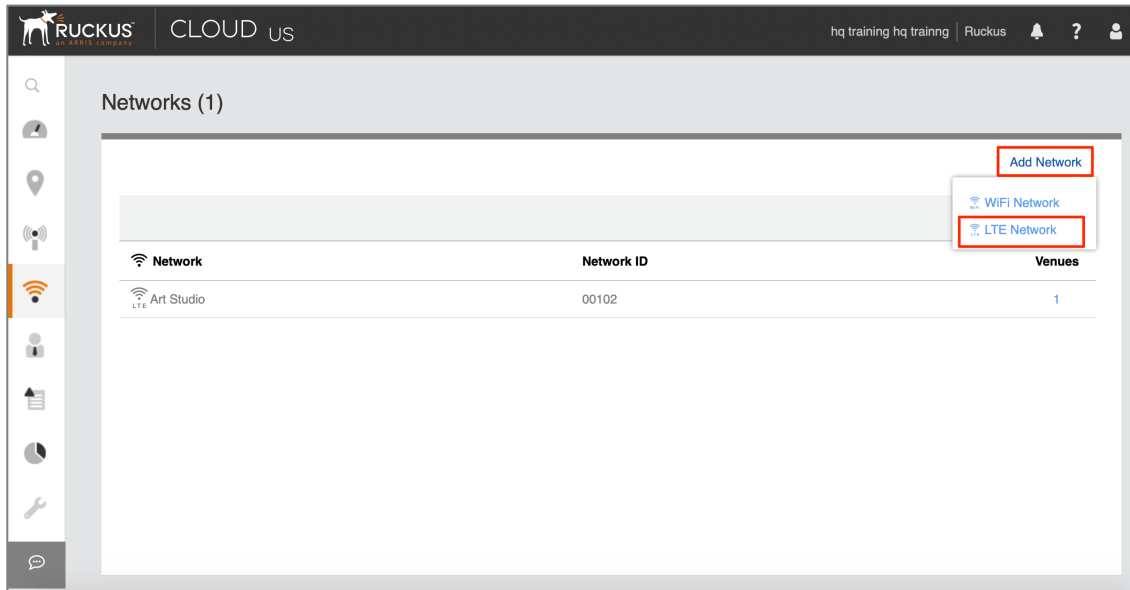


- After you click save, you now have a calibrated floorplan added to your venue.



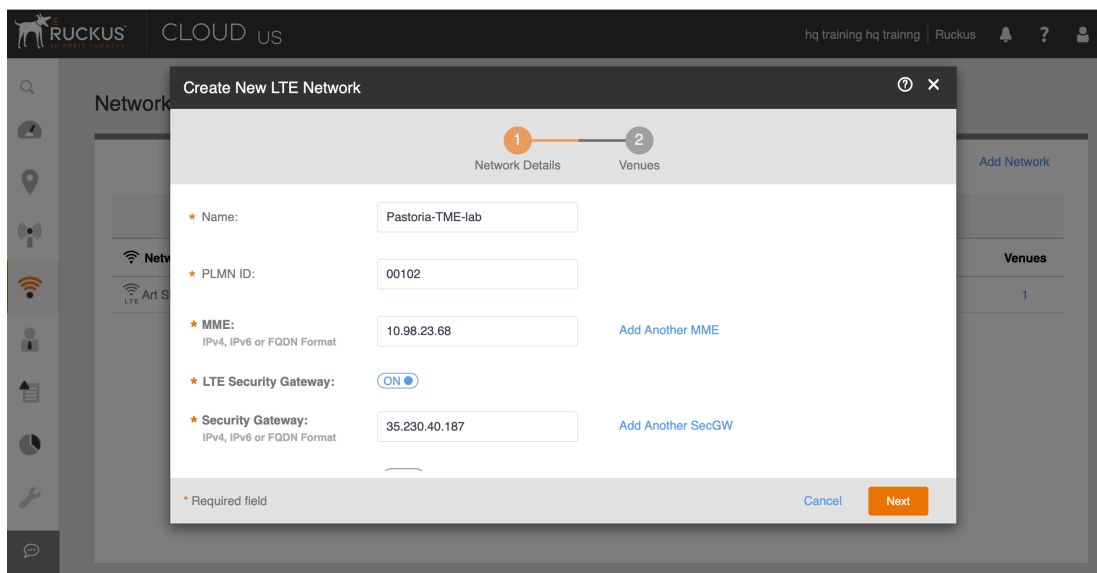
Adding an LTE Network

1. Click the “Add Network” button on the Networks page. Then click “LTE Network”.

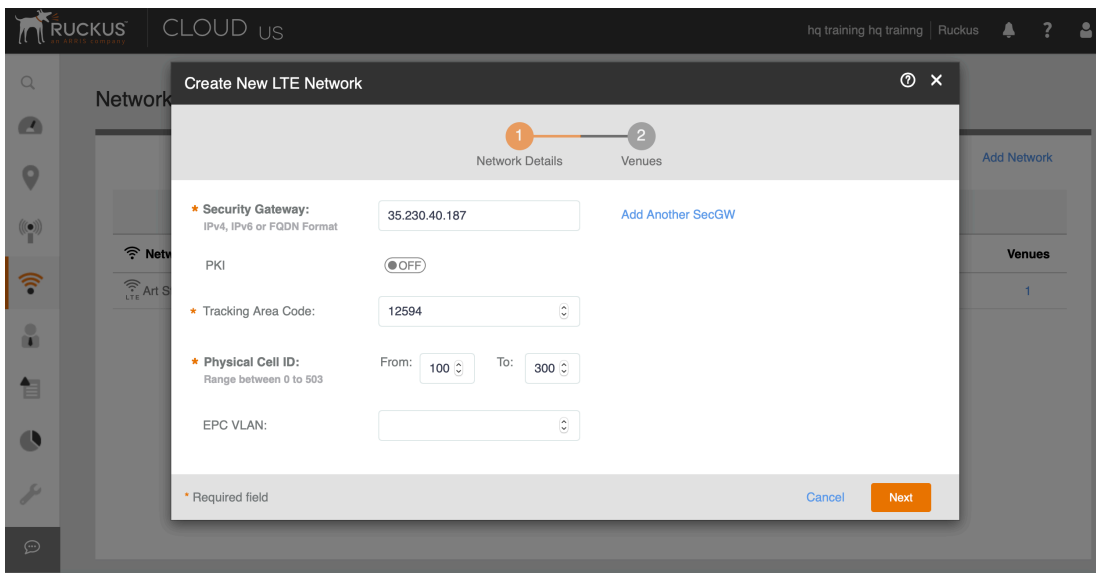


2. Enter the Network Details.

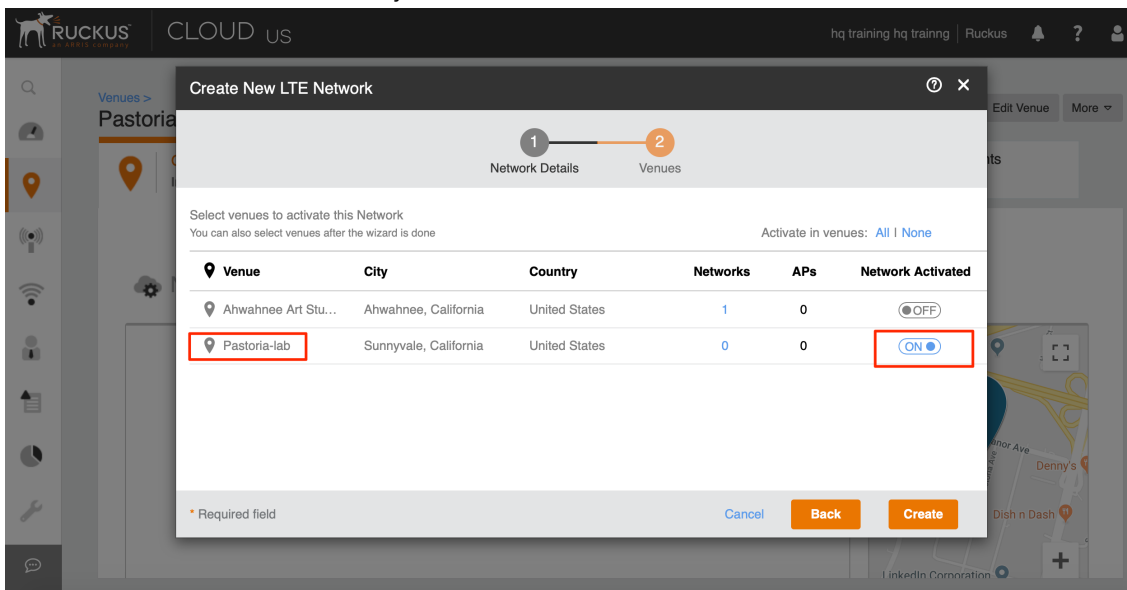
- a. A PLMN is identified by the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Each operator providing mobile services has its own unique PLMN ID. If you bought the Ruckus solution including the services bundle this info would be provided to you.
- b. The Mobility Management Entity (MME) is the key control-node for the LTE network access. It works with the LTE AP (eNodeB) and Servicing Gateway (SGW) within the Evolved Packet Core (EPC) and is responsible for initial paging and authentication of the mobile device. You can configure multiple MME control points.
- c. The Security Gateway (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.



- d. Public Key Infrastructure (PKI) - Provides the infrastructure for entities to establish trust relationships between each other based on their mutual trust of the Certificate Authority (CA). For this demo we have turned it OFF. In enterprise deployments it is recommended it to enable it for enhanced security.
- e. Tracking Area Code: Enter the unique Tracking Area Code (TAC) assigned to the LTE tracking area (TA) which helps in identifying the UE location. It is a standard LTE parameter and normally comes from the EPC vendor. *Note: For now, Ruckus is using a single TAC, but that may change in the future once we do neutral host.*
- f. Physical Cell ID - This is an LTE parameter (range is between 0-503). Normally EPC vendor selects the range and the SoN feature (Self organizing Network) will make sure each AP uses a different PCI number between neighbors.
- g. EPC VLAN - select default

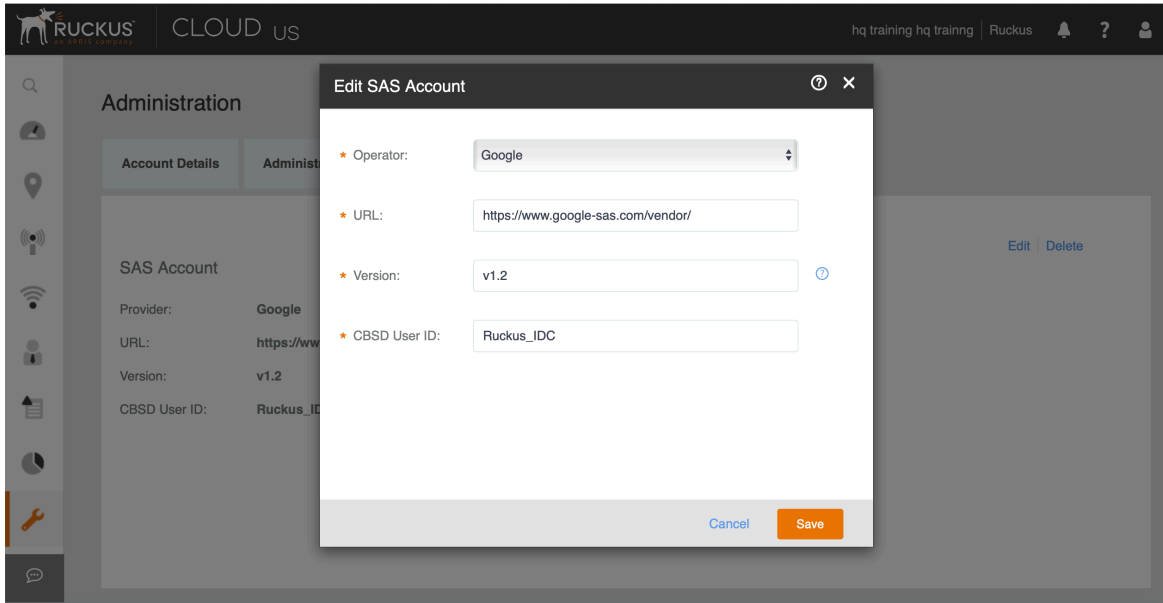


3. Turn the Network ON for the venue you created and click Create.



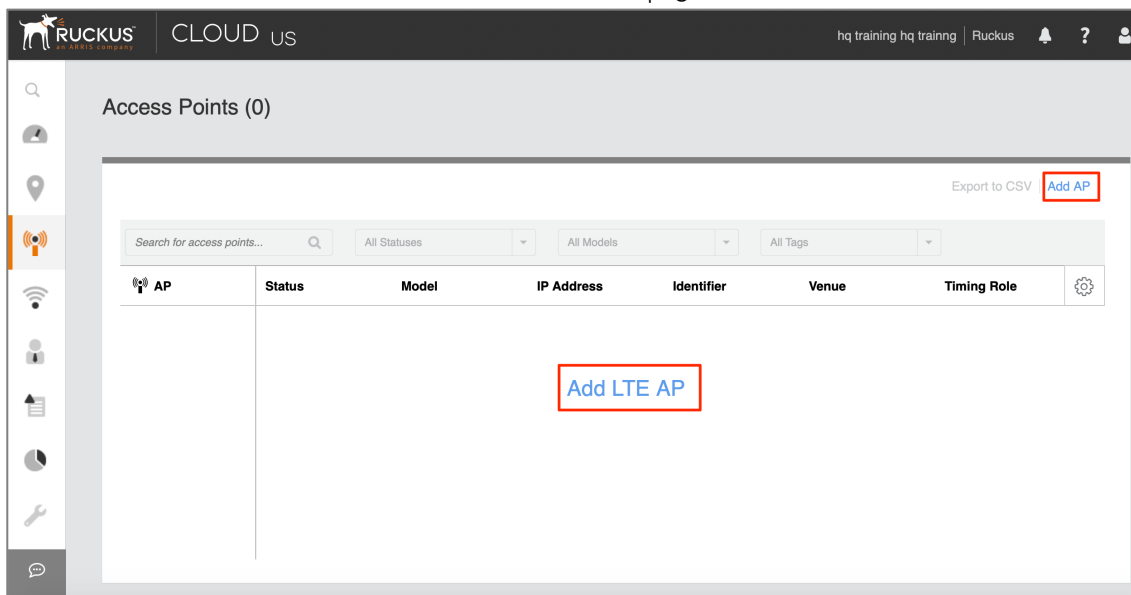
Configuring SAS

1. Go to Administration -> SAS Account to configure your SAS details.

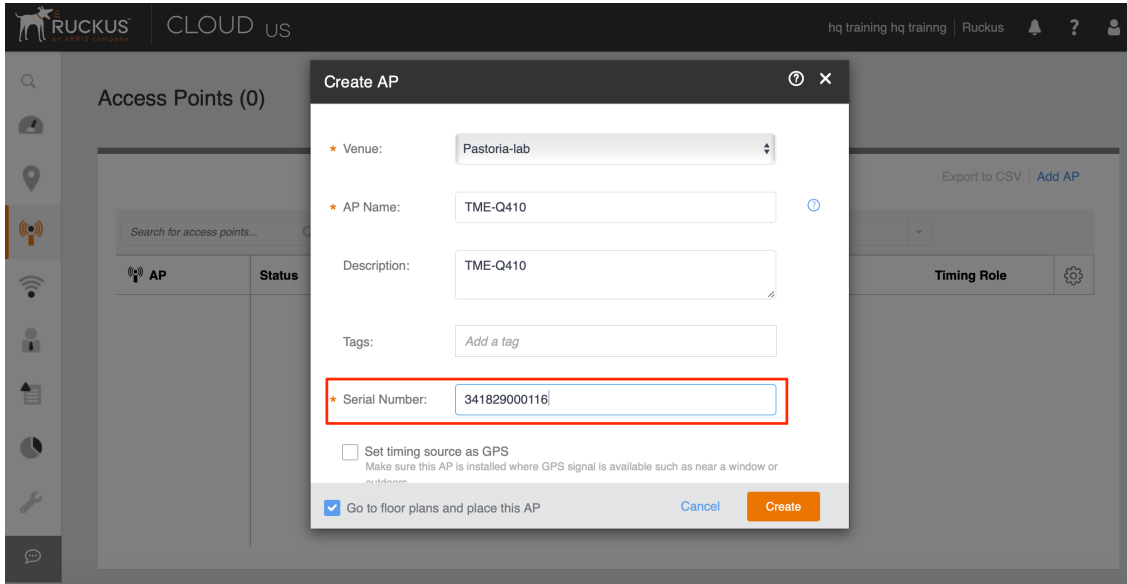


Adding LTE AP and verifying operation

1. Click either "Add LTE AP" or "Add AP" buttons on the APs page.



- Pick the Venue where you want this AP to be provisioned and give the AP a name. Enter the Serial Number from the back of the AP. When you enter the 5th digit of the serial number, it is recognized as an LTE AP and the options related to an LTE AP such as “Set timing source as GPS” appear.

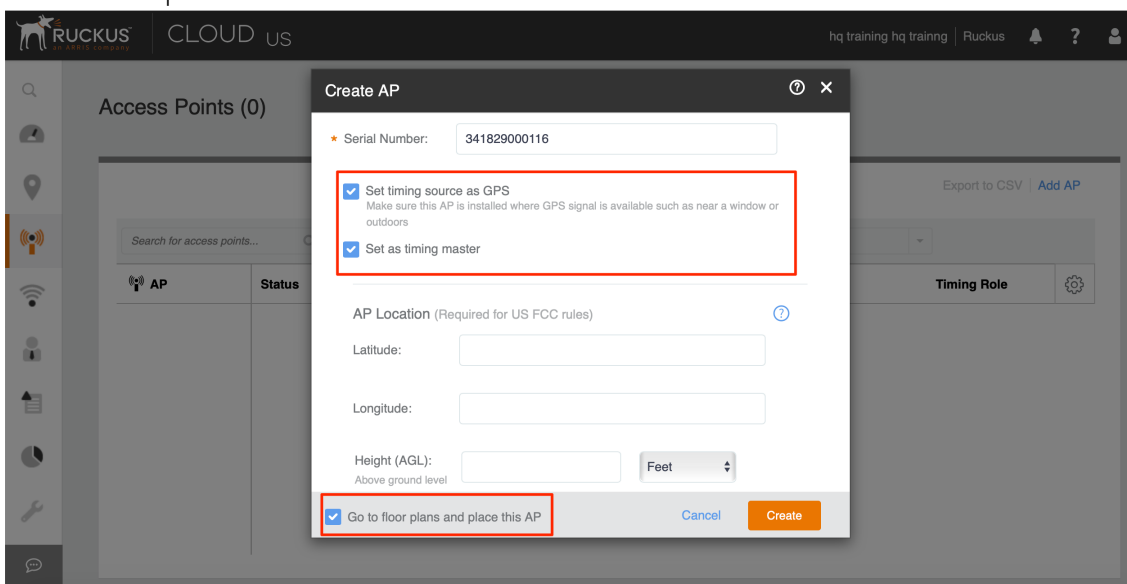


The screenshot shows the 'Create AP' dialog box in the Ruckus Cloud US interface. The 'Serial Number' field is highlighted with a red box and contains the value '341829000116'. Other fields include 'Venue: Pastoria-lab', 'AP Name: TME-Q410', and 'Description: TME-Q410'. There are checkboxes for 'Set timing source as GPS' and 'Go to floor plans and place this AP'.

- Check “Set timing source as GPS” and “Set as timing master”. This is for Precision Timing Protocol (PTP). Each AP comes with GPS, PTP and Voltage Control Temperature Compensated Crystal Oscillator (VCTCXO) to create accurate timing since CBRS is a time division duplex (TDD) system. Once you select GPS, the AP will try to lock on GPS signal for the timing. If the AP can lock on GPS, then it acts as a PTP Master to be the timing source for other APs in the venue. For the AP to obtain timing via GPS and/or function as Master timing source, please 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. This will enable the AP to sync with GPS Satellite vehicles and obtain timing and phase synchronization.

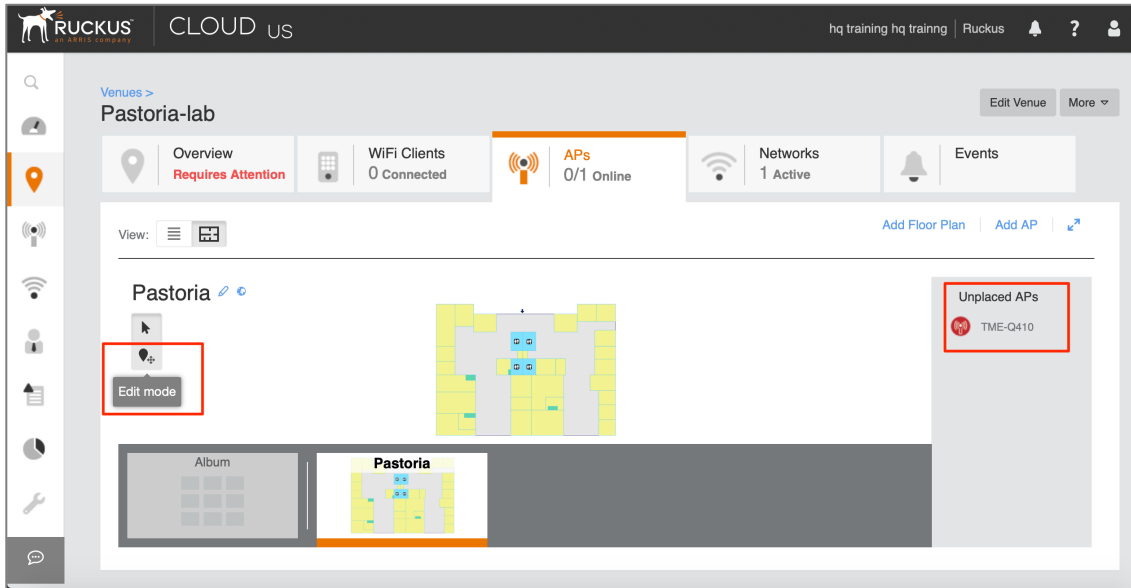
Note 1: In a planned future release, the timing process will be automated. The APs will turn the GPS on and select a PTP master automatically.

Note 2: There is no need to enter latitude, longitude, height if the floor plan has been calibrated. Keep the “Go to floor plans and place this AP” option checked and hit Create.

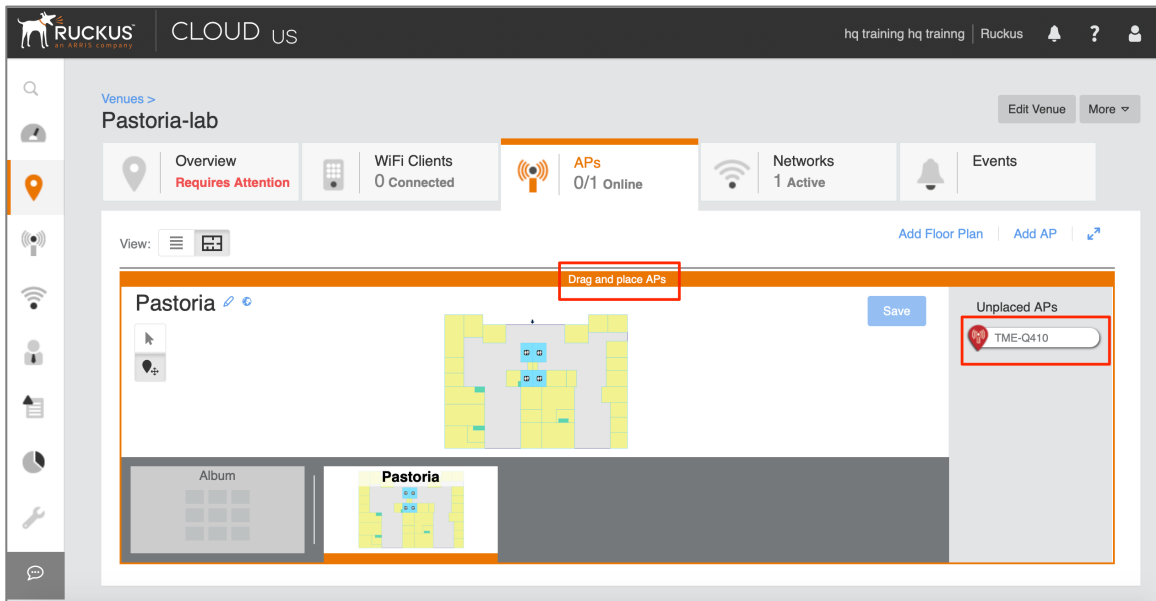


The screenshot shows the 'Create AP' dialog box in the Ruckus Cloud US interface. The 'Set timing source as GPS' and 'Set as timing master' checkboxes are highlighted with a red box. The 'Go to floor plans and place this AP' checkbox is also highlighted with a red box. The 'Serial Number' field contains '341829000116'.

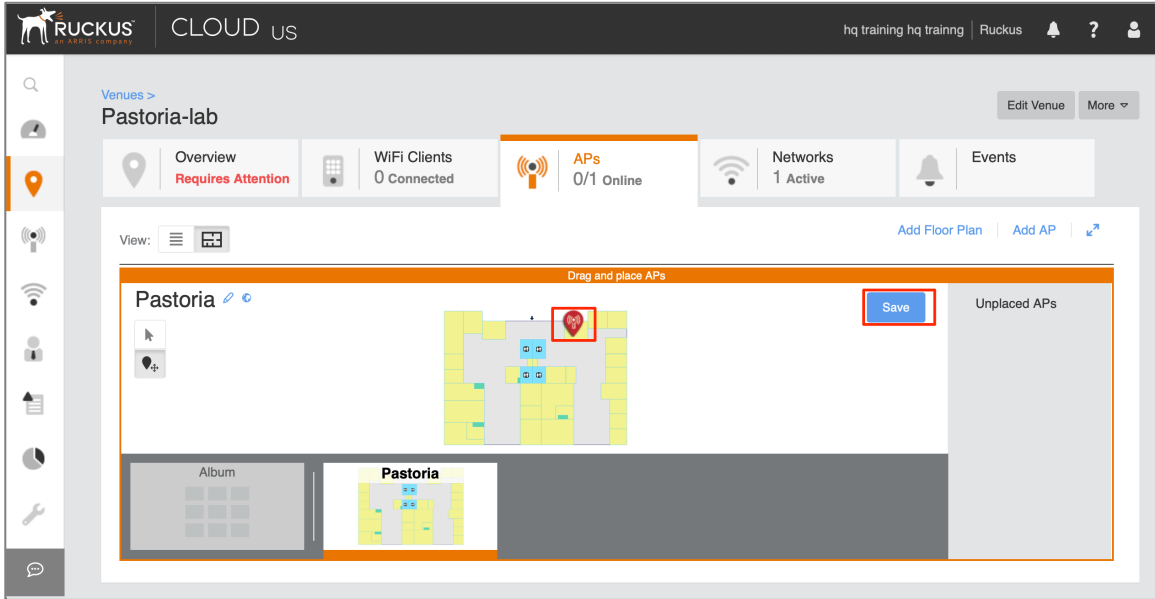
4. Click on the Edit mode pin (grey) to place the AP listed under the “Unplaced APs” onto the floor plan.



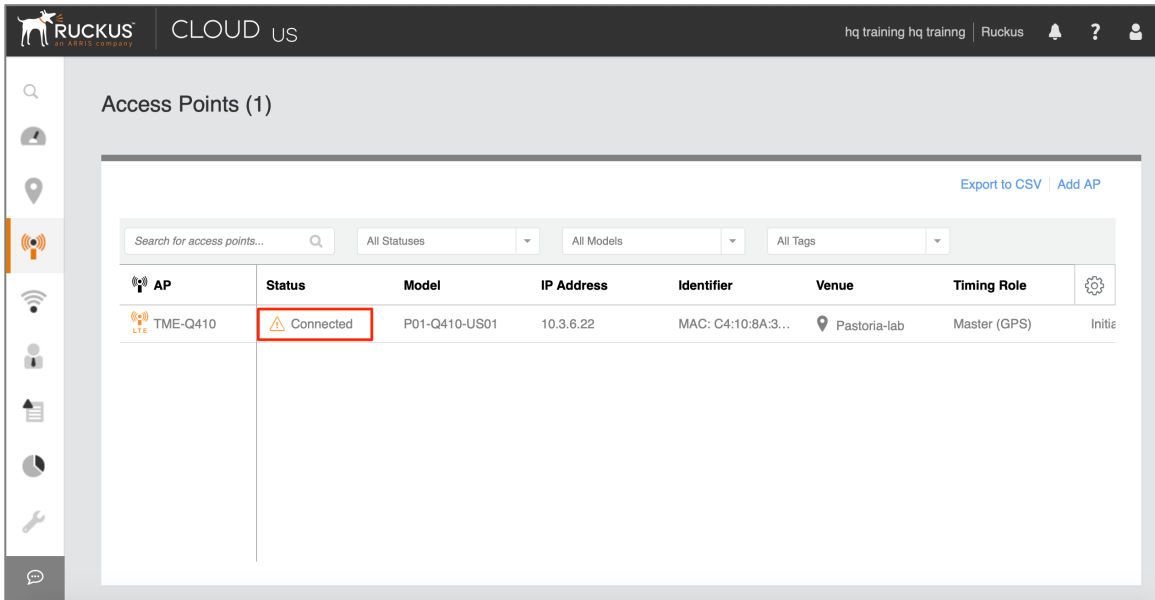
5. Once you hit the Edit mode, you will be able to drag and place this AP on the floor plan.



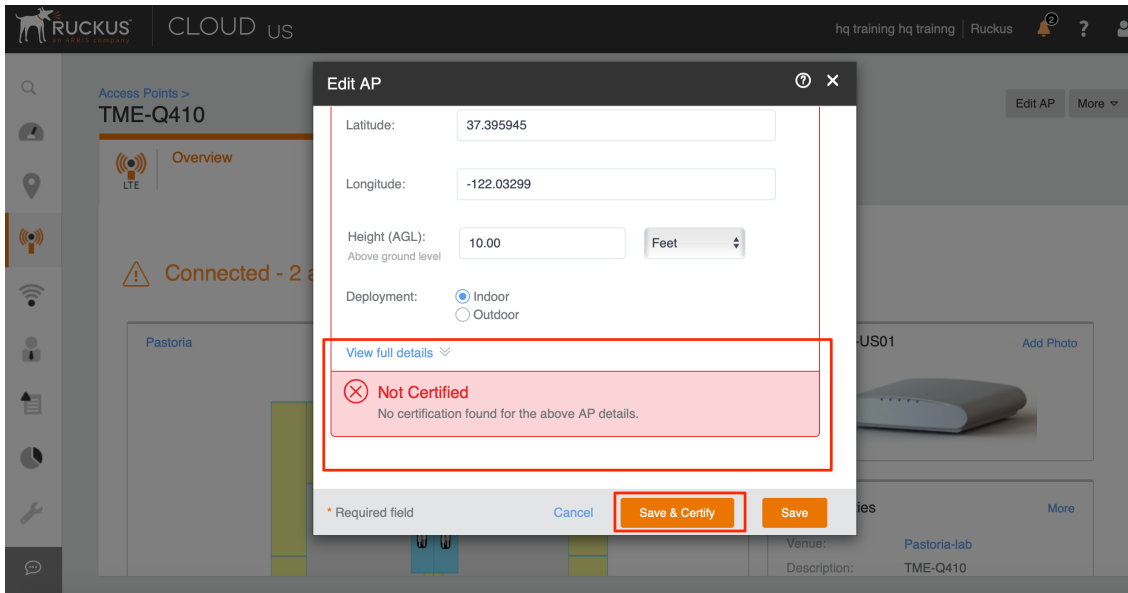
6. The AP is placed on the floor plan (red pin) and there are no more APs listed under "Unplaced APs". Click Save to continue.



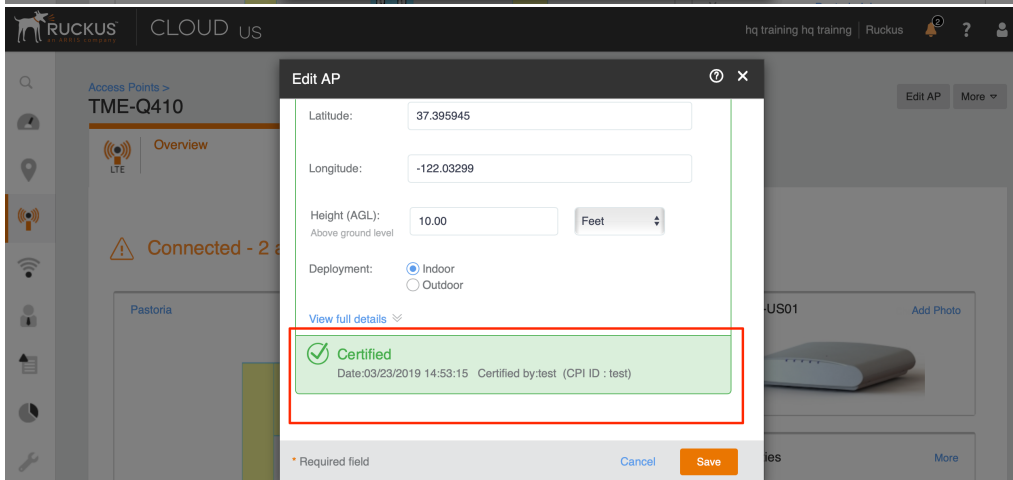
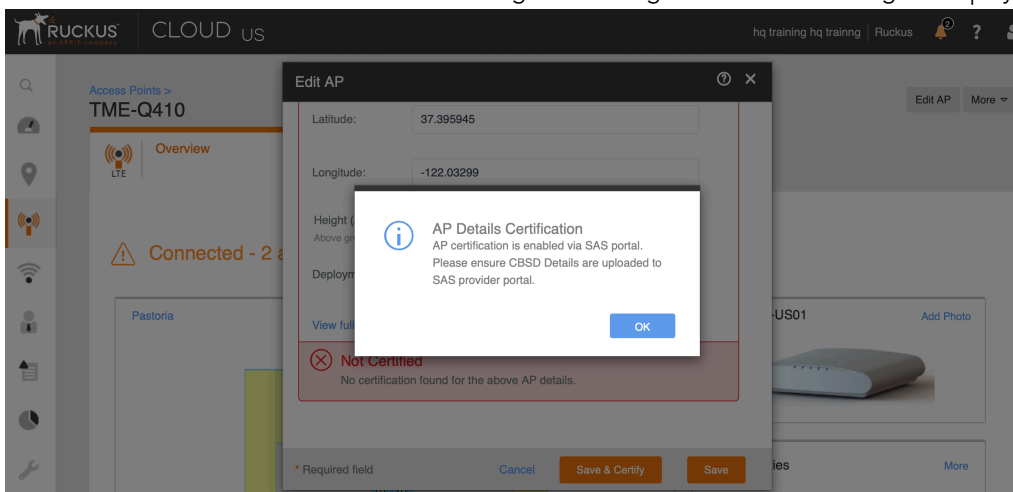
7. On the APs page, you now see your AP in "Connected" state after a few minutes of adding the AP.



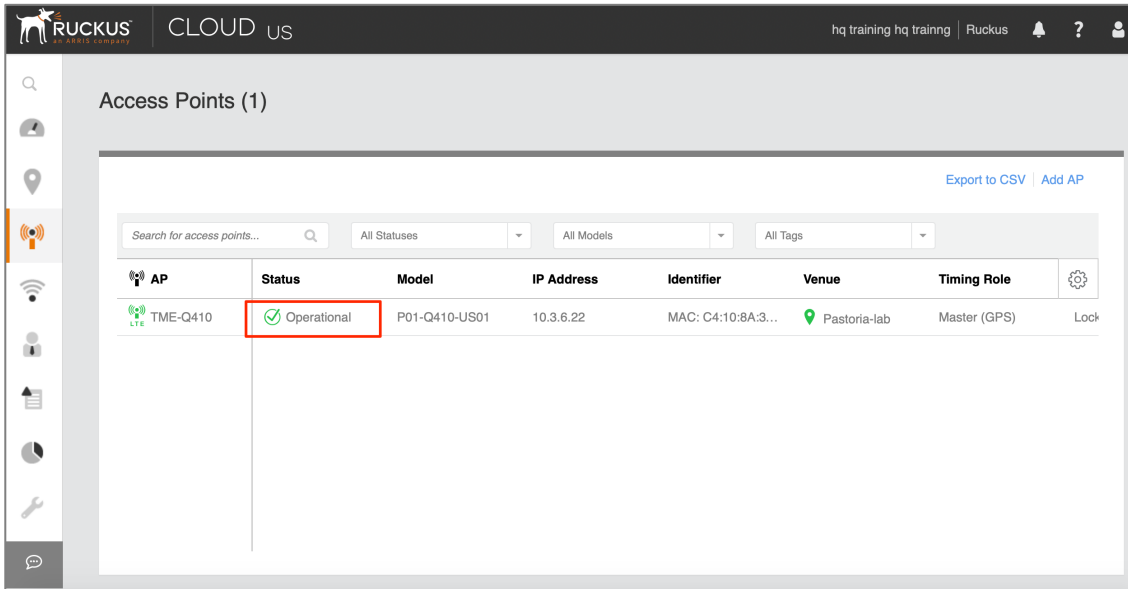
8. If you select the AP from the APs page and then click "Edit AP", a Not Certified message in red that is displayed. Click on the "Save & Certify" button above to continue. Please note this button appears after approximately 15 minutes.



9. Click OK on the AP Details Certification dialog box and a green Certified message is displayed. Click Save to continue.



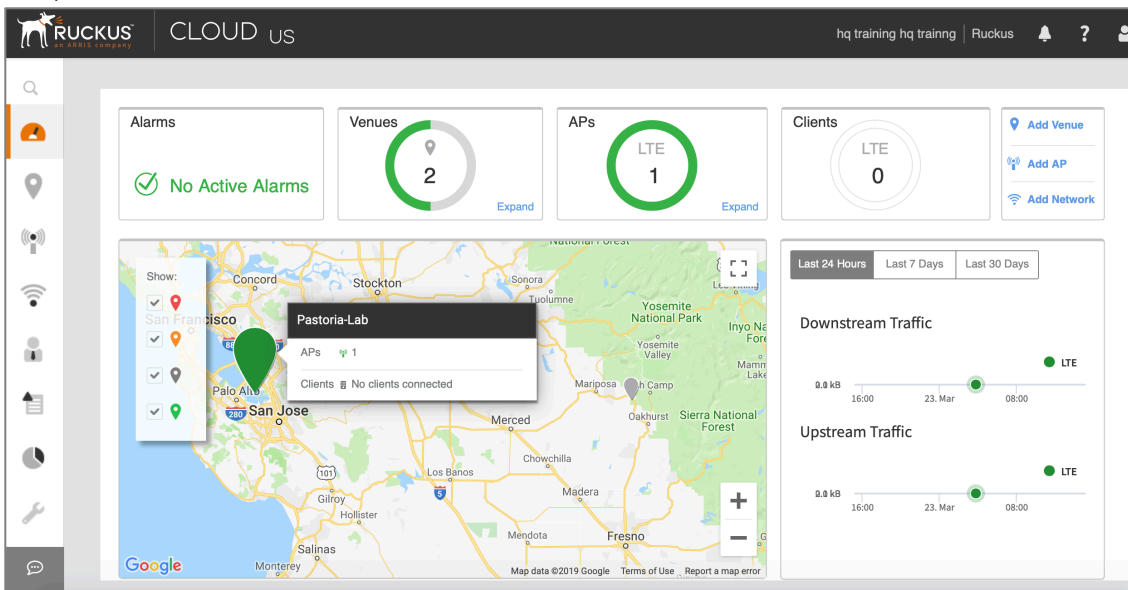
10. On the APs page you see that the status of the AP you added is "Operational" with a green check mark.



The screenshot shows the Ruckus Cloud US interface. The top navigation bar includes the Ruckus logo, 'CLOUD US', and user information. The main content area is titled 'Access Points (1)'. Below the title is a search bar and filter options for 'All Statuses', 'All Models', and 'All Tags'. A table displays the details of the added AP:

AP	Status	Model	IP Address	Identifier	Venue	Timing Role	
TME-Q410	Operational	P01-Q410-US01	10.3.6.22	MAC: C4:10:8A:3...	Pastoria-lab	Master (GPS)	Lock

11. On the dashboard you now see that the LTE AP is shown as a green circle indicating that it has been added successfully and its operation has been verified.



The screenshot shows the Ruckus Cloud US dashboard. The top navigation bar is the same as in the previous screenshot. The dashboard features several key metrics:

- Alarms:** No Active Alarms (indicated by a green checkmark).
- Venues:** 2 (indicated by a green circle with the number 2).
- APs:** 1 LTE (indicated by a green circle with the number 1).
- Clients:** 0 (indicated by a grey circle with the number 0).

Below the metrics is a map of the San Jose area with a green pin for 'Pastoria-Lab'. A pop-up window shows 'Pastoria-Lab' with 'APs: 1' and 'Clients: No clients connected'. To the right of the map are two line graphs for 'Downstream Traffic' and 'Upstream Traffic', both showing 0.0 kB of traffic over a 24-hour period on 23 Mar.

SIM Management Service (SMS)

As part of the LTE Network Services bundle, Ruckus provides a SIM Management Service (SMS). This includes SIM cards and a portal to manage them. Any clients that are intended to be used on the private LTE network must have SIMs provisioned on the backend by Ruckus through our vendor before shipping these SIMs out to the customer. Upon receipt of the SIMs, customers will have access to the SMS portal that allows them to activate, suspend, or change the device group of these SIMs. The following graphics illustrate the SIM management portal.

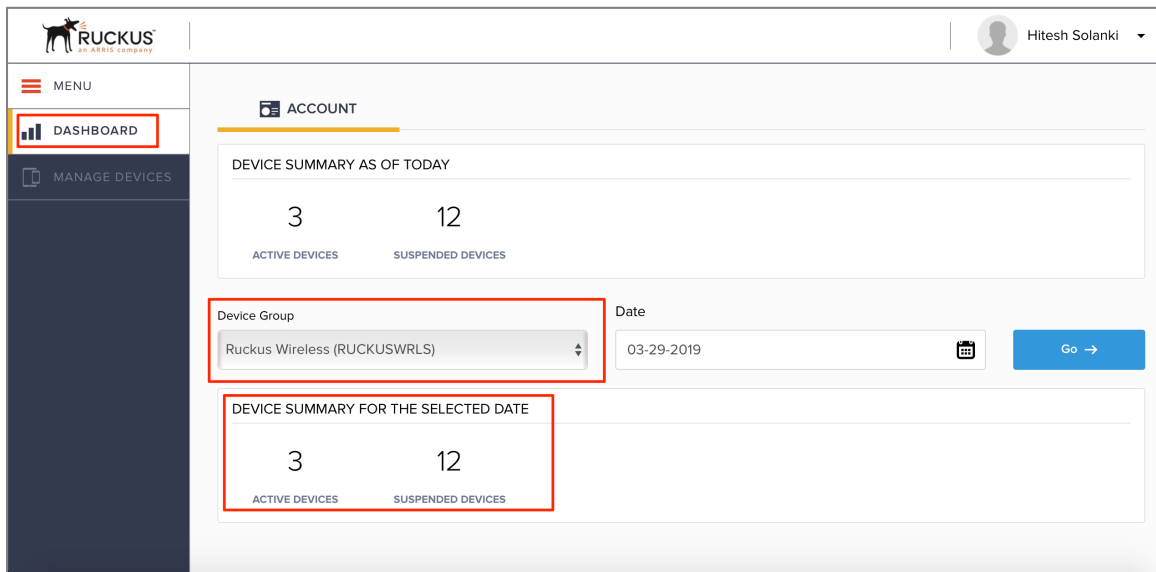


FIGURE 3: SIM MANAGEMENT PORTAL

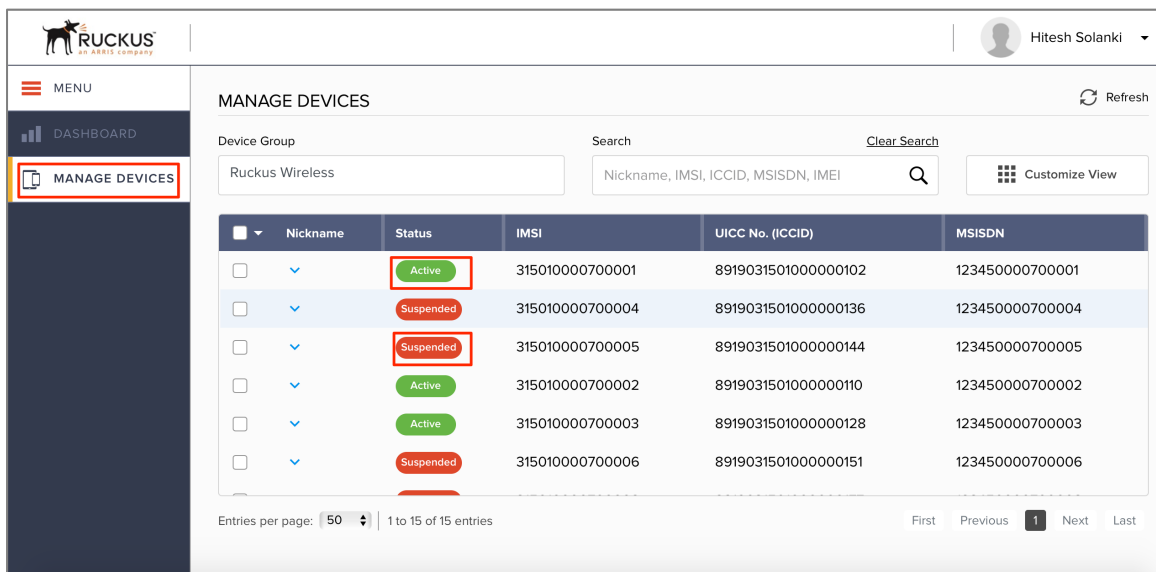
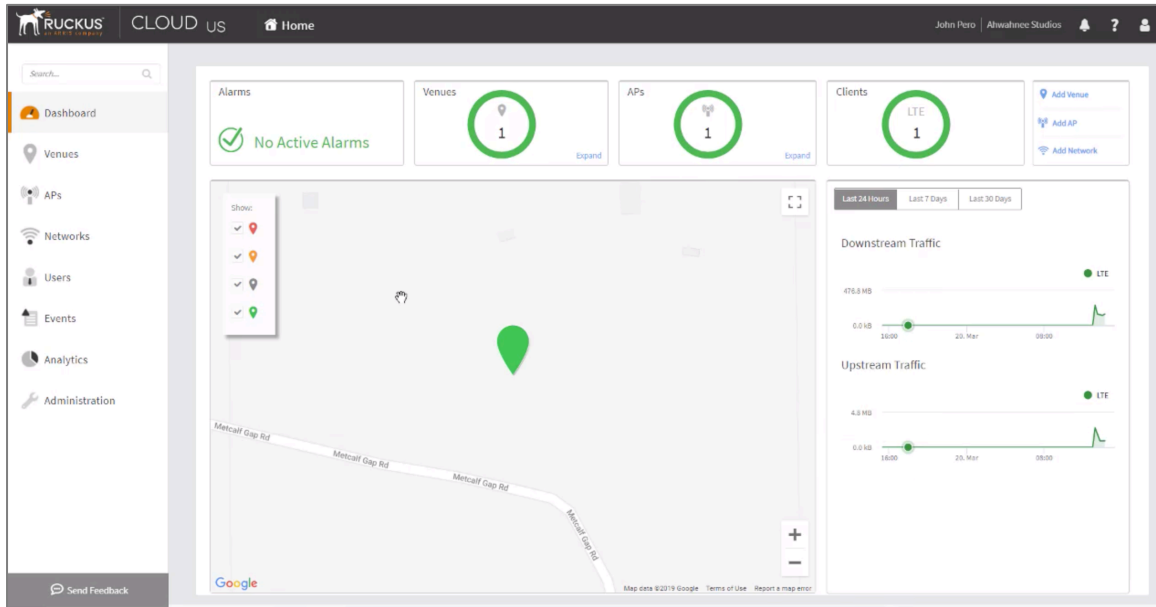


FIGURE 4: SIM MANAGEMENT PORTAL (2)

More details on the capabilities of the portal can be found in the SIM Management Service User Guide.

Once a client has a SIM that has been provisioned, it can join the LTE network that was previously configured. On the dashboard, you can see that the LTE Client is shown as a green circle, indicating that it has been associated successfully.



Summary

This document provides an introduction to Citizens Broadband Radio Service (CBRS) and Private LTE. The primary purpose of this guide is to describe recommended configurations for deploying Private LTE using the Ruckus CBRS solution. For more information on how to configure Ruckus products, please refer to the appropriate Ruckus user guide available on the Ruckus support site, <http://support.ruckuswireless.com>.

About Ruckus Networks

Ruckus Networks enables organizations of all sizes to deliver great connectivity experiences. Ruckus delivers secure access networks to delight users while easing the IT burden, affordably. Organizations turn to Ruckus to make their networks simpler to manage and to better meet their users' expectations. For more information, visit www.ruckuswireless.com.

Copyright © Ruckus, an ARRIS Company 2019. All rights reserved. The Ruckus, Ruckus Wireless, Ruckus logo, Big Dog design, BeamFlex, ChannelFly, Xclaim, ZoneFlex and OPENG trademarks are registered in the U.S. and other countries. Ruckus Networks, MediaFlex, FlexMaster, ZoneDirector, SpeedFlex, SmartCast, SmartCell, and Dynamic PSK are Ruckus trademarks worldwide. Other names and brands mentioned in this document or website may be claimed as the property of others. 17-6-A

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT, SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Ruckus Networks | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065 ruckuswireless.com

About ARRIS

ARRIS International plc (NASDAQ: ARRS) is powering a smart, connected world. The company's leading hardware, software and services transform the way that people and businesses stay informed, entertained and connected. For more information, visit www.arris.com.

For the latest ARRIS news:

Check out our blog: [ARRIS EVERYWHERE](#)

Follow us on Twitter: [@ARRIS](#)