USER GUIDE

RUCKUS Unleashed 200.14 User Guide

Supporting Release 200.14

Part Number: 800-73379-001 Rev B
Publication Date: June 2023

© 2023 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent marking notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions **9**
Contacting RUCKUS Customer Services and Support 9
What Support Do I Need? 9
Open a Case 9
Self-Service Resources 10
Document Feedback 10
RUCKUS Product Documentation Resources 10
Online Training Resources 10
Document Conventions 11
Notes, Cautions, and Safety Warnings 11
Command Syntax Conventions 11

About This Guide **13**
New in This Document 13

Introducing RUCKUS Unleashed **15**
Overview 15
Network Overview 15
Unleashed Dedicated Master Network Overview 16
Feature Parity with ZoneDirector 17
Limitations and Deviations from ZoneDirector 19
RUCKUS Unleashed-Only Features 19
Access Point Physical Features 19
C110 19
E510 24
H320 28
H350 33
H510 37
H550 42
M510 46
R320 54
R350 59
R510 63
R550 67
R610 72
R650 76
R710 80
R720 84
R750 89
R850 93
T310 Family 97
T350 Family 102
T350SE 106
T610 and T610s 111
T710 and T710s 115
T750 120
T750SE 124

Setting Up an Unleashed Wi-Fi Network **131**
Overview of the Setup Process 131
Step 1: Unpack and Install the Unleashed Master AP 132
Step 2: Configure Your Unleashed Network 132
Step 2a: Setup Using the Mobile App 132
Step 2b: Setup Using a Web Browser 137
Step 2c: Setup Using the Command Line Interface 154
Step 3: Customize Your Wireless LANs 158
Step 4: Deploy Additional Unleashed Member Access Points 161

Using the Admin Interface **163**
Unleashed Administration Interface Overview 163
Navigating the Dashboard 163
Using the Dashboard Components 164
Internet 164
Dedicated Master 164
WiFi Networks 165
Clients 166
Access Points 166
Switches 167
Admin & Services 168

Dedicated Master Configuration **169**
Dedicated Master Overview 169
Converting an Unleashed Master AP to Dedicated Master 169
Checking Whether the Current Active Master AP is an R750 or R850 169
Converting an Active Master AP to Dedicated Master 170
Joining a Member AP to the Dedicated Master Network 171
Joining a Member AP to Dedicated Master Using Option 43 (Recommended) 171
Placing a Member AP in the Same Network as Dedicated Master 172
Setting the Dedicated Master IP Address in the Member AP CLI 173
Dedicated Master AP or Member AP Behind NAT 174
Basic NAT Topologies 174
Configuration Requirements for Ports or IP Addresses for NAT Topologies 175
Checking Dedicated Master Status in the Unleashed Web Interface 175
Smart Redundancy Configuration 176
Smart Redundancy Setup Overview 176
Configuring Dedicated Master for Smart Redundancy 176
Checking the Standby Dedicated Master 184
Disabling Smart Redundancy 185

WLAN Configuration **189**
WLAN Configuration Overview 189
WLAN Usage Types 191
Creating a New WLAN 192
802.1X EAP WLANs 195
802.1X WLAN Survivability 195
Guest WLANs 198
Deploying a Guest WLAN 198
Hotspot WLANs 263
Configuring Global WLAN Settings 264
Editing an Existing WLAN 265

Using a QR Code to Join a Wi-Fi Network ... 266
Deleting a WLAN ... 267
Disabling a WLAN Temporarily ... 268

Advanced WLAN Configuration ... 269
Advanced WLAN Configuration Overview ... 269
Configuring Advanced WLAN Options ... 269
Zero-IT and DPSK Settings ... 271
Zero-IT ... 271
Dynamic PSK ... 272
Enabling Zero-IT for a WLAN ... 273
Enabling DPSK for a WLAN ... 273
WLAN Priority Settings ... 278
Access Control Settings ... 279
Application Policies ... 281
Creating an Application Control Policy ... 281
Radio Control Settings ... 284
Creating Separate WLANs for 2.4 GHz and 5 GHz Radios ... 285
Other Advanced WLAN Settings ... 286
Configuring Client Isolation Allowlists ... 288
Bypass Apple CNA ... 289

Access Point Configuration ... 291
Access Points Configuration Overview ... 291
Show Mesh Topology ... 293
Show Client Info ... 294
Show Events and Alarms ... 296
Configuring Global AP Settings ... 297
Radio (2.4G) ... 297
Radio (5G) ... 298
Other ... 299
Monitoring an Individual AP ... 303
Show Client Info ... 304
Show WLANs Info ... 305
Show AP Info ... 306
Show Events and Alarms ... 309
Client Status and Traffic Graphs ... 310
Configuring an Individual AP ... 310
Renaming an AP ... 313
Working with AP Groups ... 314
Viewing AP Group Members ... 315
Modifying the System Default AP Group ... 316
Creating a New AP Group ... 320
Modifying Model Specific Controls ... 322
Configuring AP Ethernet Ports ... 324
Restarting an AP ... 330
Removing an AP ... 331

ICX Switch Management ... 333
ICX Switch Management Overview ... 333
Requirements ... 333
Preparing an ICX Switch for Unleashed Management ... 334

Approving a New Switch to Join Unleashed....337
Monitoring Connected ICX Switches....340
Accessing the RUCKUS Switch Home Page....342
Managing Switch Ports....342
Backup and Restore Switch Configuration....345
Upgrading ICX Switch Firmware....348

Working with Clients....351
Client Management Overview....351
Viewing the Clients List....351
Renaming a Client....353
Deleting a Client....355
Permanently Blocking a Client Device....355
Marking a Client as a Favorite....356
Running a SpeedFlex Performance Test on a Wireless Client....357
Client Connection Troubleshooting....361
Marking a Client as a Legacy Device....363
Adding User Accounts to the Internal User Database....363
Authenticating Clients Using an External Database....364

Configuring Admin & Services Settings....365
Admin & Services Overview....365
System Settings....365
System Info Settings....366
IP Settings....375
Configuring the System Time....388
Setting the Country Code....390
Configuring User Roles....392
Adding New Users to the Local Database....393
Changing an Existing User Account....395
Importing Users into the Local Database using CSV File....396
Deleting a User Record....397
Changing User Password....398
Mesh Networking....399
Enabling Log Delivery to Remote Syslog Server....408
Services....409
AAA Servers....410
Access Control....415
Application Recognition and Control....419
Bonjour Gateway....425
Dynamic PSK....428
Guest Access Services....435
Hotspot Services....436
Radio Control....439
WIPS....447
URL Filtering....452
Wi-Fi Calling....458
Tunnel Configuration....461
Administration Settings....461
Preferences....462
Backup and Restore....463

Upgrade....466
Diagnostics....474
Working with SSL Certificates....483
Testing Network Connectivity....490
Network Management....491
Enabling Mobile App Remote Management....496
Technical Support....498

Unleashed Access Point Power Supply Considerations....501
AP Power Warnings....501
Power Limitations by PoE Mode and AP Model....503
R850....503
R750....503
R720....503
R710....504
R650....504
R610....504
R550....504
H550....505
T610....505
M510....505
T750....505
T750SE....506
T350c....506
T350d....506
T350SE....507

Contact Information, Resources, and Conventions

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

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.ruckusnetworks.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://community.ruckuswireless.com
- 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.

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.ruckusnetworks.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://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

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

TABLE 1 Text Conventions

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

Notes, Cautions, and Safety Warnings

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

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

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

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

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

Command Syntax Conventions

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

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

About This Guide

- New in This Document..... 13

New in This Document

TABLE 2 Summary of Changes in Unleashed 200.14 (Rev B), June 2023

Feature	Description	Reference
Addressing reported defects	**Updated**: Updating the CLI command.	Setting the Dedicated Master IP Address in the Member AP CLI on page 173

Introducing RUCKUS Unleashed

- Overview 15
- Network Overview 15
- Feature Parity with ZoneDirector 17
- Limitations and Deviations from ZoneDirector 19
- RUCKUS Unleashed-Only Features 19
- Access Point Physical Features 19

Overview

RUCKUS Unleashed is custom designed to help small business owners grow their businesses, deliver an excellent customer experience and manage costs while supporting enterprise-class Wi-Fi and highly customizable control of mobile devices with minimal IT staff.

RUCKUS Unleashed provides a controllerless option for small to medium-sized Wi-Fi deployments where up to 128 access points can be deployed in a self-healing, redundant wireless network with no controller required, while still providing many of the enterprise-class features that traditionally required a RUCKUS WLAN controller (for example, ZoneDirector or SmartZone controller). Beginning with Unleashed 200.13, Dedicated Master is introduced as a replacement for ZoneDirector 1200, which provides controller functionalities such as Smart Redundancy, tunnel WLAN, cross-network segment networking, and so on.

RUCKUS Unleashed access points (APs) have built-in controller capabilities including user access controls, guest networking features, advanced Wi-Fi security and traffic management. As businesses grow to multiple sites or larger scale deployments, RUCKUS offers an easy migration path to cloud-based or controller-based Wi-Fi, using the same RUCKUS access points.

RUCKUS Unleashed provides small to medium-sized business environments with superior performance, lower costs, and simplified management. Separate controller support contracts and access point licenses are not needed, significantly reducing upfront and recurring costs, and the simplified web interface also makes deploying RUCKUS Unleashed easy.

The RUCKUS Unleashed platform offers many of the features that previously required a controller, and without having to sacrifice many features that previously required a controller, such as Zero-IT, Dynamic PSK (DPSK), Smart Mesh, ChannelFly, Application Recognition and Control (ARC), Bonjour Gateway, Bonjour Fencing, and one-step firmware upgrades of the entire network from a single interface.

Network Overview

A RUCKUS Unleashed network consists of a RUCKUS Unleashed "Master AP" and a number of RUCKUS Unleashed member APs (up to 128 total).

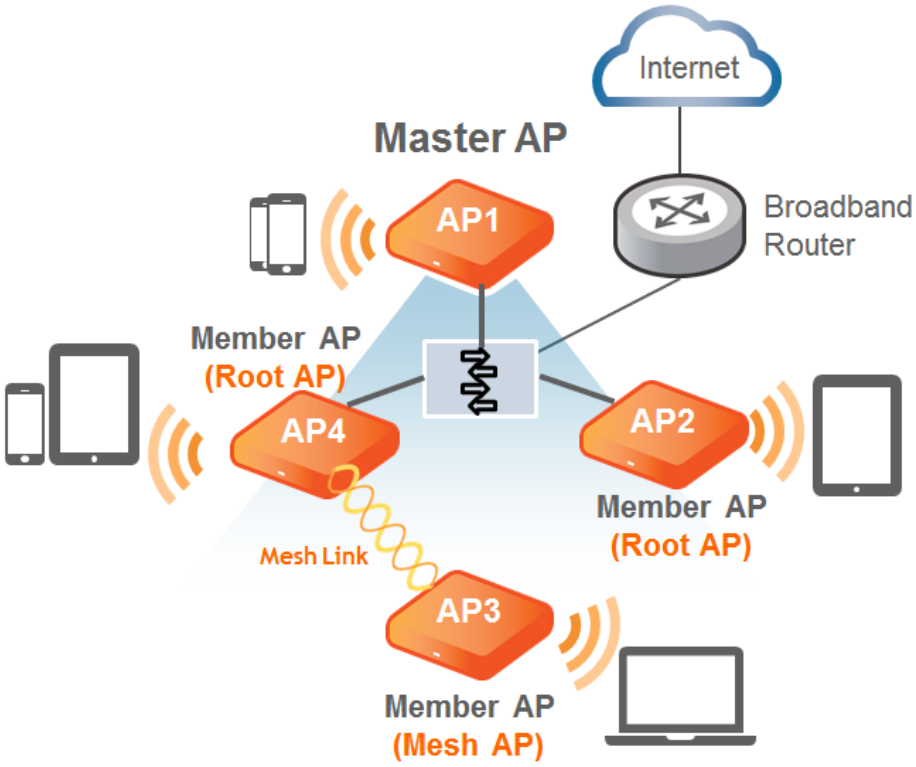
> **NOTE**
> Beginning with release 200.8, the maximum capacity limit has been increased from 50 APs and 1,024 clients to 128 APs and 2,048 clients per RUCKUS Unleashed network in bridge mode (gateway mode supports up to 25 APs and 512 clients).

In addition to serving Wi-Fi clients like a standard AP, the Master AP also performs the same functions as a controller; all control functions are performed through the Master AP and pushed to the other APs on the network.

A RUCKUS Unleashed member AP joins a Master AP in the same subnet automatically. RUCKUS Unleashed member APs do not attempt to join a ZoneDirector or SmartZone controller on the network. If the Master AP is offline, one of the member APs assumes the role of RUCKUS Unleashed Master and takes over control of the RUCKUS Unleashed network.

The following figure illustrates the basic components of a RUCKUS Unleashed network.

FIGURE 1 Basic Unleashed Network Topology



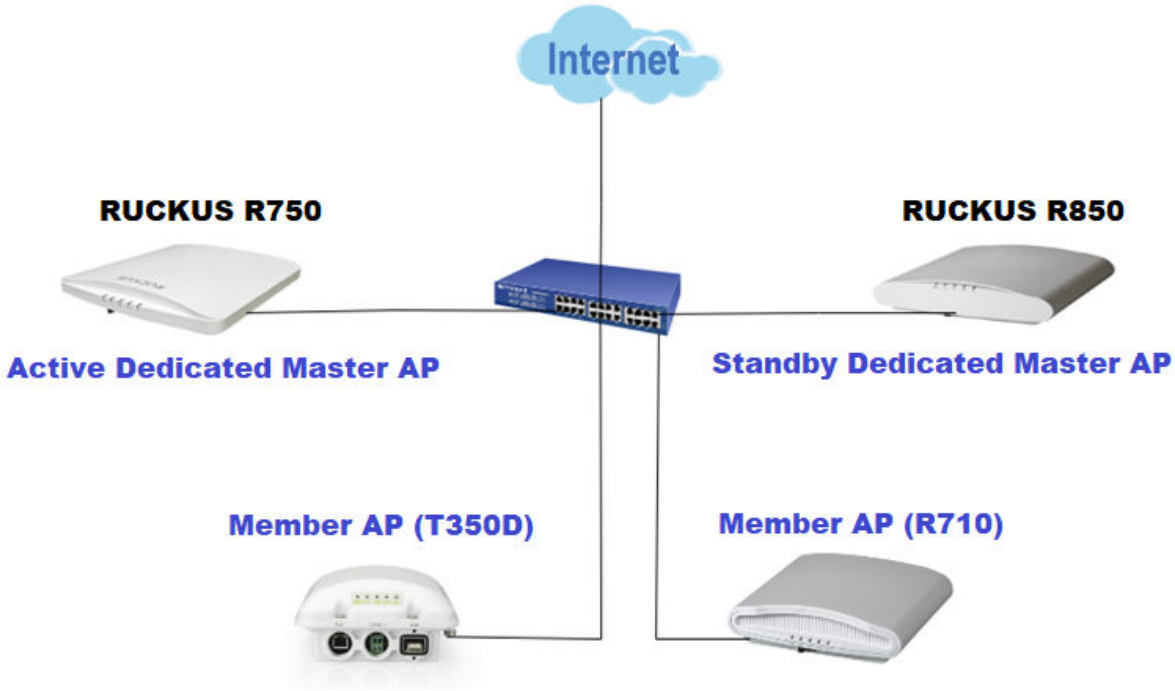
Unleashed Dedicated Master Network Overview

A RUCKUS Unleashed Dedicated Master network consists of two Dedicated Master APs, R750 and R850, and a number of Unleashed member APs (up to 128 total).

When Unleashed is switched to Dedicated Master mode, a maximum capacity limit of 4,000 clients is supported. The maximum DPSK number and Guest key is increased from 2,048 through 4,000. The maximum station cache number that is used for recording a client's fingerprinting data is enhanced from 4,096 through 8,000.

The following figure illustrates the basic components of an Unleashed Dedicated Master network.

FIGURE 2 Basic Unleashed Dedicated Master Network Topology



To configure a Dedicated Master AP, refer to Dedicated Master Configuration on page 169.

Feature Parity with ZoneDirector

The RUCKUS Unleashed platform provides many of the same features that are currently available using a ZoneDirector wireless LAN controller:

- Smart Mesh
- One-step firmware upgrades of the entire network from a single interface
- Layer 2 roaming
- Layer 3 discovery support
- Zero-IT support for automatic client Wi-Fi configuration
- Dynamic Pre-Shared Keys (DPSK)
- Guest WLANs
- WLAN types:
  - Captive Portal (Web Auth)
  - Hotspot (WISPr)
  - Guest Access (Guest Pass)
  - Social Media (Facebook, LinkedIn, Microsoft, Google, WeChat)
- 802.1X EAP authentication using an external AAA server (RADIUS)
- Bonjour Gateway
- WLAN encryption and authentication options:
  - Open + None

  - Open + None + MAC Auth
  - Open + None + Web Auth
  - Open + WPA2 + AES + PSK
  - Open + WPA2 + AES + DPSK
  - 802.1X + WPA2 + AES + AAA
  - 802.1X + WPA3 + SAE + AAA
  - Open + WPA3 + SAE
  - Open + WPA2/WPA3-Mixed + SAE + AES
  - Open + OWE
- Radio Frequency (RF) management features:
  - BeamFlex
  - ChannelFly
  - Background Scanning
  - Automatic Channel Selection based on ChannelFly or Background Scanning
  - SpeedFlex
  - Rogue AP detection
- Client management features:
  - Access Control Lists
  - Application Recognition and Control (ARC)
  - HTTP/HTTPs Redirect
  - Up to 1,024 local users supported (on the internal database)
  - Up to 1,024 client devices supported (depending on encryption and authentication method)
  - Self-Service Guest Pass
  - Client Load Balancing
  - Band Steering
  - Client Isolation
  - Client Fingerprinting
  - Device Access Policies
- DHCP server (configured manually from Network Master AP)
- SNMP Management
- Syslog Delivery to External Syslog Server
- Management IP Interface
- Multi-Language support
- WLAN Prioritization
- Dynamic VLANs
- Enable or Disable WLANs on a per-radio basis
- AP Groups
- Tunnel configuration support for Dedicated Master
- Smart Redundancy ability
- AP VLAN support

Limitations and Deviations from ZoneDirector

While many ZoneDirector features are included, RUCKUS Unleashed does not provide the entire ZoneDirector feature set.

The following features are either not supported, supported but with limitations, or are currently unsupported but planned for a future release:

- IPv6 is not supported.
- No interface to communicate with SmartCell Insight analytics engine or SPoT location services.
- No Northbound Interface to pass client authentication responsibility to an external entity.
- No WLAN groups.

RUCKUS Unleashed-Only Features

The following features are unique to the RUCKUS Unleashed platform and do not correspond to any existing ZoneDirector or other RUCKUS controller features:

- The RUCKUS Unleashed platform does not require an external controller - all controller functions are performed through a single "Master AP" web interface. The Master AP serves the same functions as a ZoneDirector controller would perform on the network; that is, all control functions are performed through the controller and pushed to the other APs on the network.
- A Member AP automatically takes over all AP control functions if the Master AP is offline.
- Preferred Master: Administrators can configure an AP to serve as the "preferred" Master AP. If the preferred Master is offline, another member AP will become the Master. When the preferred Master comes back online, it will resume the RUCKUS Unleashed Master role.
- Dedicated Master: You can enable Dedicated Master mode only when the Master AP is an R750 AP or R850 AP. Specify one Dedicated Master AP as the primary and the other Dedicated Master AP as the secondary to act as the active and standby Dedicated Masters.
- The user interface provides simplified and more intuitive controls for some controller functions, and hides or removes some of the less-used options for easier navigation and configuration.
- Gateway Mode: The Master AP can be configured as a gateway router, performing all NAT and DHCP functions as well as serving as the RUCKUS Unleashed network controller and serving wireless clients.

  NOTE
  When gateway mode is enabled, RUCKUS Unleashed supports a maximum 25 APs and 512 concurrent clients due to the additional resource demands placed on the Master AP when in gateway mode.

- ICX Switch Management: RUCKUS Unleashed provides a user interface for monitoring and managing RUCKUS ICX switches and ICX switch stacks.

Access Point Physical Features

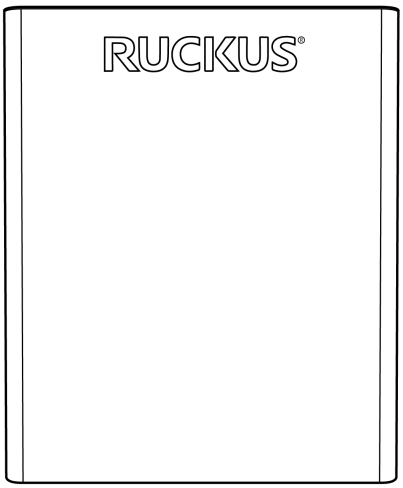
This section describes the physical features of the RUCKUS Unleashed Access Points currently available.

C110

The Unleashed C110 is an 802.11ac Wave 2 dual-band concurrent Wi-Fi Wall Switch AP with integrated 4-port gigabit Ethernet and Cable Modem backhaul in a form factor designed for mounting to electrical outlet boxes.

This section describes the physical features of the RUCKUS Unleashed C110 802.11ac Cable Modem Access Point.

FIGURE 3 C110 Access Point



Rear Panel

The C110 AP features five LEDs on its rear panel. (LEDs are concealed when mounted.)

TABLE 3 Front Panel LEDs

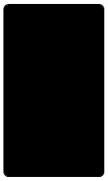
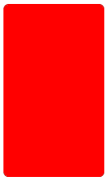
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 3 Front Panel LEDs (continued)

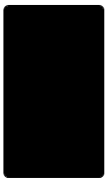
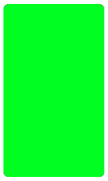
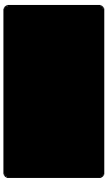
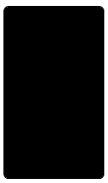
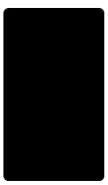
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 3 Front Panel LEDs (continued)

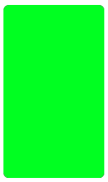
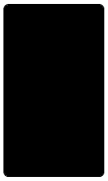
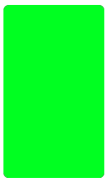
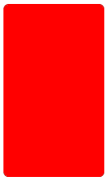
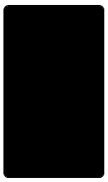
LED	Status	Description
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.

TABLE 3 Front Panel LEDs (continued)

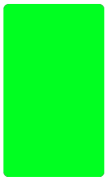
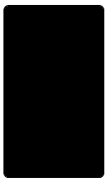
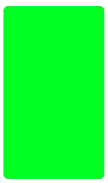
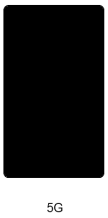
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 3 Front Panel LEDs (continued)

LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

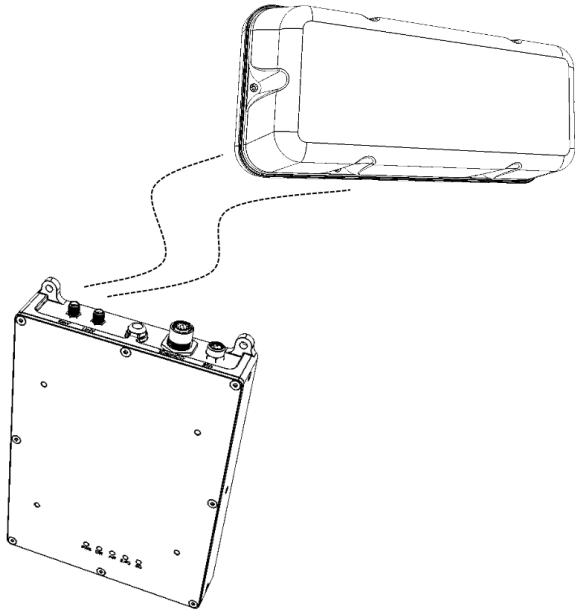
E510

The Unleashed E510 is a modular access point designed for deployment in scenarios with specific form factor needs such as outdoor lighting, railway, street furniture, and sports and entertainment venues.

The E510 addresses the need for a modular AP where specific deployment situations preclude the antenna structure and onboard intelligence being installed as a single module.

This section describes the physical features of the RUCKUS Unleashed E510 802.11ac Wave 2 Access Point.

FIGURE 4 E510 Access Point



Front Panel

The E510 AP features five LEDs on its front panel.

TABLE 4 Front Panel LEDs

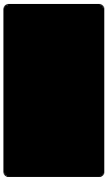
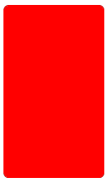
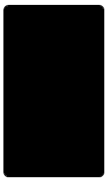
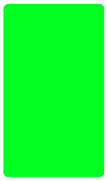
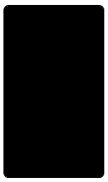
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.

TABLE 4 Front Panel LEDs (continued)

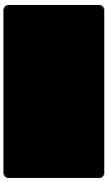
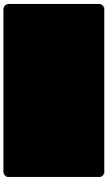
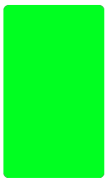
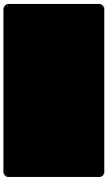
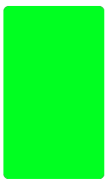
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 4 Front Panel LEDs (continued)

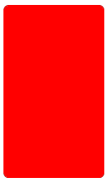
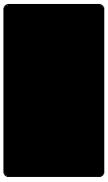
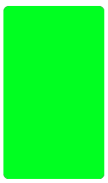
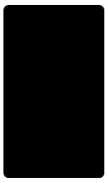
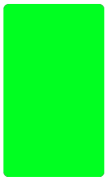
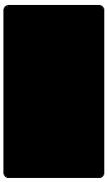
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 4 Front Panel LEDs (continued)

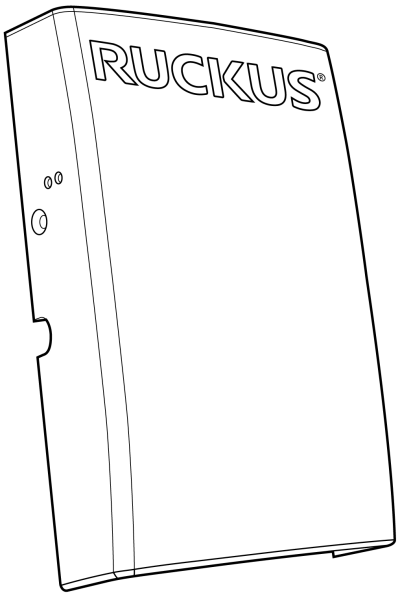
LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

H320

The H320 is an 802.11ac Wave 2 dual-band concurrent Wi-Fi Wall Switch AP with one Gigabit uplink port and two 10/100 access ports, in a form factor designed for mounting to electrical outlet boxes.

This section describes the physical features of the RUCKUS Unleashed H320 802.11ac Access Point.

FIGURE 5 H320 Access Point



Rear Panel

The H320 AP features five LEDs on its rear panel. (LEDs are concealed when mounted.)

TABLE 5 Front Panel LEDs

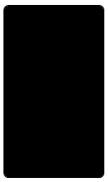
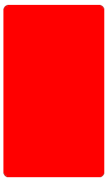
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 5 Front Panel LEDs (continued)

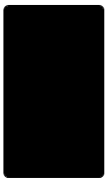
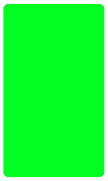
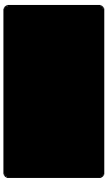
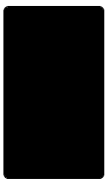
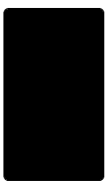
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 5 Front Panel LEDs (continued)

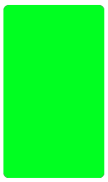
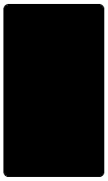
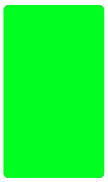
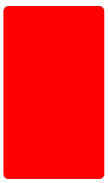
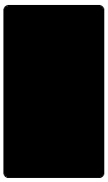
LED	Status	Description
CTL	 Solid Green	Unleashed Master AP.
AIR	 N/A	No upstream mesh connection (Root AP).
AIR		Upstream mesh connection established (Mesh AP).
AIR		Upstream mesh connection issue.
2.4G	 Off	Radio is down.

TABLE 5 Front Panel LEDs (continued)

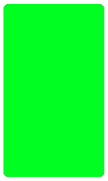
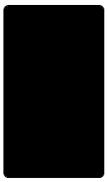
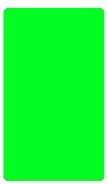
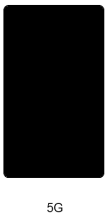
LED	Status	Description
2.4G	Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 5 Front Panel LEDs (continued)

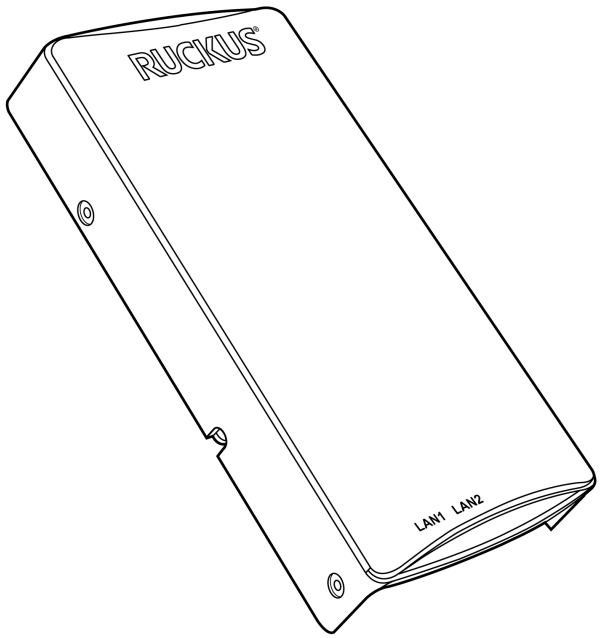
LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

H350

The H350 is a Wi-Fi 6 (802.11ax) Wi-Fi access point with integrated switch in a wall-plate form factor.

This section describes the physical features of the RUCKUS Unleashed H350 802.11ax Access Point.

FIGURE 6 H350 Access Point



Rear Panel

The H350 AP features five LEDs on its rear panel. (LEDs are concealed when mounted.)

TABLE 6 Front Panel LEDs

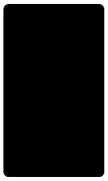
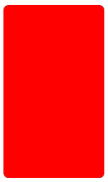
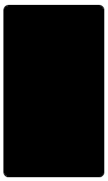
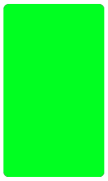
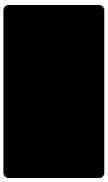
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.

TABLE 6 Front Panel LEDs (continued)

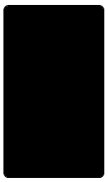
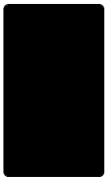
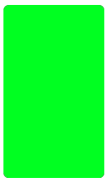
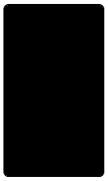
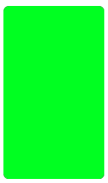
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 6 Front Panel LEDs (continued)

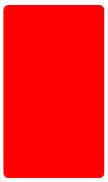
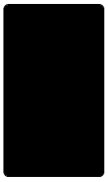
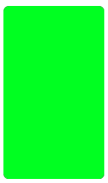
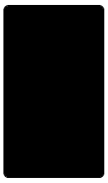
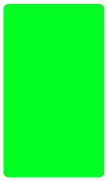
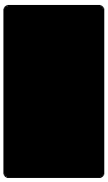
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 6 Front Panel LEDs (continued)

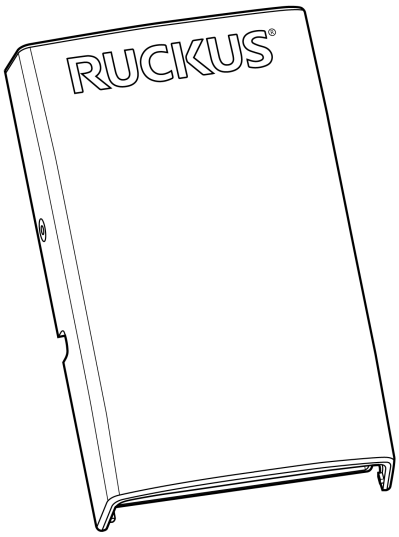
LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

H510

The H510 is an 802.11ac Wave 2 dual-band concurrent Wi-Fi Wall Switch AP with integrated 5-port gigabit Ethernet, in a form factor designed for mounting to electrical outlet boxes.

This section describes the physical features of the RUCKUS Unleashed H510 802.11ac Access Point.

FIGURE 7 H510 Access Point



Rear Panel

The H510 AP features five LEDs on its rear panel. (LEDs are concealed when mounted.)

TABLE 7 Front Panel LEDs

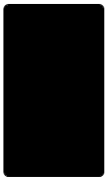
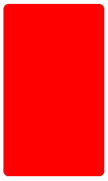
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 7 Front Panel LEDs (continued)

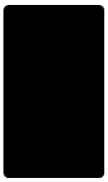
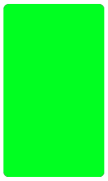
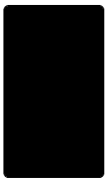
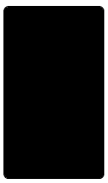
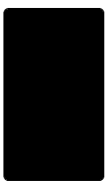
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 7 Front Panel LEDs (continued)

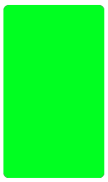
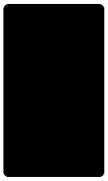
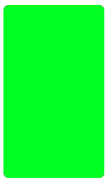
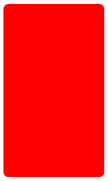
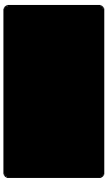
LED	Status	Description
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.

TABLE 7 Front Panel LEDs (continued)

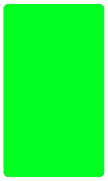
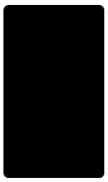
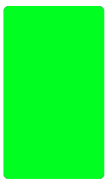
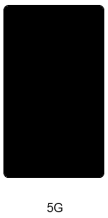
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 7 Front Panel LEDs (continued)

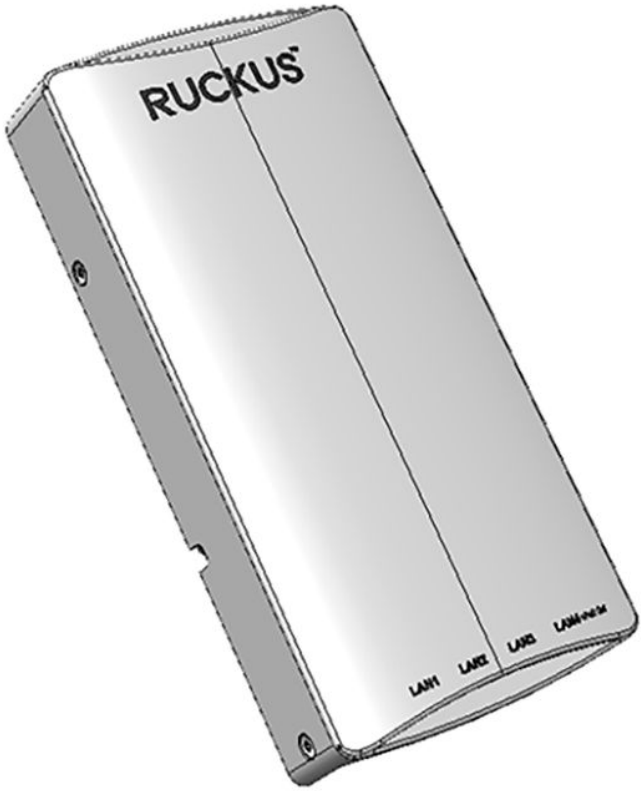
LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

H550

The H550 is an 802.11ax Wave 2 dual-band concurrent Wi-Fi Wall Switch with integrated 5-port gigabit Ethernet, in a form factor designed for mounting to electrical outlet boxes.

This section describes the physical features of the RUCKUS Unleashed H550 802.11ax Access Point.

FIGURE 8 H550 Access Point



Rear Panel

The H550 AP features five LEDs on its rear panel. (LEDs are concealed when mounted.)

TABLE 8 Front Panel LEDs

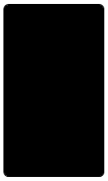
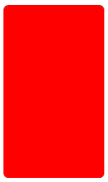
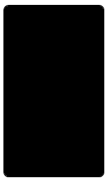
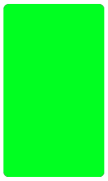
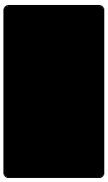
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.

TABLE 8 Front Panel LEDs (continued)

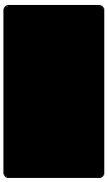
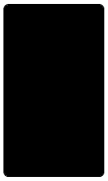
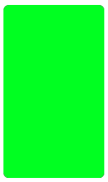
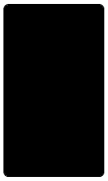
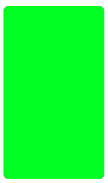
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 8 Front Panel LEDs (continued)

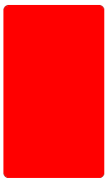
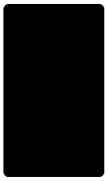
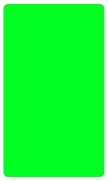
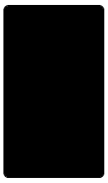
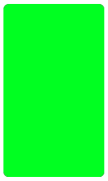
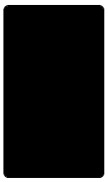
LED	Status	Description
AIR		Upstream mesh connection issue.
2.4G	 Off	Radio is down.
2.4G	Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.

TABLE 8 Front Panel LEDs (continued)

LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

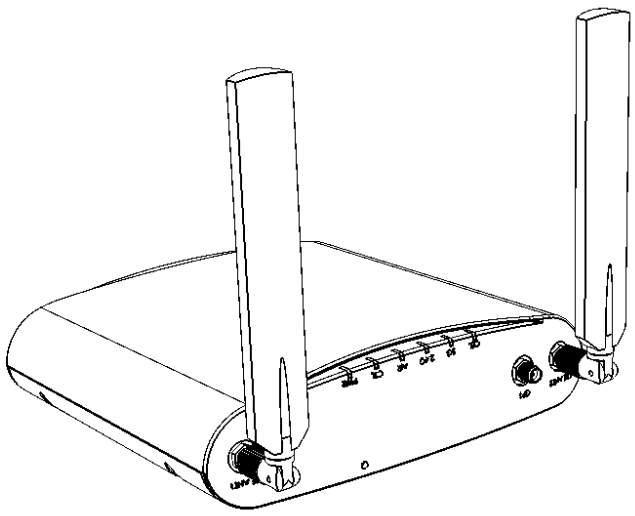
M510

The Unleashed M510 is an 802.11ac Wave 2 Access Point with embedded LTE module for cellular backhaul. The M510 is designed for deployment in scenarios where there is no readily accessible wired connectivity for backhaul, such as in buses, taxis, or other in-vehicle deployments, or in remote locations where the cost of establishing a fixed line ISP connection outweighs that of a wireless connection to a local 3G/4G network.

NOTE
Because the M510 supports LTE backhaul, it requires special setup procedures different from other Unleashed APs. For information, see M510 Configuration on page 52.

This section describes the physical features of the RUCKUS Unleashed M510 LTE Access Point.

FIGURE 9 M510 Access Point



Front Panel

The M510 AP features six LEDs on its front panel.

TABLE 9 Front Panel LEDs

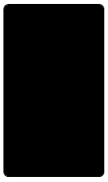
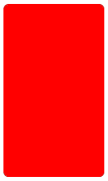
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 9 Front Panel LEDs (continued)

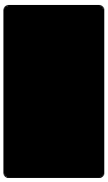
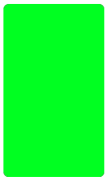
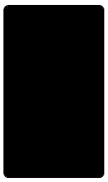
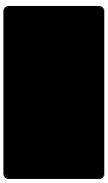
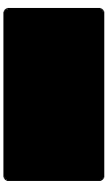
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable Ethernet IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 9 Front Panel LEDs (continued)

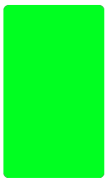
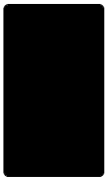
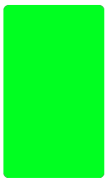
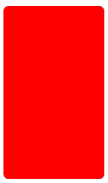
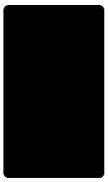
LED	Status	Description
CTL	 Solid Green	Unleashed Master AP.
AIR	 N/A	No upstream mesh connection (Root AP).
AIR		Upstream mesh connection established (Mesh AP).
AIR		Upstream mesh connection issue.
2.4G	 Off	Radio is down.

TABLE 9 Front Panel LEDs (continued)

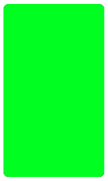
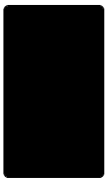
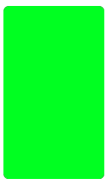
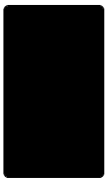
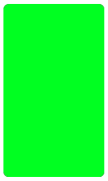
LED	Status	Description
2.4G	Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 9 Front Panel LEDs (continued)

LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.
CEL	 Solid Green	• Off: No cellular connection. • Amber: 3G connection. • Green: 4G/LTE connection.

NOTE
CEL LED will remain in "Off" status until the Unleashed M510 is provisioned.

Bottom Panel

The bottom panel of the M510 includes the following:

- Two 10/100/1000 Mbps Ethernet ports
- 12V DC power socket
- Reset button
- Two redundant SIM card slots for LTE backhaul

FIGURE 10 M510 bottom panel

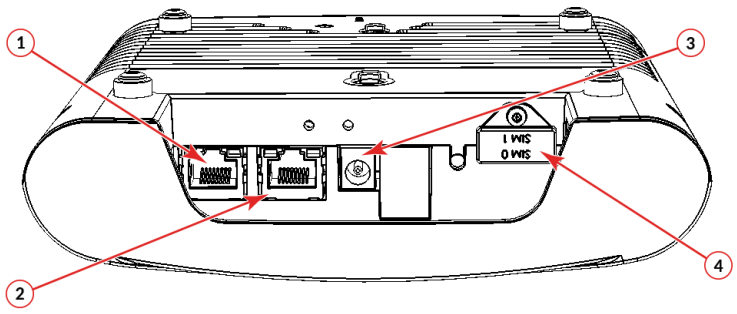


TABLE 10 M510 bottom panel elements

No.	Label	Description
1	ETH 0 WAN / PoE	10/100/1000 Mbps RJ-45 Ethernet port with PoE support

TABLE 10 M510 bottom panel elements (continued)

No.	Label	Description
2	ETH 1 LAN	10/100/1000 Mbps RJ-45 Ethernet port
3	12V DC input, terminal block and DC connector	Connect a customer-ordered RUCKUS DC power adapter (sold separately), or connect power directly using DC terminal block.
4	SIM Card Slots	Insert an activated SIM card into the primary slot, and optionally, a second SIM card into secondary slot for redundancy. **NOTE** The orientation of the SIM cards is reversed, refer to the *M510 Quick Setup Guide* for details on SIM card insertion.

Ethernet Port LEDs

TABLE 11 Behavior of Ethernet port LEDs on the M510

LED	Description
Off	Not connected
Amber + Green	Connected to 10Mbps device
Amber	Connected to 100Mbps device
Green	Connected to 1000Mbps device

Deployment Considerations

The Unleashed M510 is designed for the following two primary deployment scenarios:

- *Mobile Environment*: M510 configured as Master AP in Gateway Mode with an LTE connection as the uplink WAN port.
- *LTE Backup Environment*: M510 in Gateway Mode with the Ethernet port as the WAN port and the LTE connection as the backup WAN port, only one of which can be active at any time. If the Ethernet connection goes down, the LTE connection becomes active to provide a backup internet uplink.

Both options can be configured using the **WAN Connection** setting on the *IP Settings* page when the M510 is configured as the Unleashed Master AP in Gateway Mode.

Limitations

- M510 does not support configuration as the Master AP in bridge mode or as a member AP. Only Master AP in Gateway mode is supported.
- Backup and restore may not function properly if the backup was created on an M510 and restored to a non-M510 AP, or vice-versa.

M510 Configuration

The M510 Wi-Fi + LTE Access Point requires additional setup steps to configure the cellular uplink connection.

The M510 is designed to be deployed in one of the following two deployment scenarios: Ethernet WAN port with Cellular backup, or Cellular Only.

To configure the M510 using the Setup Wizard, select **Gateway Mode** on the *IP Setting* page (page 2 of the Setup Wizard).

In *WAN Connection*, select one of the following options:

- **Ethernet (primary) with Cellular failover**
- **Cellular only**

If *Ethernet with Cellular failover* is selected, you must configure the WAN port settings (Manual or DHCP) as well as the Cellular Radio Settings, and the internal network IP address settings.

If *Cellular only* is selected, you do not need to enter WAN port IP address settings.

FIGURE 11 Ethernet (Primary) with Cellular failover

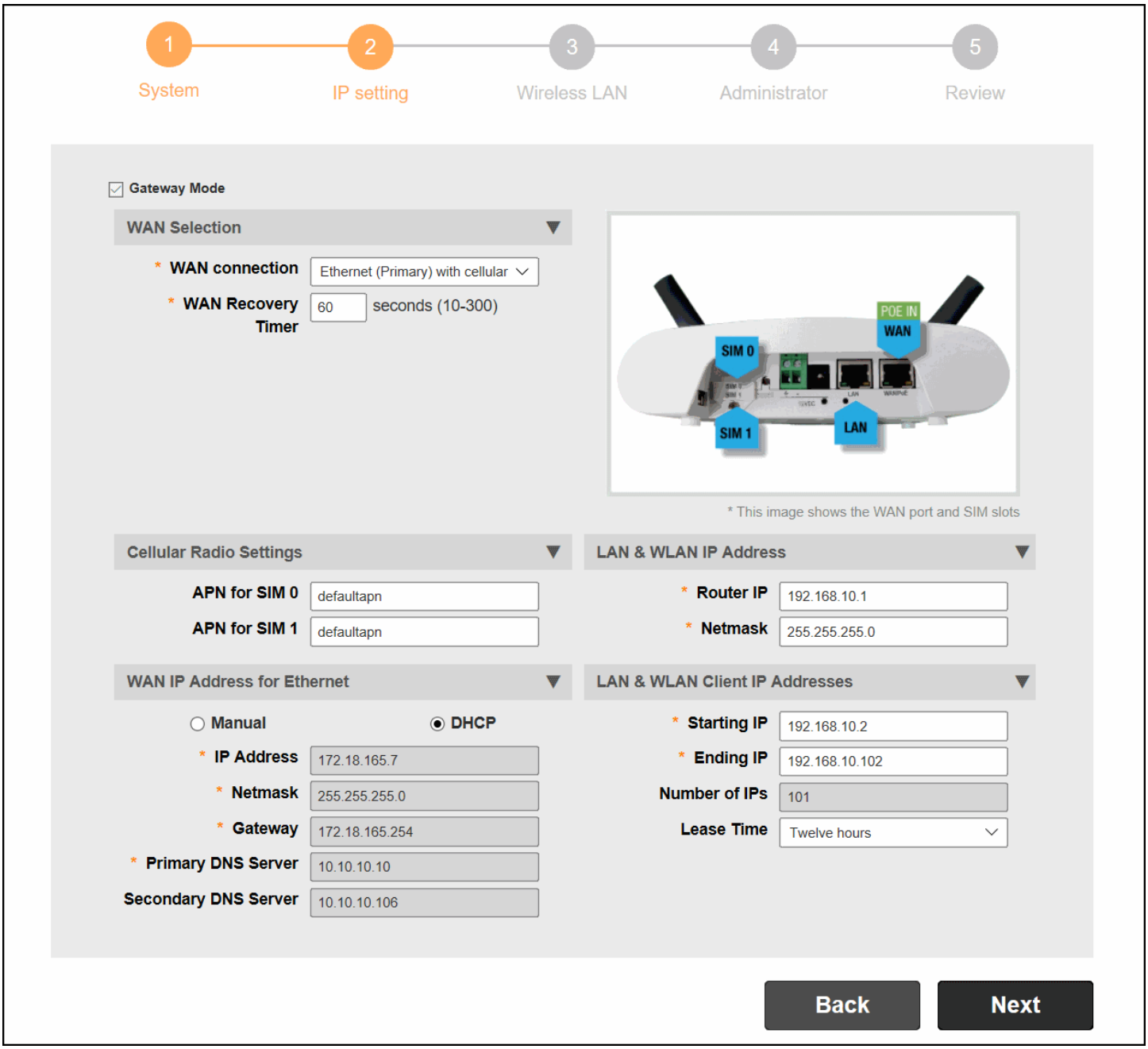
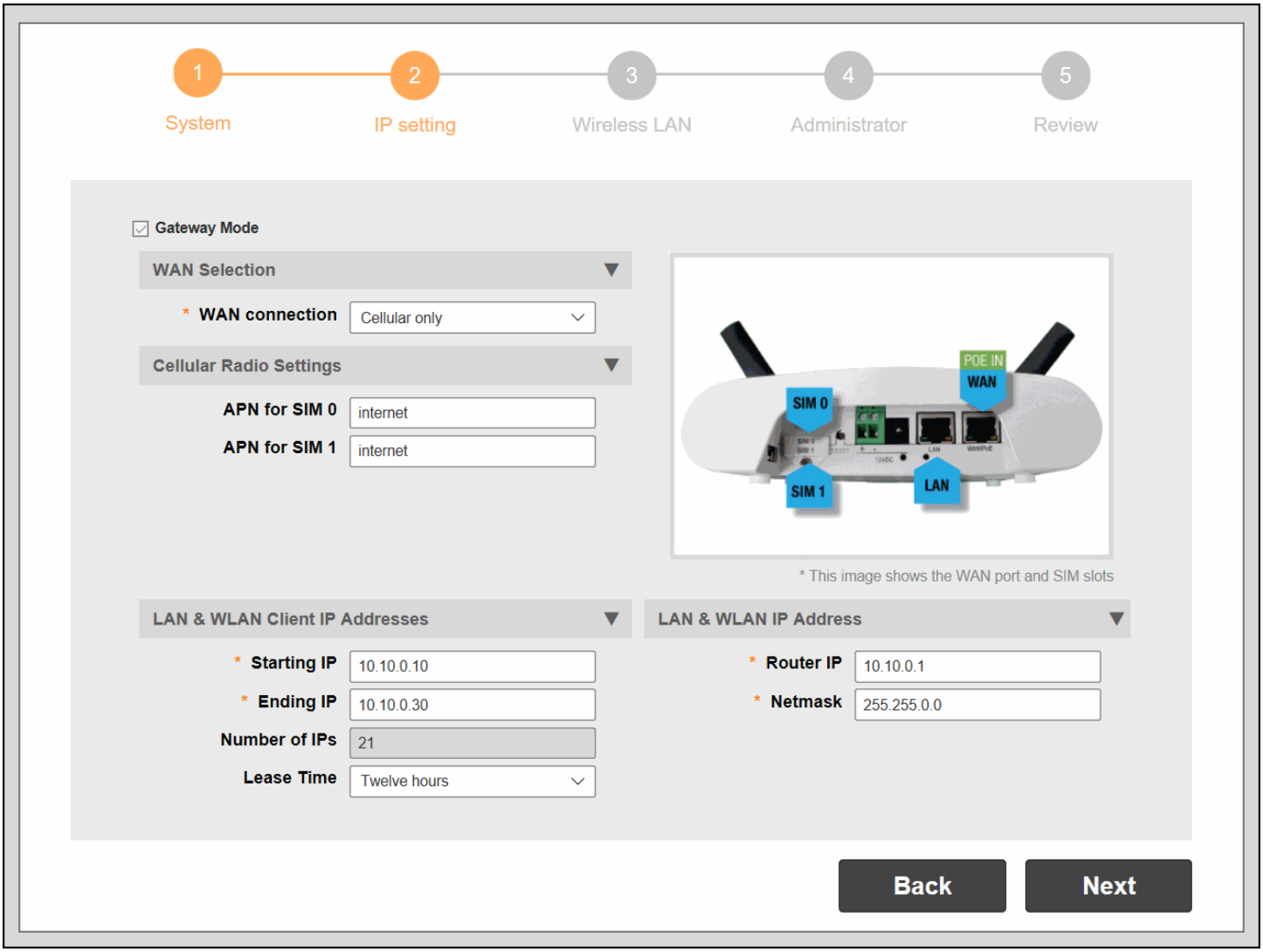


FIGURE 12 Cellular only



NOTE
M510 does not support Bridge mode.

NOTE
Cellular is disabled by default. The CEL LED will remain off until the Setup Wizard setup is completed.

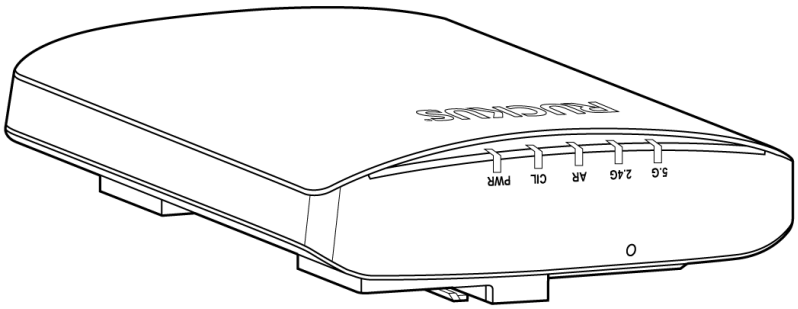
NOTE
PPPoE IP address mode is not supported on Unleashed M510.

R320

R320 is a dual-band concurrent 2x2:2 802.11ac Wave 2 Access Point that delivers high-performance wireless networking at a competitive price point in a compact form factor.

This section describes the physical features of RUCKUS Unleashed R320 802.11ac Access Point.

FIGURE 13 R320 Access Point



Front Panel

The R320 AP features five LEDs on its front panel.

TABLE 12 Front Panel LEDs

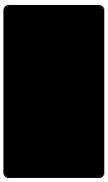
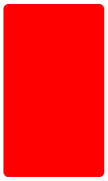
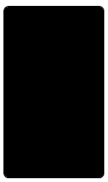
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.

TABLE 12 Front Panel LEDs (continued)

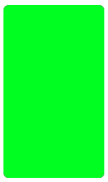
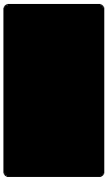
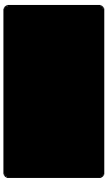
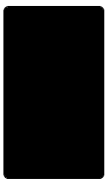
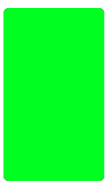
LED	Status	Description
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Master AP.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Master AP.

TABLE 12 Front Panel LEDs (continued)

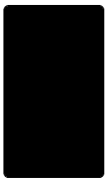
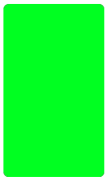
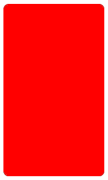
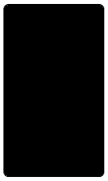
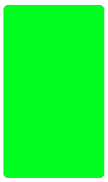
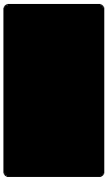
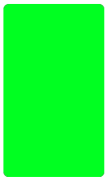
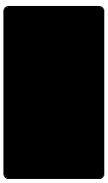
LED	Status	Description
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.

TABLE 12 Front Panel LEDs (continued)

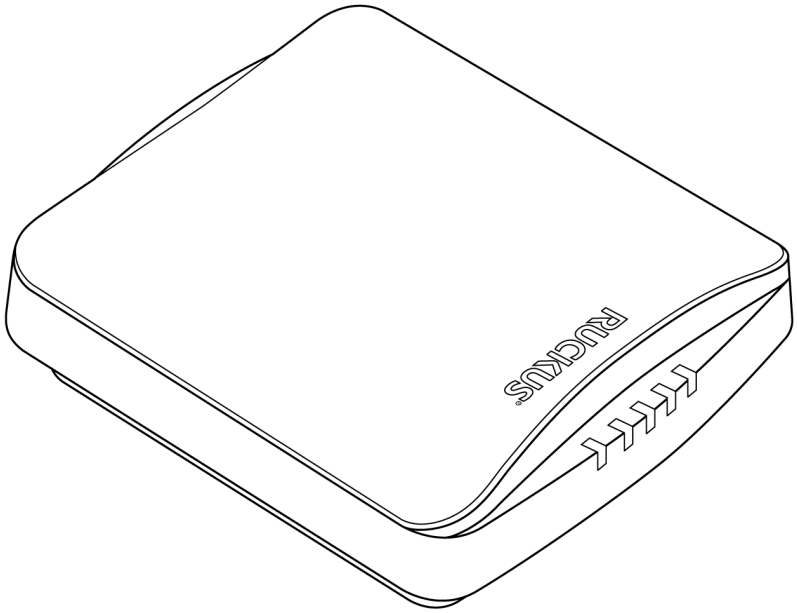
LED	Status	Description
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R350

The Unleashed R350 is a dual-band concurrent 2x2:2 802.11ax Wave 2 Access Point that delivers high-performance wireless networking at a competitive price point in a compact form factor.

This section describes the physical features of the RUCKUS Unleashed R350 802.11ax Access Point.

FIGURE 14 R350 Access Point



Front Panel

The R350 AP features five LEDs on its front panel.

TABLE 13 Front Panel LEDs

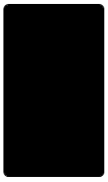
LED	Status	Description
PWR	 PWR Off	No power connected.

TABLE 13 Front Panel LEDs (continued)

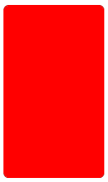
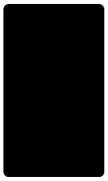
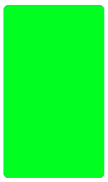
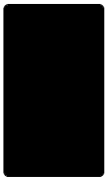
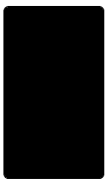
LED	Status	Description
PWR	 Solid Red	Boot up in process.
PWR	 Flashing Green	System started, no routable IP address detected.
PWR	 Solid Green	Routable IP address received.
CTL	 Off	Unleashed Member AP.
CTL	 Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.

TABLE 13 Front Panel LEDs (continued)

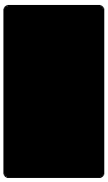
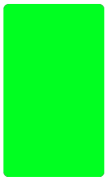
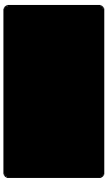
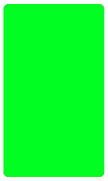
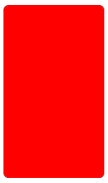
LED	Status	Description
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.

TABLE 13 Front Panel LEDs (continued)

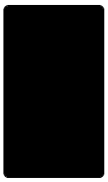
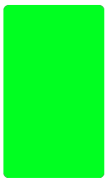
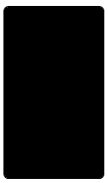
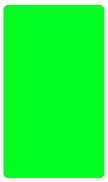
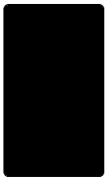
LED	Status	Description
2.4G	 Off	Radio is down.
2.4G	Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.

TABLE 13 Front Panel LEDs (continued)

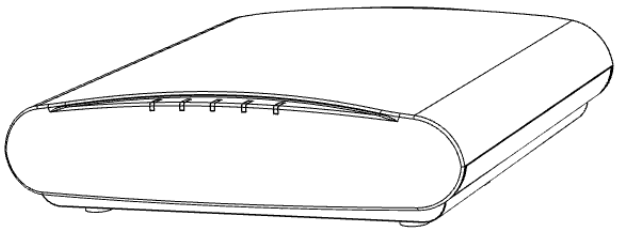
LED	Status	Description
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R510

The Unleashed R510 brings cutting edge 802.11ac Wave 2 to the mid-tier segment. It improves aggregate network throughput and benefits both Wave 2 & non-Wave 2 clients.

This section describes the physical features of the RUCKUS Unleashed R510 802.11ac Wave 2 Access Point.

FIGURE 15 R510 Access Point



Front Panel

The R510 AP features five LEDs on its front panel.

TABLE 14 Front Panel LEDs

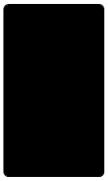
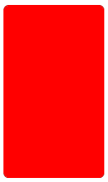
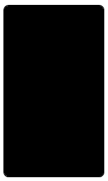
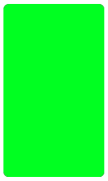
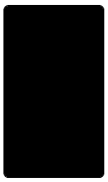
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.

TABLE 14 Front Panel LEDs (continued)

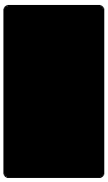
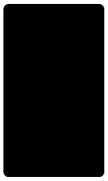
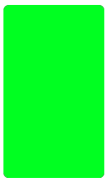
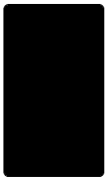
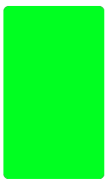
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 14 Front Panel LEDs (continued)

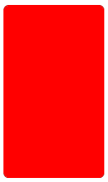
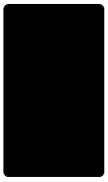
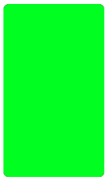
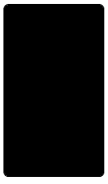
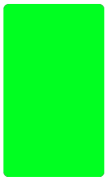
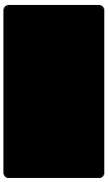
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 14 Front Panel LEDs (continued)

LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R550

The RUCKUS R550 is a mid-range indoor 2x2:2 Wi-Fi 6 (802.11ax) dual-band access point with integrated 2-port Ethernet interface. The R550 is targeted for medium-density, small to mid-size indoor enterprise WLAN applications in the enterprise, education, hospitality, carrier, healthcare and retail industries.

This section describes the physical features of the RUCKUS Unleashed R550 AP.

FIGURE 16 Unleashed R550 Access Point

Front Panel

The R550 AP features five LEDs on its front panel.

TABLE 15 Front Panel LEDs

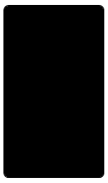
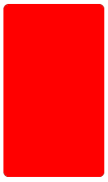
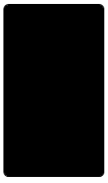
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.

TABLE 15 Front Panel LEDs (continued)

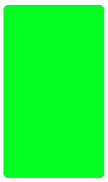
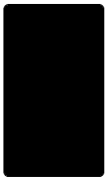
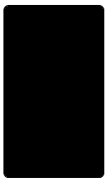
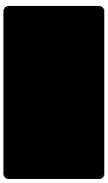
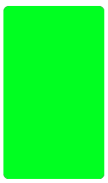
LED	Status	Description
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.

TABLE 15 Front Panel LEDs (continued)

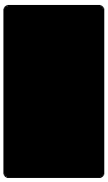
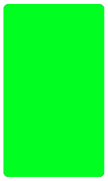
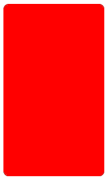
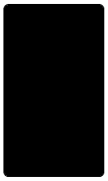
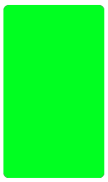
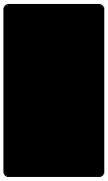
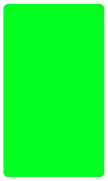
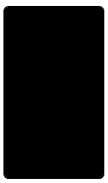
LED	Status	Description
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.

TABLE 15 Front Panel LEDs (continued)

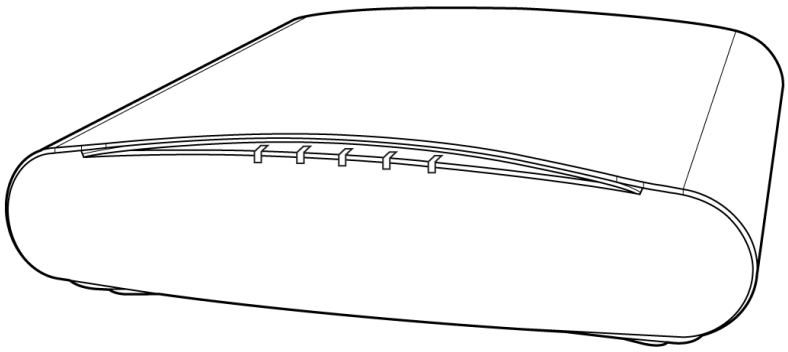
LED	Status	Description
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R610

The Unleashed R610 is a dual-band concurrent 3x3:3 802.11ac Wave 2 Access Point that delivers high-performance wireless networking with aggregate rates of up to 1300 Mbps (5GHz) 600 Mbps (2.4GHz) maximum PHY rate.

This section describes the physical features of the RUCKUS Unleashed R610 802.11ac Wave 2 Access Point.

FIGURE 17 R610 Access Point



Front Panel

The R610 AP features five LEDs on its front panel.

TABLE 16 Front Panel LEDs

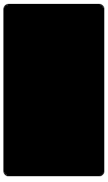
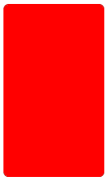
LED	Status	Description
PWR	 Off	No power connected.
PWR	 Solid Red	Boot up in process.

TABLE 16 Front Panel LEDs (continued)

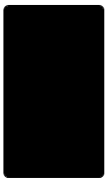
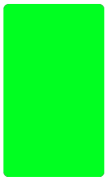
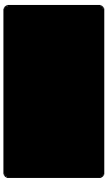
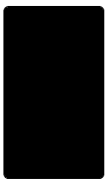
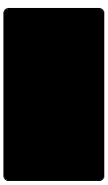
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 16 Front Panel LEDs (continued)

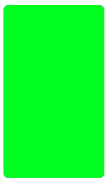
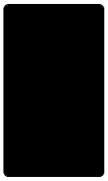
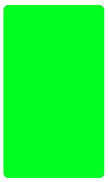
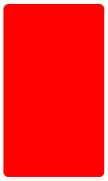
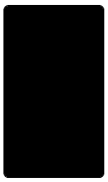
LED	Status	Description
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.

TABLE 16 Front Panel LEDs (continued)

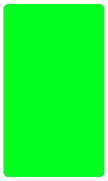
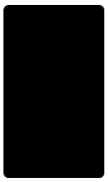
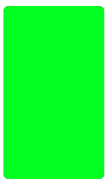
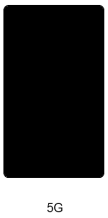
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 16 Front Panel LEDs (continued)

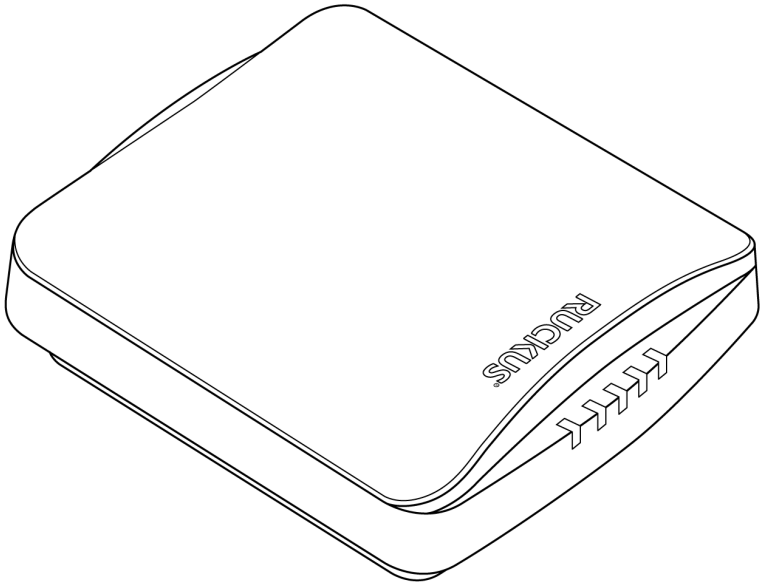
LED	Status	Description
5G	 5G Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R650

The RUCKUS R650 is a mid-range "Wi-Fi 6" (802.11ax) dual-band indoor 4x4: 4 AP with BeamFlex+, one 2.5 Gbps PoE+ port, and one 1 Gbps Ethernet port.

This section describes the physical features of the RUCKUS Unleashed R650 AP.

FIGURE 18 Unleashed R650 Access Point



Front Panel

The R650 AP features five LEDs on its front panel.

TABLE 17 Front Panel LEDs

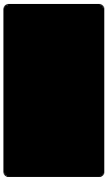
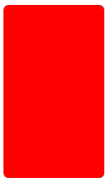
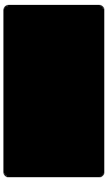
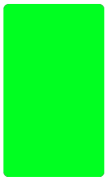
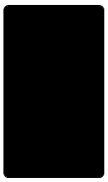
LED	Status	Description
PWR	 Off	No power connected.
PWR	 Solid Red	Boot up in process.
PWR	 Flashing Green	System started, no routable IP address detected.
PWR	 Solid Green	Routable IP address received.
CTL	 Off	Unleashed Member AP.

TABLE 17 Front Panel LEDs (continued)

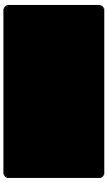
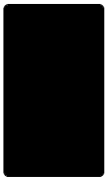
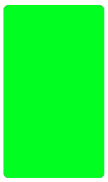
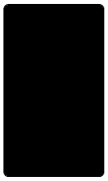
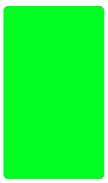
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 17 Front Panel LEDs (continued)

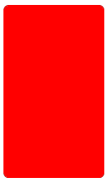
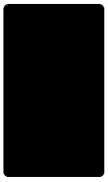
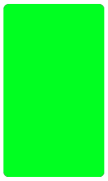
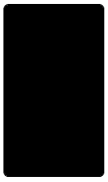
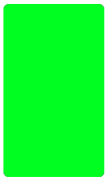
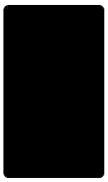
LED	Status	Description
AIR		Upstream mesh connection issue.
2.4G	 Off	Radio is down.
2.4G	Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.

TABLE 17 Front Panel LEDs (continued)

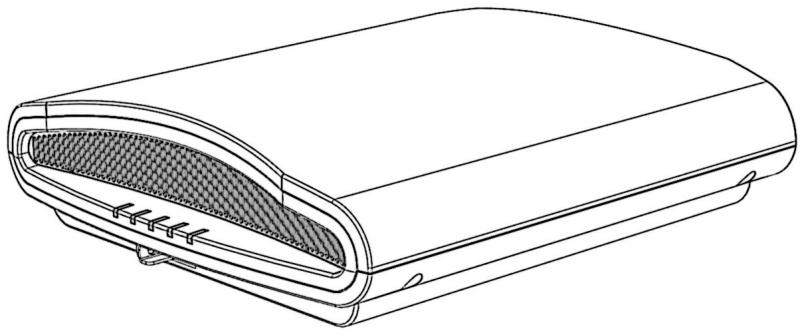
LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R710

The Unleashed R710 is the first RUCKUS Unleashed 802.11ac Wave 2 access point, providing 4x4:4 radio chains and MU-MIMO support for high density installations.

This section describes the physical features of the RUCKUS Unleashed R710 AP.

FIGURE 19 R710 Access Point



Front Panel

The R710 AP features five LEDs on its front panel.

TABLE 18 Front Panel LEDs

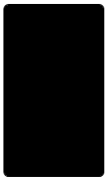
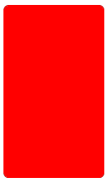
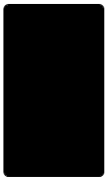
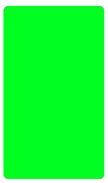
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.

TABLE 18 Front Panel LEDs (continued)

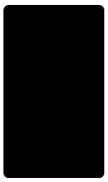
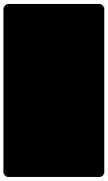
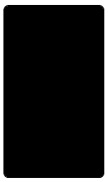
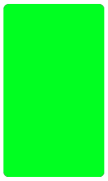
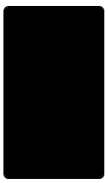
LED	Status	Description
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).

TABLE 18 Front Panel LEDs (continued)

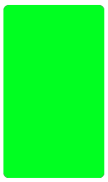
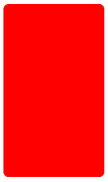
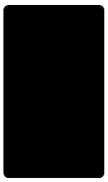
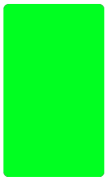
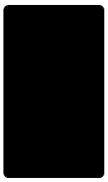
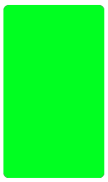
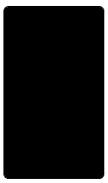
LED	Status	Description
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.

TABLE 18 Front Panel LEDs (continued)

LED	Status	Description
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

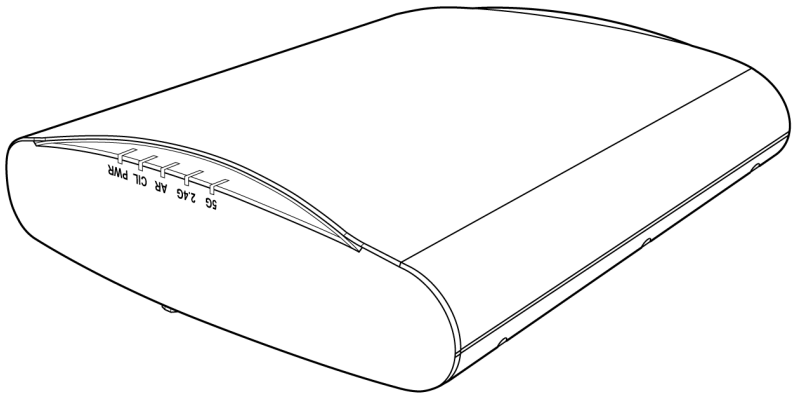
R720

The Unleashed R720 is a dual-band concurrent 4x4 802.11ac Wave 2 Access Point capable of 160 MHz and 80+80 MHz channelization, designed for high density indoor applications.

The R720 features one 10/100/1000 Etherenet port, and one 100/1000/2500 Ethernet port that supports 802.3af and 802.3at Power Over Ethernet (PoE), and a USB port.

This section describes the physical features of the RUCKUS Unleashed R720 AP.

FIGURE 20 R720 Access Point



Front Panel

The R720 AP features five LEDs on its front panel.

TABLE 19 Front Panel LEDs

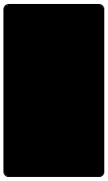
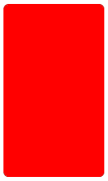
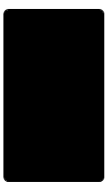
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.

TABLE 19 Front Panel LEDs (continued)

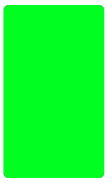
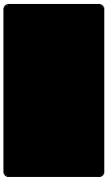
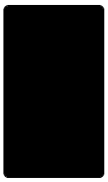
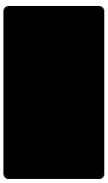
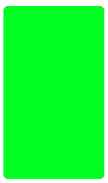
LED	Status	Description
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.

TABLE 19 Front Panel LEDs (continued)

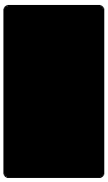
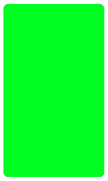
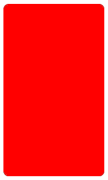
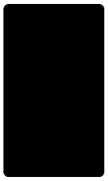
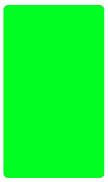
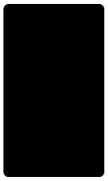
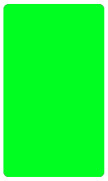
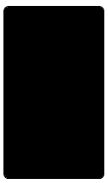
LED	Status	Description
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.

TABLE 19 Front Panel LEDs (continued)

LED	Status	Description
2.4G	 Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 Off	Radio is down.
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R750

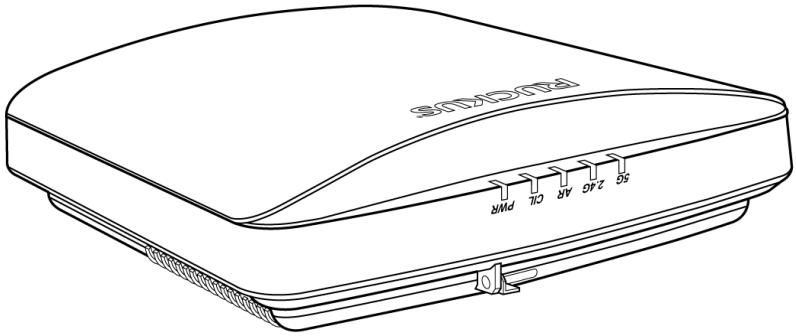
The Unleashed R750 is a dual-band concurrent "Wi-Fi 6" (802.11ax) AP that supports 8 spatial streams (4x4:4 in 5GHz, 4x4:4 in 2.4GHz).

The Unleashed R750 provides advanced 11ax features such as OFDMA, MU-MIMO, 11ax power save, and WPA3. It includes a USB port and a 2.5 GbE port that supports 802.3af, 802.3at and 802.3bt (40W) PoE, and one 1 GbE port (non-PoE).

NOTE
Dedicated Master mode is supported if an R750 AP is the Master AP in the Unleashed network.

This section describes the physical features of the RUCKUS Unleashed R750 AP.

FIGURE 21 Unleashed R750 Access Point



Front Panel

The R750 AP features five LEDs on its front panel.

TABLE 20 Front Panel LEDs

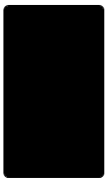
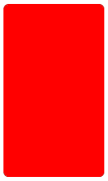
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 20 Front Panel LEDs (continued)

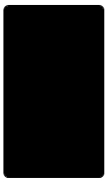
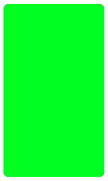
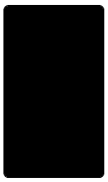
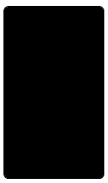
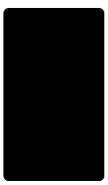
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 20 Front Panel LEDs (continued)

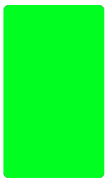
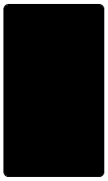
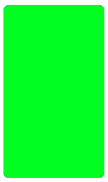
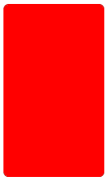
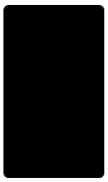
LED	Status	Description
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.

TABLE 20 Front Panel LEDs (continued)

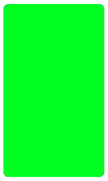
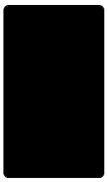
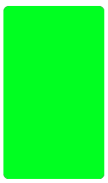
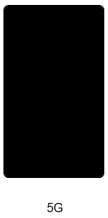
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 20 Front Panel LEDs (continued)

LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

R850

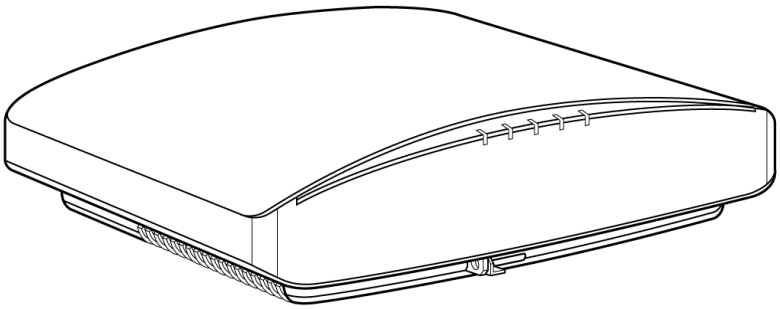
The Unleashed R850 is a dual-band Wi-Fi 6 Indoor access point with 12 radio chains, operating in 8x8:8 mode on the 5GHz band and in 4x4:4 mode on the 2.4GHz band, supporting peak PHY rates of 4.8Gbps (5GHz) and 1.148Gbps (2.4GHz).

The R850 has one 5 Gbps PoE Ethernet port and one 1 Gbps port and a USB port for additional connectivity. The R850 will operate with PoH, uPOE and 802.3at power.

NOTE
Dedicated Master mode is supported if an R850 AP is the Master AP in the Unleashed network.

This section describes the physical features of the RUCKUS Unleashed R850 AP.

FIGURE 22 Unleashed R850 Access Point



Front Panel

The R850 AP features five LEDs on its front panel.

TABLE 21 Front Panel LEDs

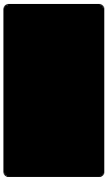
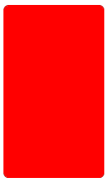
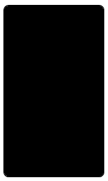
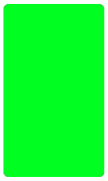
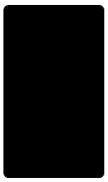
LED	Status	Description
PWR	 Off	No power connected.
PWR	 Solid Red	Boot up in process.
PWR	 Flashing Green	System started, no routable IP address detected.
PWR	 Solid Green	Routable IP address received.
CTL	 Off	Unleashed Member AP.

TABLE 21 Front Panel LEDs (continued)

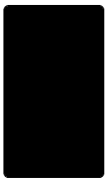
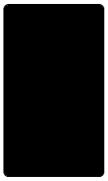
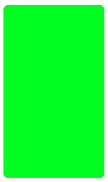
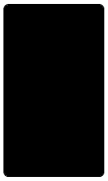
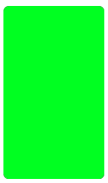
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 21 Front Panel LEDs (continued)

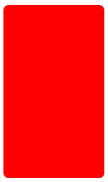
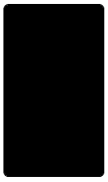
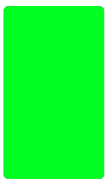
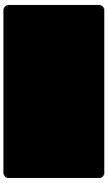
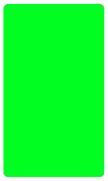
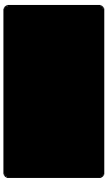
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 21 Front Panel LEDs (continued)

LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

T310 Family

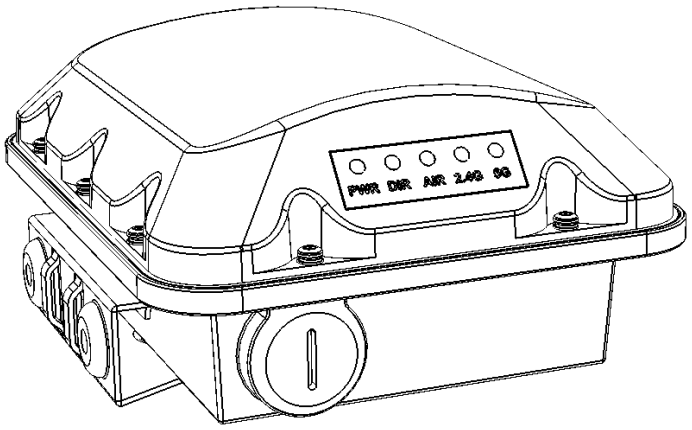
The T310 family provides 802.11ac "Wave 2" features, including MU-MIMO, in an outdoor access point.

This section describes the physical features of the RUCKUS Unleashed T310 family of dual-band 802.11ac Wave 2 Outdoor Access Points.

The T310 is available in four antenna variants:

- T310c: Standard omni antenna
- T310d: Standard omni antenna, extended temperature range
- T310n: Narrow sector antenna variant
- T310s: Sector antenna variant

FIGURE 23 T310d Outdoor Access Point



Front Panel

The T310 features five LEDs on its front panel.

TABLE 22 Front Panel LEDs

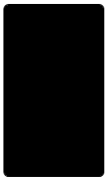
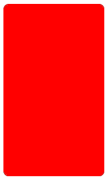
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 22 Front Panel LEDs (continued)

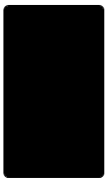
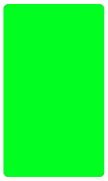
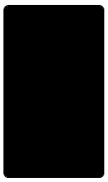
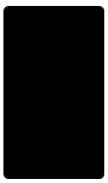
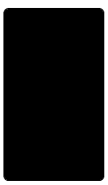
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Master AP.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 22 Front Panel LEDs (continued)

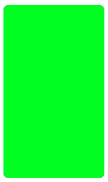
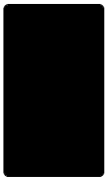
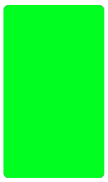
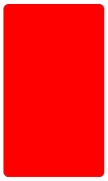
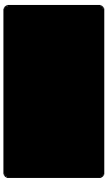
LED	Status	Description
CTL	 CTL Solid Green	Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.

TABLE 22 Front Panel LEDs (continued)

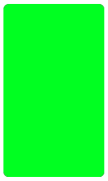
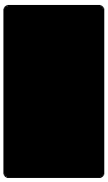
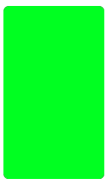
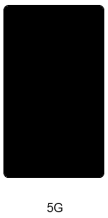
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 22 Front Panel LEDs (continued)

LED	Status	Description
5G	 5G Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

T350 Family

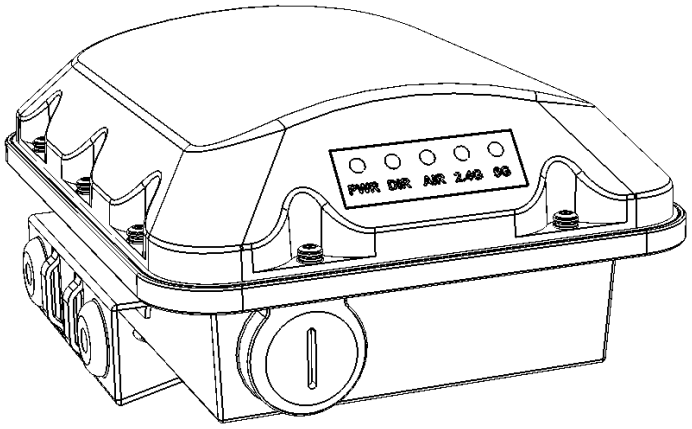
The Unleashed T350 family provides 802.11ax "Wave 2" features, including MU-MIMO, in an outdoor access point.

This section describes the physical features of the RUCKUS Unleashed T310 family of dual-band 802.11ax Wave 2 Outdoor Access Points.

The T350 is available in four antenna variants:

- T350c: Standard omni antenna
- T350d: Standard omni antenna, extended temperature range

FIGURE 24 T350d Outdoor Access Point



Front Panel

The T350 features five LEDs on its front panel.

TABLE 23 Front Panel LEDs

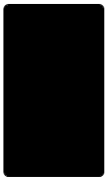
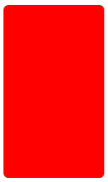
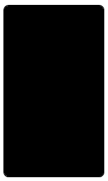
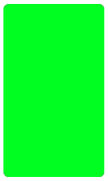
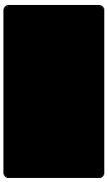
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.

TABLE 23 Front Panel LEDs (continued)

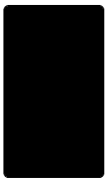
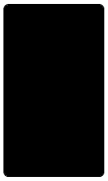
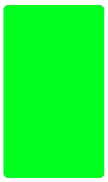
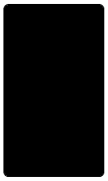
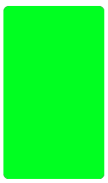
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 23 Front Panel LEDs (continued)

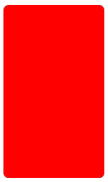
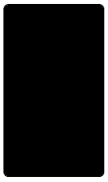
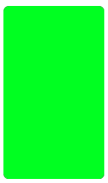
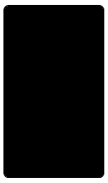
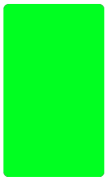
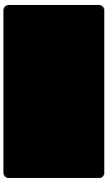
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 23 Front Panel LEDs (continued)

LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

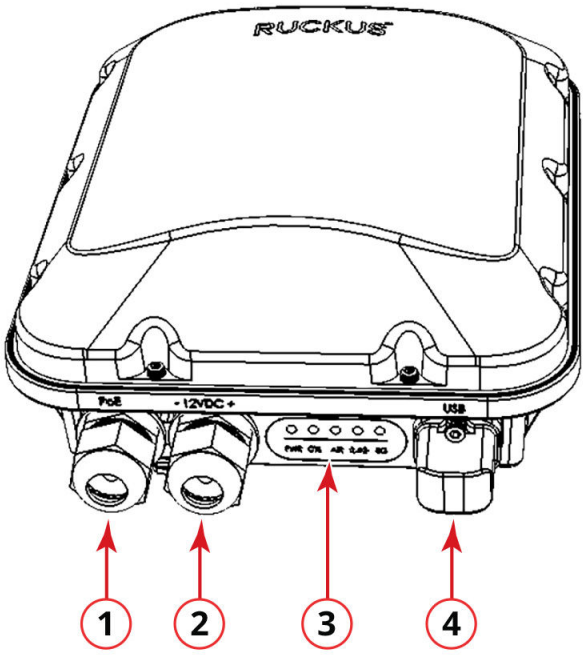
T350SE

The RUCKUS T350se is a Wi-Fi 6 (802.11ax) Wi-Fi access point supporting dual-band concurrent 2x2:2 802.11ax (5GHz) and 2x2:2 802.11ax (2.4GHz) for outdoor applications.

The T350se has an internal 120-degree sectorized antenna, an integrated single 1-Gbps Ethernet port, a DC port, an USB port, and 2 N-type ports to connect to an external antenna.

This section describes the physical features of the RUCKUS Unleashed T350SE AP.

FIGURE 25 Unleashed T350SE Access Point



1. PoE
2. 12V DC
3. LED
4. USB

Front Panel

The T350SE AP features five LEDs on its front panel.

TABLE 24 Front Panel LEDs

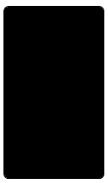
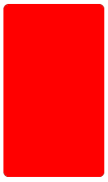
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 24 Front Panel LEDs (continued)

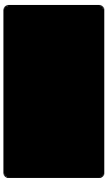
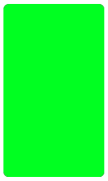
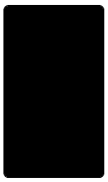
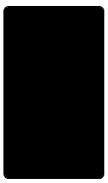
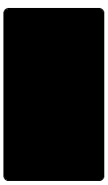
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 24 Front Panel LEDs (continued)

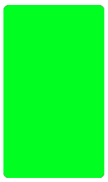
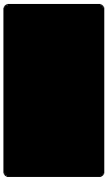
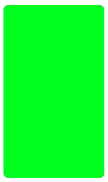
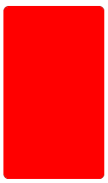
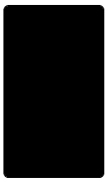
LED	Status	Description
CTL	 Solid Green	Unleashed Master AP.
AIR	 N/A	No upstream mesh connection (Root AP).
AIR		Upstream mesh connection established (Mesh AP).
AIR		Upstream mesh connection issue.
2.4G	 Off	Radio is down.

TABLE 24 Front Panel LEDs (continued)

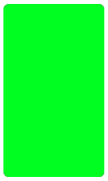
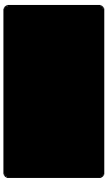
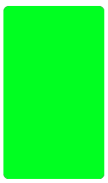
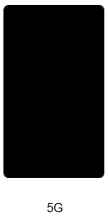
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 24 Front Panel LEDs (continued)

LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

T610 and T610s

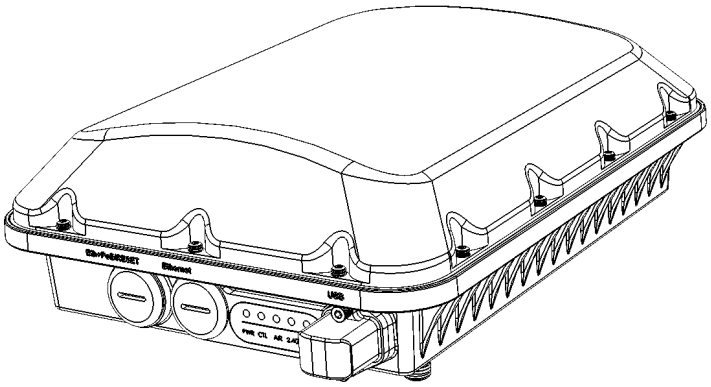
The RUCKUS Unleashed T610 is an outdoor dual radio 4x4:4 802.11ac Wave 2 access point with two 1 Gigabit Ethernet ports, PoE in, and 802.1ax Ethernet port aggregation.

The T610 also includes a USB port.

This section describes the physical features of the RUCKUS Unleashed T610 and T610s access points.

NOTE
The T610s is the 120 degree sector antenna variant of the T610. It includes all of the same physical features as the T610 (omni) version.

FIGURE 26 Unleashed T610/T610s Outdoor Access Point



Front Panel

The T610 (and T610s) AP features five LEDs on its front panel.

TABLE 25 Front Panel LEDs

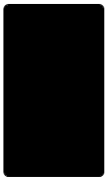
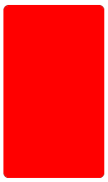
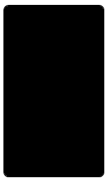
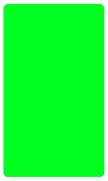
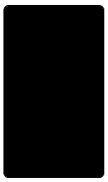
LED	Status	Description
PWR	 Off	No power connected.
PWR	 Solid Red	Boot up in process.
PWR	 Flashing Green	System started, no routable IP address detected.
PWR	 Solid Green	Routable IP address received.
CTL	 Off	Unleashed Member AP.

TABLE 25 Front Panel LEDs (continued)

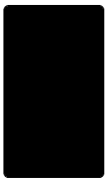
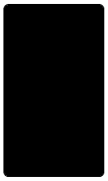
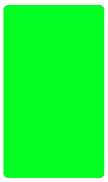
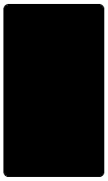
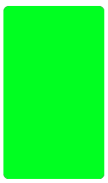
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 25 Front Panel LEDs (continued)

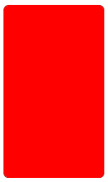
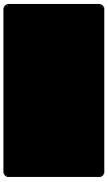
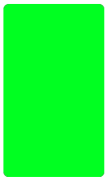
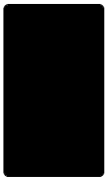
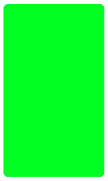
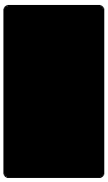
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 25 Front Panel LEDs (continued)

LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

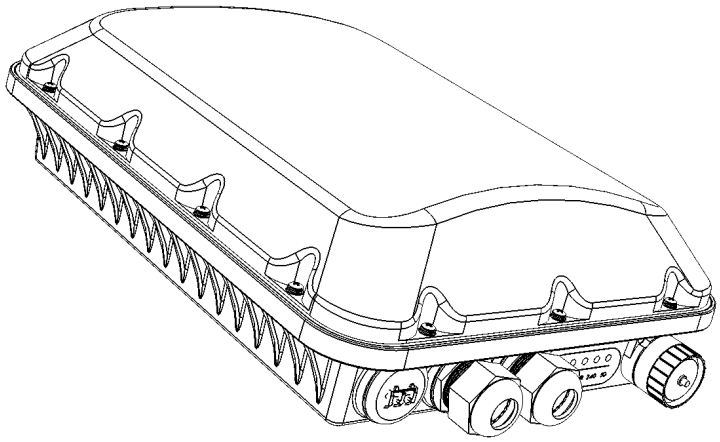
T710 and T710s

The Unleashed T710 is the first outdoor RUCKUS Unleashed 802.11ac Wave 2 access point.

This section describes the physical features of the RUCKUS Unleashed T710 and T710s access points.

NOTE
The T710s is the 120 degree sector antenna variant of the T710. It includes all of the same physical features as the T710 (omni) version.

FIGURE 27 Unleashed T710/T710s Outdoor Access Point



Front Panel

The T710 (and T710s) AP features five LEDs on its front panel.

TABLE 26 Front Panel LEDs

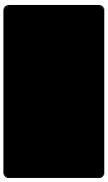
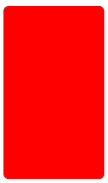
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 26 Front Panel LEDs (continued)

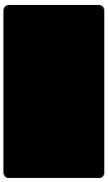
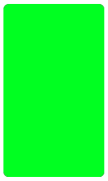
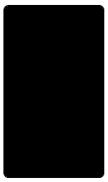
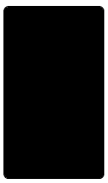
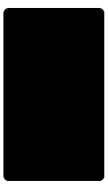
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 26 Front Panel LEDs (continued)

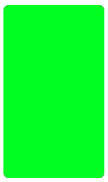
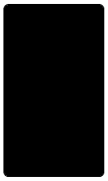
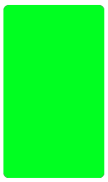
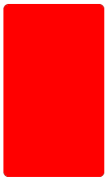
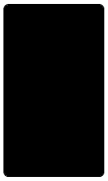
LED	Status	Description
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.

TABLE 26 Front Panel LEDs (continued)

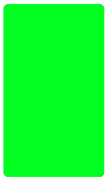
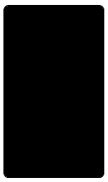
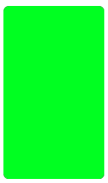
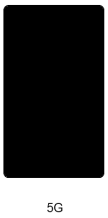
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 26 Front Panel LEDs (continued)

LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

T750

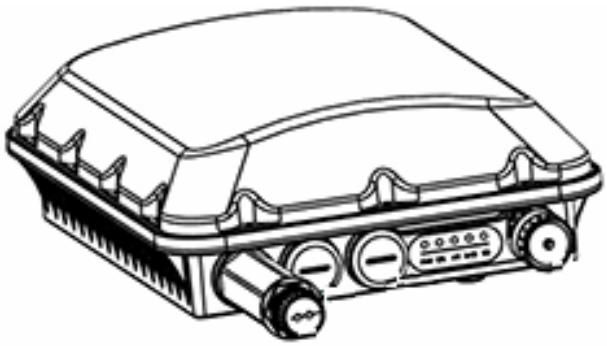
The RUCKUS T750 is a high-end dual-band outdoor Wi-Fi 6 AP that supports 8 spatial streams (4x4:4 in 5GHz, 4x4:4 in 2.4GHz).

The T750 provides advanced 802.11ax features including OFDMA and MU-MIMO, and supports up to 1,024 client connections with increased capacity, improved coverage and performance in ultra-high density environments.

The T750 includes a 2.5 GbE Ethernet PoE+ port for high speed Ethernet backhaul, along with an SFP fiber port for fiber backhaul. Additionally, it includes built-in GPS, USB port, gigabit PoE out port, and IP-67 rated weather proofing.

This section describes the physical features of the RUCKUS Unleashed T750 AP.

FIGURE 28 Unleashed T750 Access Point



Front Panel

The T750 AP features five LEDs on its front panel.

TABLE 27 Front Panel LEDs

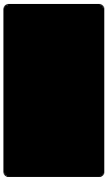
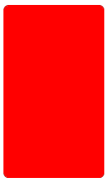
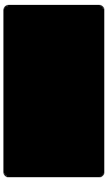
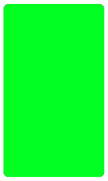
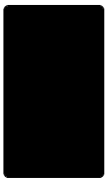
LED	Status	Description
PWR	 Off	No power connected.
PWR	 Solid Red	Boot up in process.
PWR	 Flashing Green	System started, no routable IP address detected.
PWR	 Solid Green	Routable IP address received.
CTL	 Off	Unleashed Member AP.

TABLE 27 Front Panel LEDs (continued)

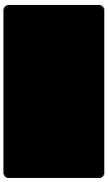
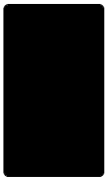
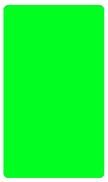
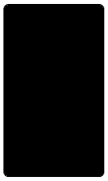
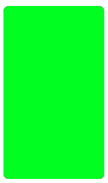
LED	Status	Description
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL	 CTL Solid Green	Unleashed Master AP.
AIR	 AIR N/A	No upstream mesh connection (Root AP).
AIR	 AIR	Upstream mesh connection established (Mesh AP).

TABLE 27 Front Panel LEDs (continued)

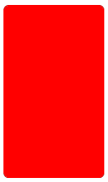
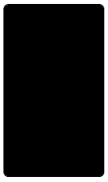
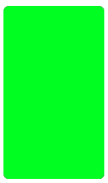
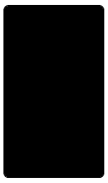
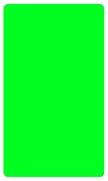
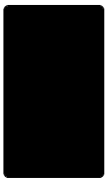
LED	Status	Description
AIR	 AIR	Upstream mesh connection issue.
2.4G	 2.4G Off	Radio is down.
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.

TABLE 27 Front Panel LEDs (continued)

LED	Status	Description
5G	Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

T750SE

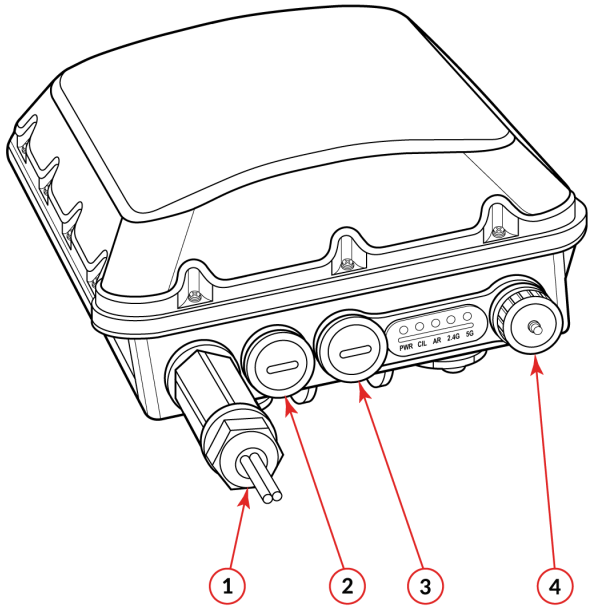
The RUCKUS T750SE is a high-end dual-band outdoor Wi-Fi 6 AP with external antenna connectors that supports 8 spatial streams (4x4:4 in 5GHz, 4x4:4 in 2.4GHz).

The T750SE provides advanced 802.11ax features including OFDMA and MU-MIMO, and supports up to 1,024 client connections with increased capacity, improved coverage and performance in ultra-high density environments.

The T750SE includes a 2.5 GbE Ethernet PoE+ port for high speed Ethernet backhaul, along with an SFP fiber port for fiber backhaul. Additionally, it includes built-in GPS, USB port, gigabit PoE out port, and IP-67 rated weather proofing.

This section describes the physical features of the RUCKUS Unleashed T750SE AP.

FIGURE 29 Unleashed T750SE Access Point



1. SFP port
2. PoE IN
3. PoE OUT
4. AC port

Front Panel

The T750SE AP features five LEDs on its front panel.

TABLE 28 Front Panel LEDs

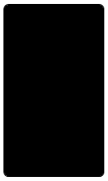
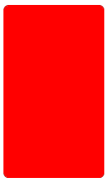
LED	Status	Description
PWR	 PWR Off	No power connected.
PWR	 PWR Solid Red	Boot up in process.

TABLE 28 Front Panel LEDs (continued)

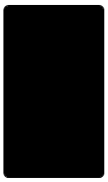
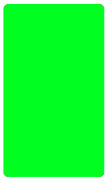
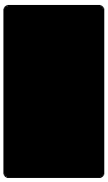
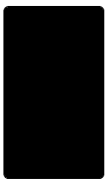
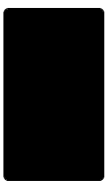
LED	Status	Description
PWR	 PWR Flashing Green	System started, no routable IP address detected.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.
CTL	 CTL Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.

TABLE 28 Front Panel LEDs (continued)

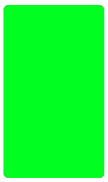
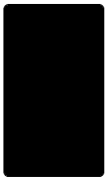
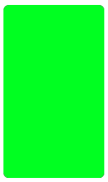
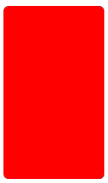
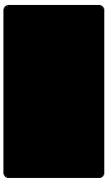
LED	Status	Description
CTL	 Solid Green	Unleashed Master AP.
AIR	 N/A	No upstream mesh connection (Root AP).
AIR		Upstream mesh connection established (Mesh AP).
AIR		Upstream mesh connection issue.
2.4G	 Off	Radio is down.

TABLE 28 Front Panel LEDs (continued)

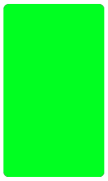
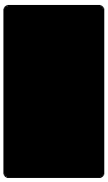
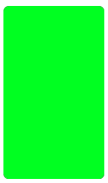
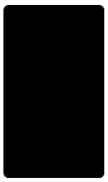
LED	Status	Description
2.4G	2.4G Amber (solid)	Radio is up, no clients are connected to the 2.4 GHz radio.
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.

TABLE 28 Front Panel LEDs (continued)

LED	Status	Description
5G	 Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

Setting Up an Unleashed Wi-Fi Network

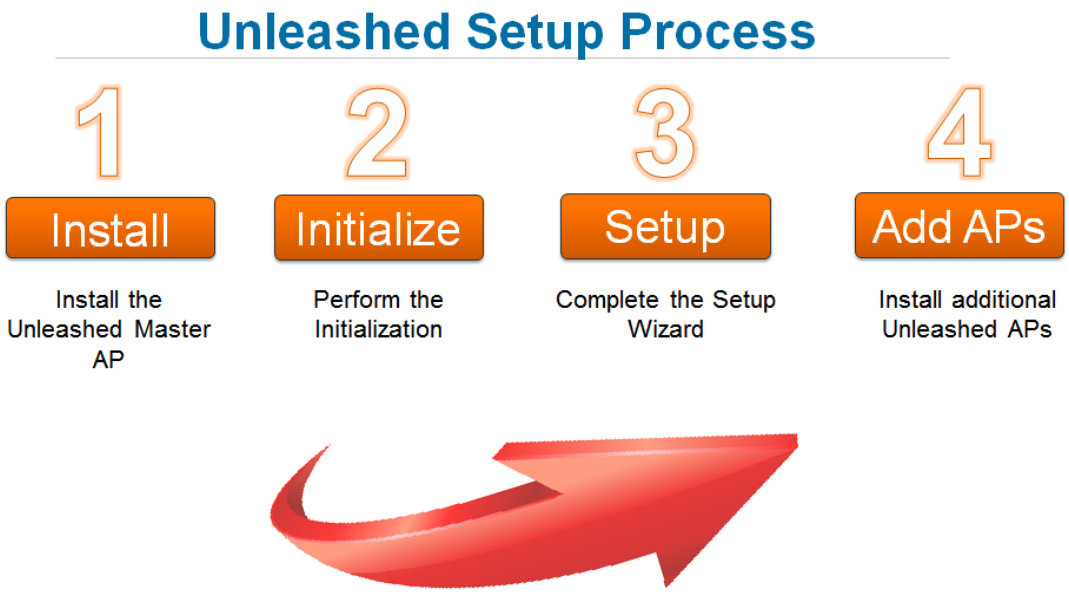
- Overview of the Setup Process....131
- Step 1: Unpack and Install the Unleashed Master AP....132
- Step 2: Configure Your Unleashed Network....132
- Step 3: Customize Your Wireless LANs....158
- Step 4: Deploy Additional Unleashed Member Access Points....161

Overview of the Setup Process

The following steps are required for setup and configuration of a RUCKUS Unleashed wireless network.

1. Step 1: Unpack and Install the Unleashed Master AP on page 132
2. Step 2: Configure Your Unleashed Network on page 132
3. Step 3: Customize Your Wireless LANs on page 158
4. Step 4: Deploy Additional Unleashed Member Access Points on page 161
5. Begin Using Your RUCKUS Unleashed Network!

FIGURE 30 RUCKUS Unleashed Setup Overview



NOTE

For a video presentation of this setup process, see the RUCKUS Training video Installing the Unleashed Master AP.

Step 1: Unpack and Install the Unleashed Master AP

1. Choose which Unleashed AP will become the Unleashed Master AP (the AP that performs all of the control functions of your Unleashed network). Any Unleashed AP can be the Master.

   NOTE
   Do NOT connect multiple APs to power and the network all at once. In the initial setup stage, you should choose one AP as the Master AP and connect it to the network and power, and then complete the initial setup steps on this Master AP before connecting any other APs. Once setup is complete, you can continue connecting other APs to power and the network.

2. Perform the hardware installation according to the instructions in the *Unleashed Access Point Quick Setup Guide* that is included in the box with each Unleashed AP.
3. Once powered on and connected to the local network, the Unleashed AP boots up and begins broadcasting a temporary unencrypted WLAN named "ConfigureMe-[xxxxxx]".

   NOTE
   DNS-spoof is enabled on the AP to intercept DNS queries and respond with the Master AP's IP address. Clients associated to this temporary WLAN do not have Internet access.

Step 2: Configure Your Unleashed Network

Unleashed can be deployed using either a Mobile App (available for iOS and Android), or using your PC's web browser.

Beginning with release 200.7, Unleashed initial setup can also be performed using the command line interface (CLI).

Refer to the relevant section depending on which method you prefer to use:

Step 2a: Setup Using the Mobile App

To perform setup using the Mobile App, download the iOS or Android app from your app store.

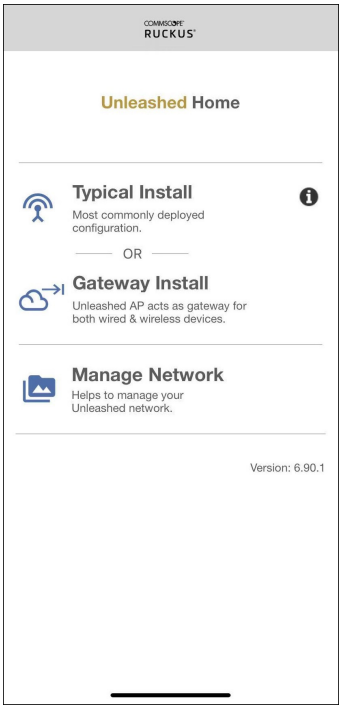
As soon as the AP is powered on and connected to the local network, it boots up and begins broadcasting a temporary unencrypted WLAN named "Configure.Me-[xxxxxx]" from both radios.

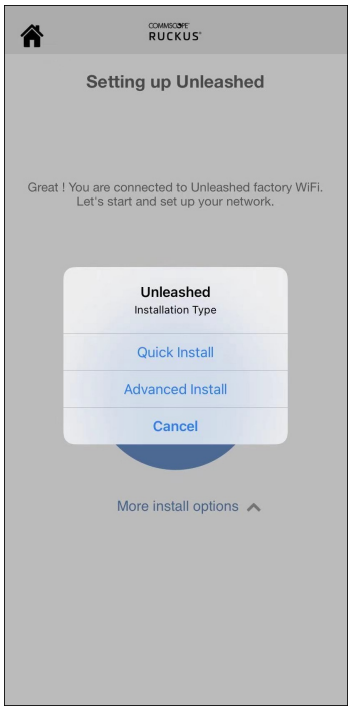
1. Using your client's Wi-Fi connection settings, select and associate to the "Configure.Me-[xxxxxx]" WLAN.

2. Launch the app, and follow the on-screen instructions to configure your RUCKUS Unleashed networks.

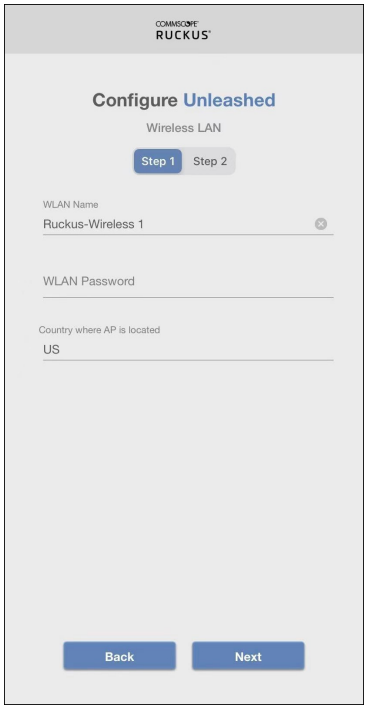
   For a quick installation, click **Typical Install** > **Start** > **Quick Install**.

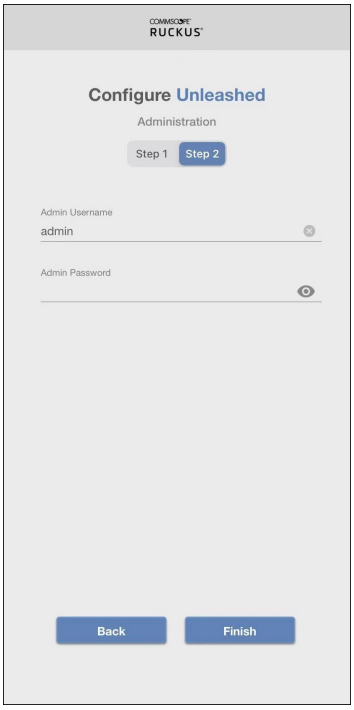
   FIGURE 31 RUCKUS Unleashed Mobile App for iOS and Android

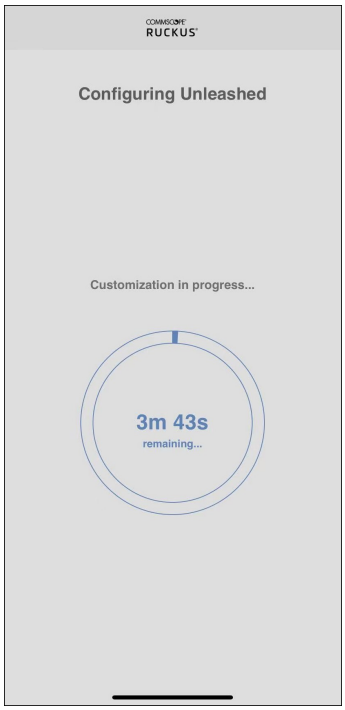




To configure RUCKUS Unleashed, in the **Wireless LAN** page, enter WLAN name, password, and the country where the AP is located, and click **Next**. In the **Administration** page, enter admin username and password, and click **Finish**.






RUCKUS
Configuring Unleashed
Customization in progress...
3m 43s
remaining...

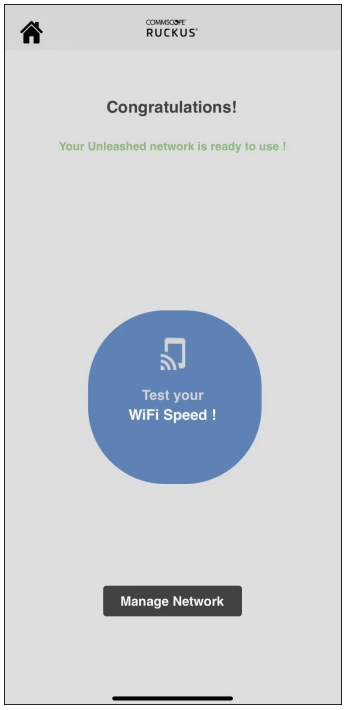
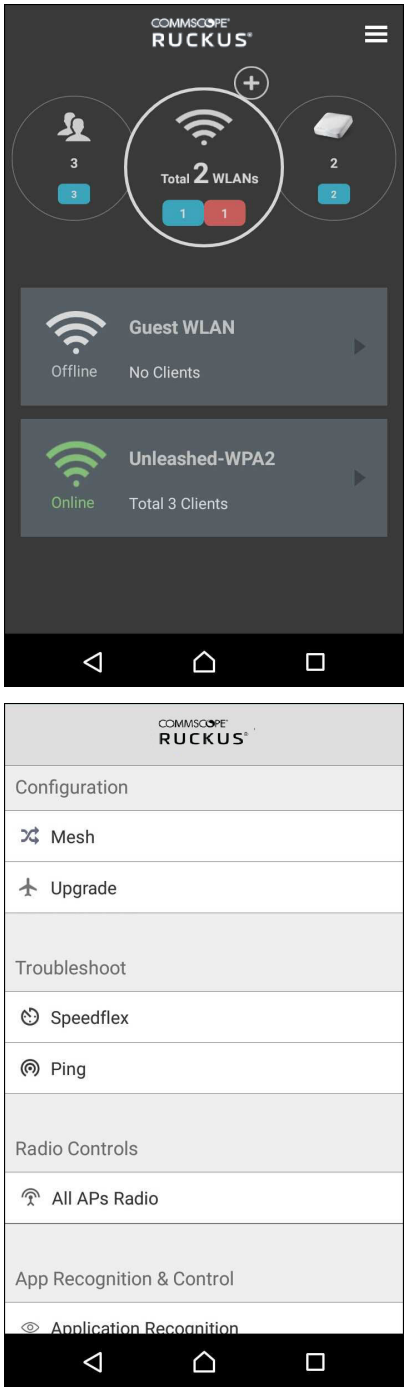

RUCKUS
Congratulations!
Your Unleashed network is ready to use !
Test your
WiFi Speed !
Manage Network

FIGURE 32 Configuring RUCKUS Unleashed from the Mobile App for iOS and Android



Step 2b: Setup Using a Web Browser

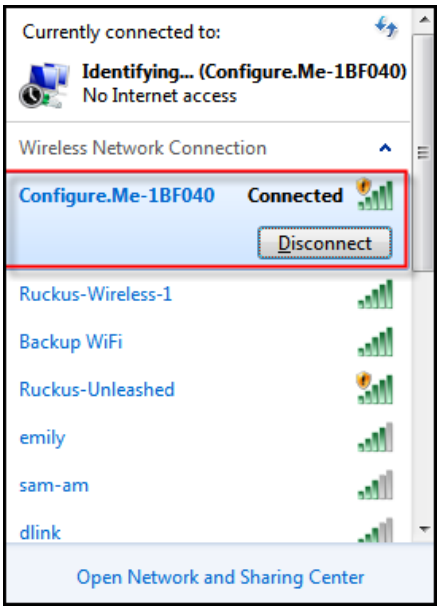
To perform setup using a web browser, connect to the RUCKUS Unleashed setup network using any Wi-Fi capable client device.

1. Using your the Wi-Fi configuration settings on your client device (such as a laptop or mobile device), select and associate to the **Configure.Me-[xxxxxx]** WLAN, and launch a web browser.

   NOTE
   Only R750 AP or R850 AP support Dedicated Master mode.

2. In your browser's URL bar, enter the following address and press **Enter**: unleashed.ruckuswireless.com.

FIGURE 33 Connecting to "Configure.Me-[xxxxxx]" WLAN, then launch a web browser

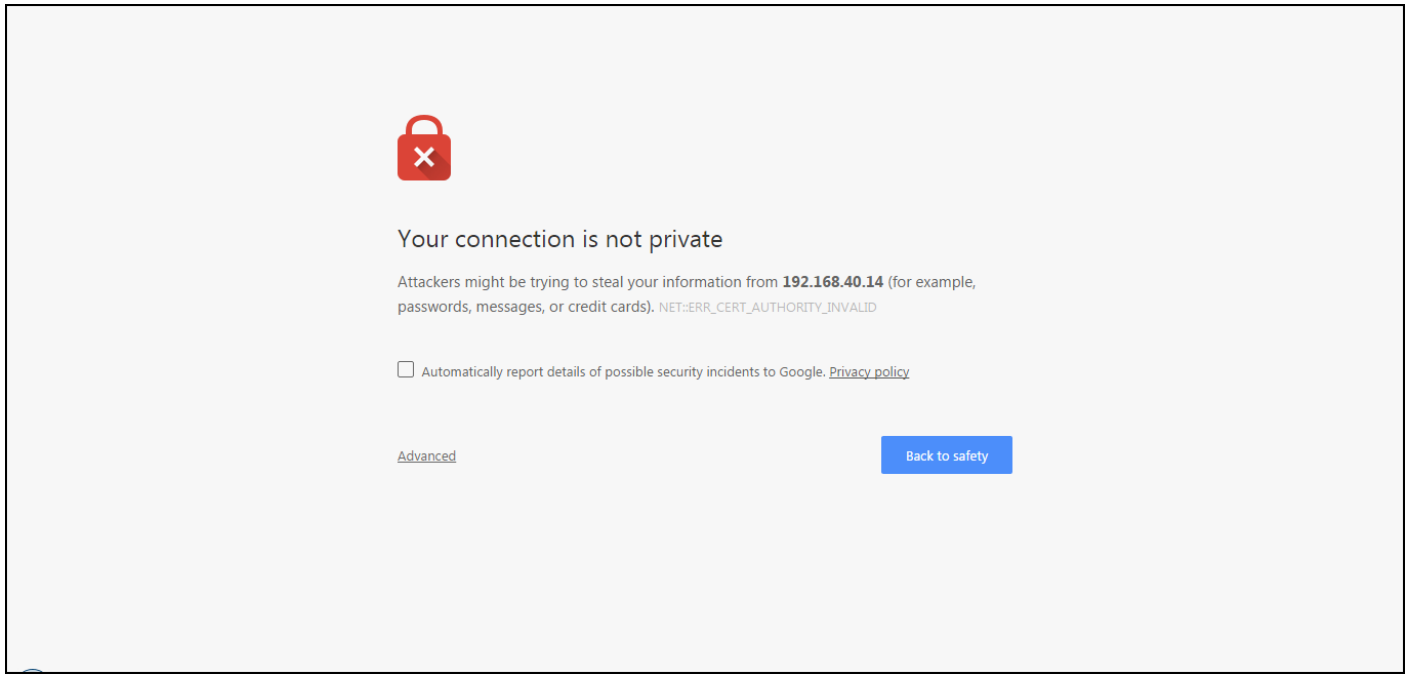


Depending on your browser, you may be presented with one of the following security warnings:

- This connection is not trusted (Firefox)
- Your connection is not private (Chrome)
- There is a problem with this website's security certificate (Internet Explorer)

This is normal, as the RUCKUS Unleashed AP does not have an SSL certificate that is recognized by your browser.

FIGURE 34 Security Warning (Chrome)

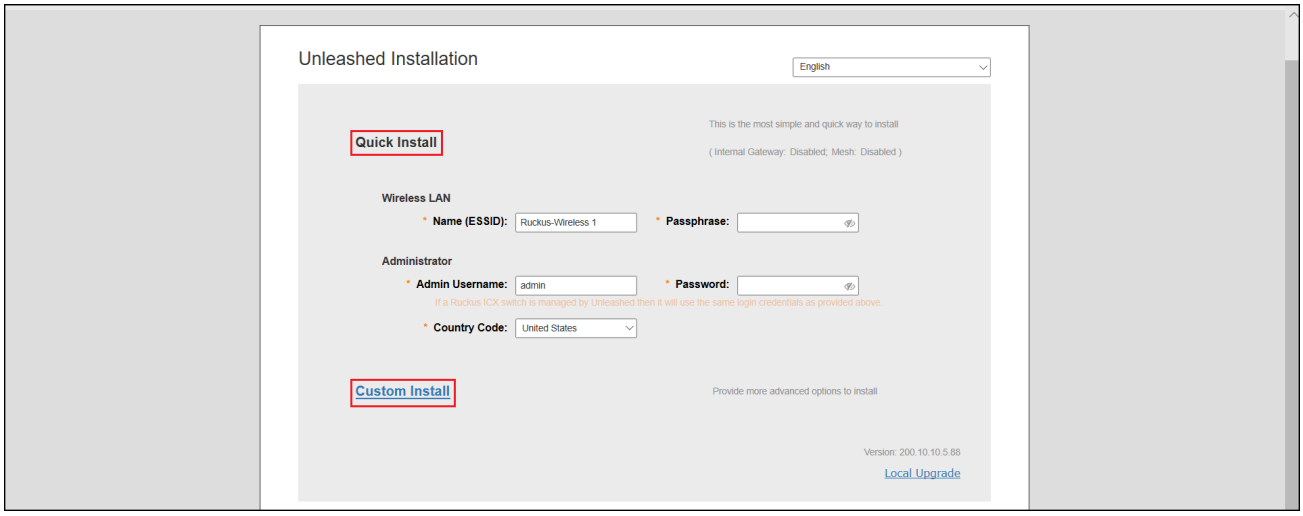


3. In response to the security warning, complete one of the following processes:
   - Click **I Understand the Risks > Add Exception... > Confirm Security Exception** (Firefox)
   - Click **Advanced > Proceed to [IP address] (unsafe)** (Chrome)
   - Click **Continue to this website (not recommended)** (Internet Explorer)

   You will be redirected to the *Setup Wizard*, which guides you through the process of setting up the Master AP.

4. Work through the Setup Wizard and check your configuration choices on the final page, before clicking **Finish** to complete the setup.
   a) On the first page of the wizard, select your language from the menu.
   b) Under **Quick Install**, fill in the following options:
      - Under **Wireless LAN**, enter the name (ESSID) and password.
      - Under **Administrator**, enter the admin username and password.
      - Under **Country Code**, select a country.

   FIGURE 35 Installation Page



NOTE
Click **Custom Install** for other installation options. For more information, refer to Advanced Install on page 140 and UMM Install on page 150. For information on **Local Upgrade** options, refer to Installation with Local Upgrade on page 152.

Advanced Install

Advanced Install is the typical way to install if you do not want to use UMM.

1. On the first page of the **Installation** window, select **Custom Install** > **Advanced Install**.

2. On the **System** page, complete the following steps:
   a) Enter a name for the Unleashed system. This system name can be used to identify the Unleashed device on your local area network.
   b) Select your country code from the menu.

      NOTE
      The **Country Code** option is not displayed if the AP is shipped from the factory with a fixed country code.

   c) If you want to enable Mesh networking for your Unleashed network, select the **Mesh** check box. Refer to Mesh Networking on page 399 for more information.

      NOTE
      If the Unleashed AP does not support Mesh (for example, the R310), it can be configured as the Unleashed Master AP, but it will not be able to participate in the Mesh network.

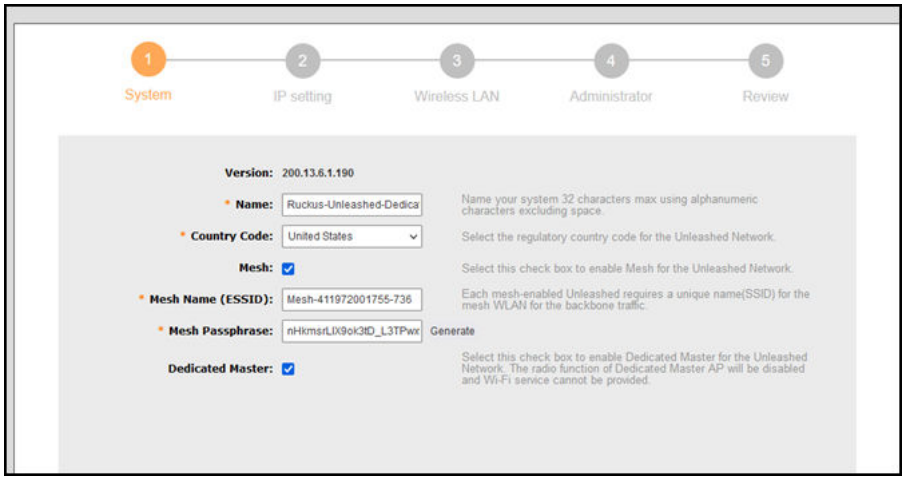
      NOTE
      If the Master AP is in Gateway mode and the WAN port is connected through PPPoE, Mesh can be enabled, but the Master AP cannot be a member of a Mesh tree; all of the other connected member APs can be part of a Mesh tree.

   d) Select the **Dedicated Master** check box if you want to enable Dedicated Master for the Unleashed network.

      NOTE
      Dedicated Master is supported only for the R750 AP and R850 AP.

   e) Click **Next** to continue.

FIGURE 36 Setup Wizard: System Page



3. On the **IP Setting** page, select whether the AP will serve as a gateway using one Ethernet port as a WAN port (connected to a cable or DSL modem, PPPoE connection, and so on), and the other as a LAN port.

   NOTE
   If your modem or router already provides gateway functionality, do not enable Gateway mode on the Unleashed Master AP. For more information, refer to Gateway Mode on page 376.

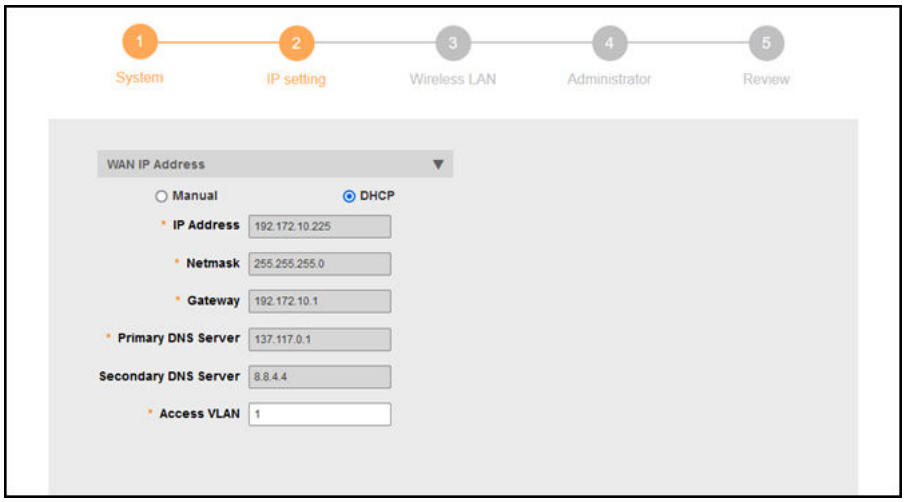
   a) Select whether to assign a manual IP address or allow the system to obtain an IP address automatically using DHCP. The default is **DHCP** (Dynamic).

      NOTE
      If you plan to manually assign and maintain IP addresses for your wireless network, select **Manual** (Static) and enter the IP address of your Unleashed Master AP. Ensure that the IP address is outside the range assigned for Wi-Fi clients. Otherwise, leave the default of **DHCP** (Dynamic) and let Unleashed do all the work for you.

   b) If you select **Manual**, enter an IP address, netmask, gateway address, and DNS server addresses in the fields provided.

      NOTE
      Optionally, if a manual IP address is configured, you can enable the built-in DHCP Server to provide IP addresses to clients on the Unleashed subnet. For more information, refer to DHCP Server on page 382.

   FIGURE 37 Setup Wizard: IP Setting Page



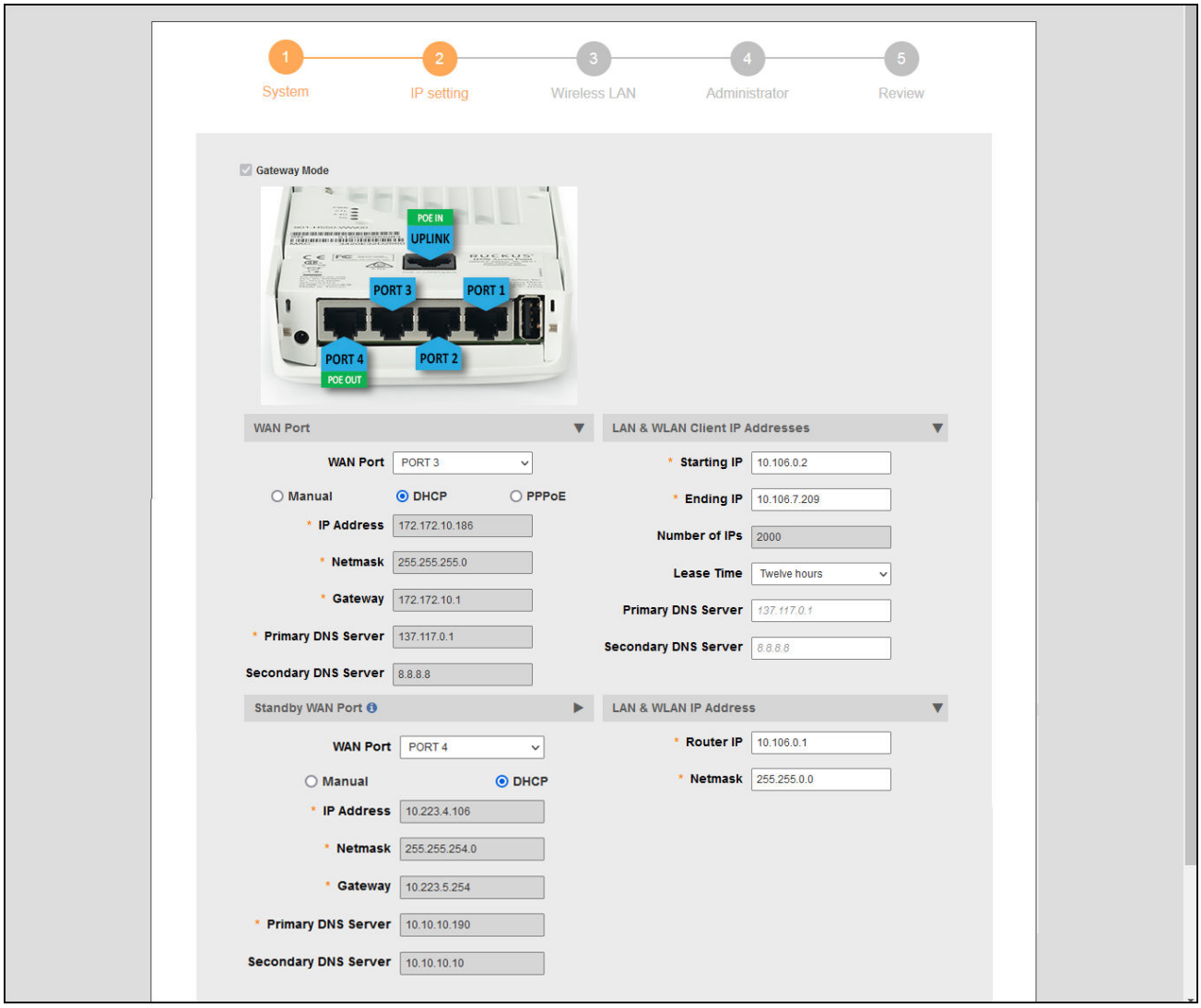
   c) Enter the access VLAN ID for Dedicated Master and click **Next**.

      NOTE
      The default value of the access VLAN ID is 1.

   d) If Gateway mode is enabled, select whether to assign a manual IP address or allow the system to obtain an IP address automatically using DHCP or PPPoE for the WAN port, and configure the local subnet settings for the LAN port. Under **Standby WAN Port**, select whether to assign a manual IP address or allow the system to obtain an IP address automatically using DHCP. The default is **DHCP** (Dynamic). For more information on Gateway mode, refer to Gateway Mode on page 376.

      NOTE
      A standby WAN port is applicable only for the H350 AP and H550 AP.

FIGURE 38 Enabling Gateway Mode



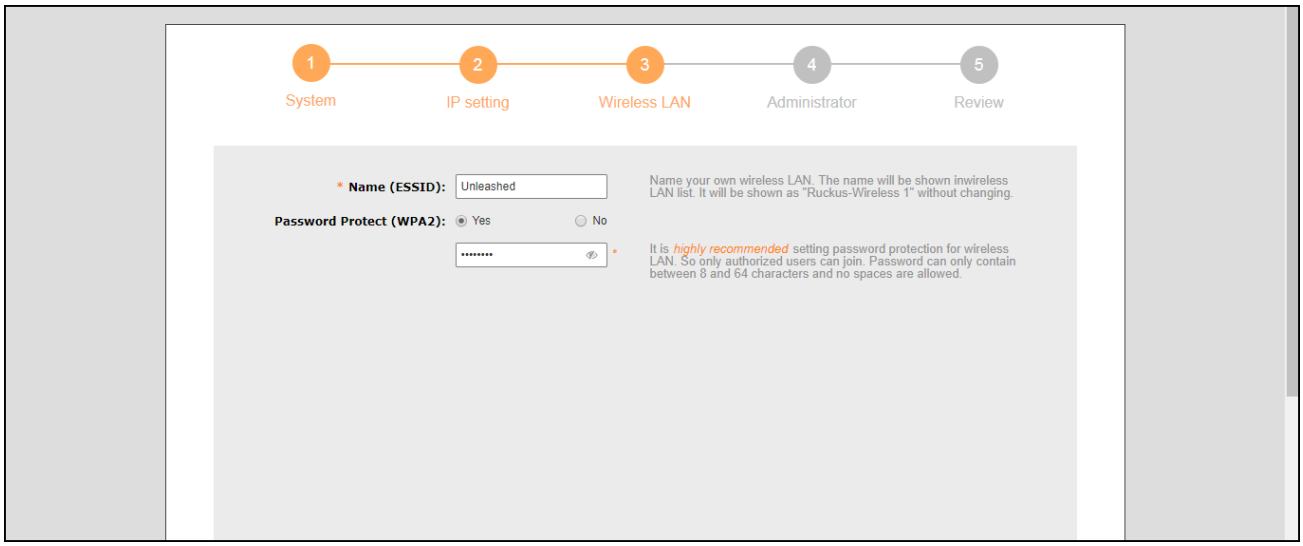
e) Click **Next** to continue.

4. On the **Wireless LAN** page, complete the following steps:
   a) In the **Name (ESSID)** field, enter a name for your first wireless LAN.
   b) For **Password Protect (WPA2)**, select **Yes** or **No**.

      NOTE
      WPA2 is highly recommended for the highest level of security.

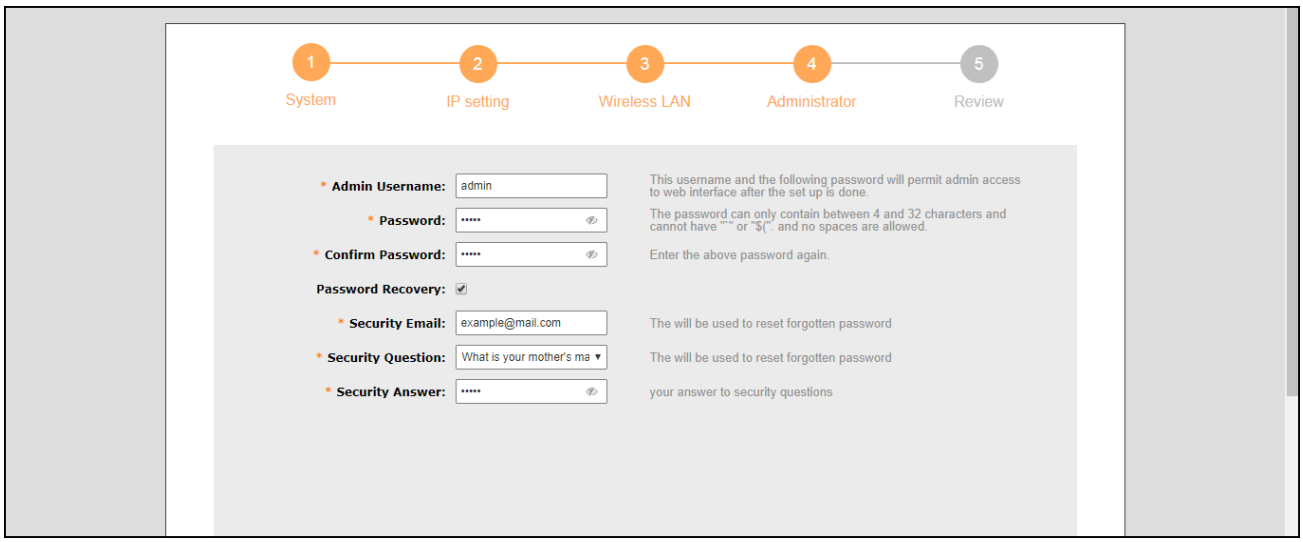
   c) If WPA2 encryption is selected, enter a password. The password must contain from 8 through 63 alphanumeric characters.
   d) Click **Next** to continue.

FIGURE 39 Setup Wizard: Wireless LAN Page



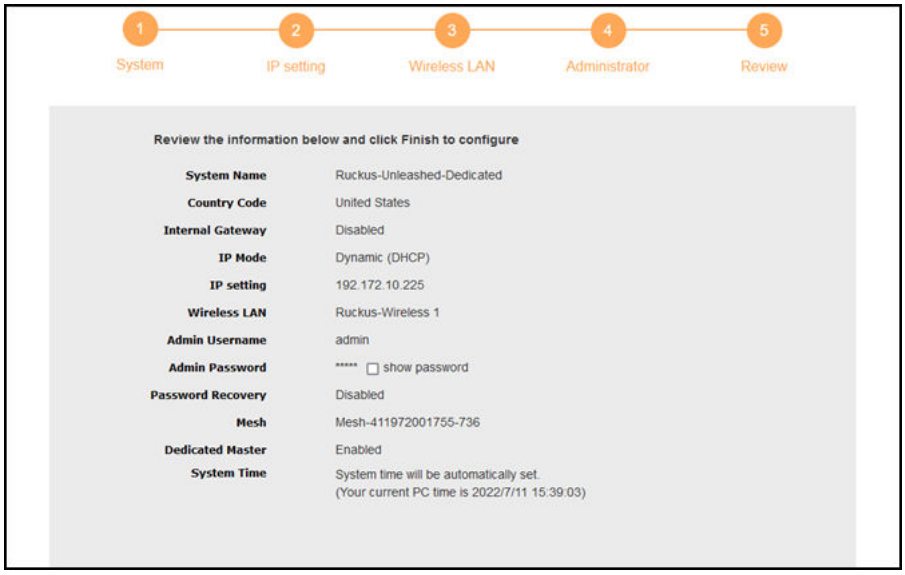
5. On the **Administrator** page, complete the following steps:
   a) Enter your admin username and password.
   b) Re-enter the password in the **Confirm Password** field.
   c) (Optional) Click the **Password Recovery** check box to allow you to reset your password in the event that your username or password is forgotten.
   d) Enter a security email address, security question, and security answer.
   e) Click **Next** to continue.

FIGURE 40 Setup Wizard: Administrator Page



6. On the **Review** page, check that all the settings you have made are correct. If any settings must be changed, click **Back** to return to the previous wizard page.

FIGURE 41 Setup Wizard: Review Page

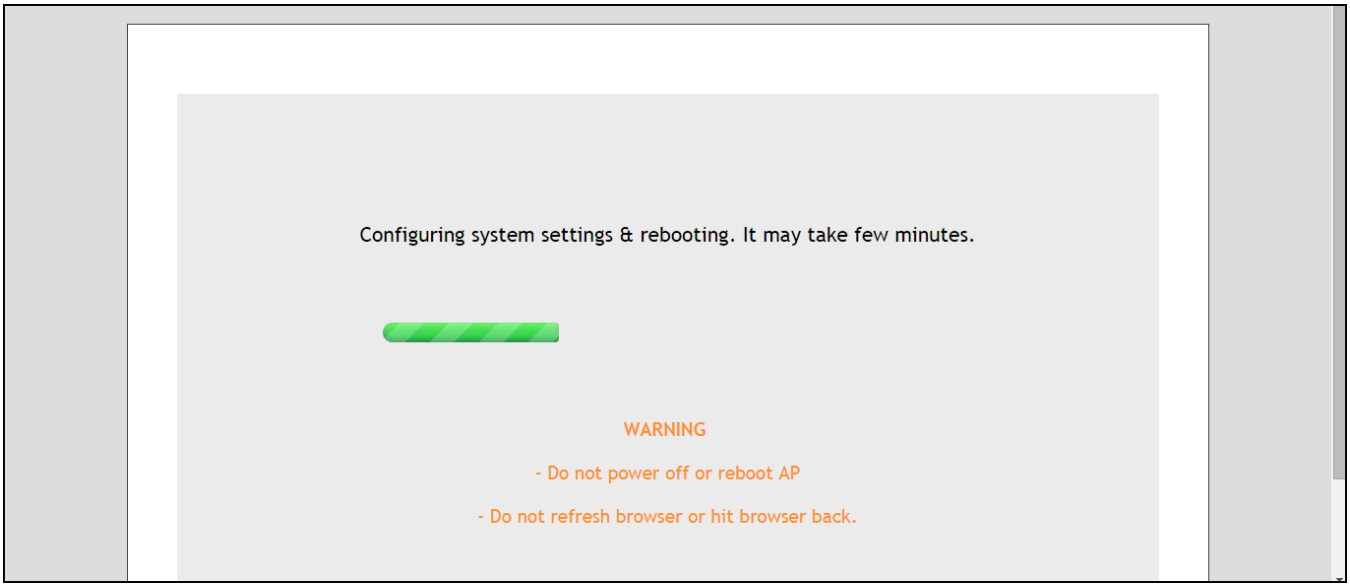


7. If you are satisfied with your choices, click **Finish** to complete the setup.

   After clicking the **Finish** button, the Unleashed Master AP reboots and a **Configuring system settings & rebooting** page is displayed. Wait for the progress screen to complete before proceeding.

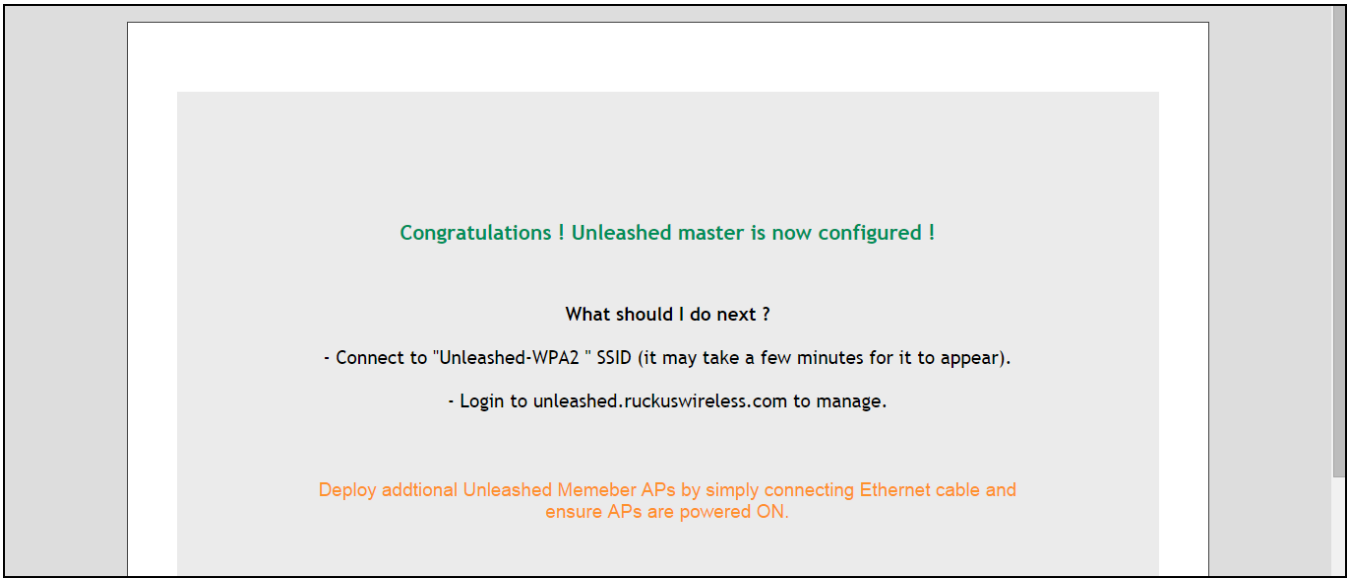
   NOTE
   Do not disconnect power or network cables during this process, and do not click Back or Refresh in your web browser.

FIGURE 42 Configuring System Settings & Rebooting Page



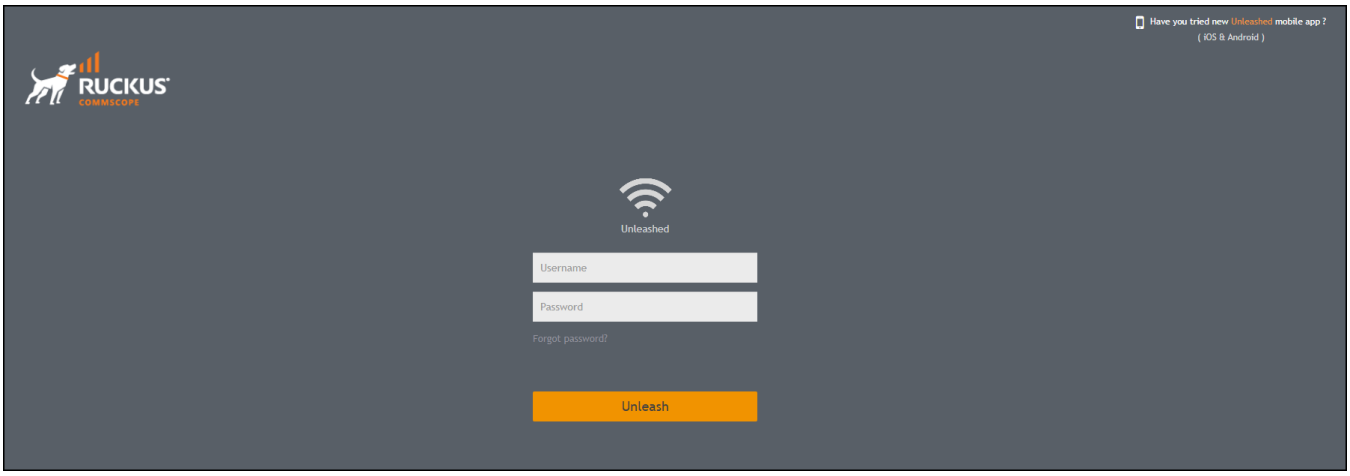
8. After setup is complete, the **Congratulations!** page is displayed. Ensure that you are connected to the WLAN that you configured, and click **Finish**. You will be redirected to the login page.

FIGURE 43 Congratulations! Page



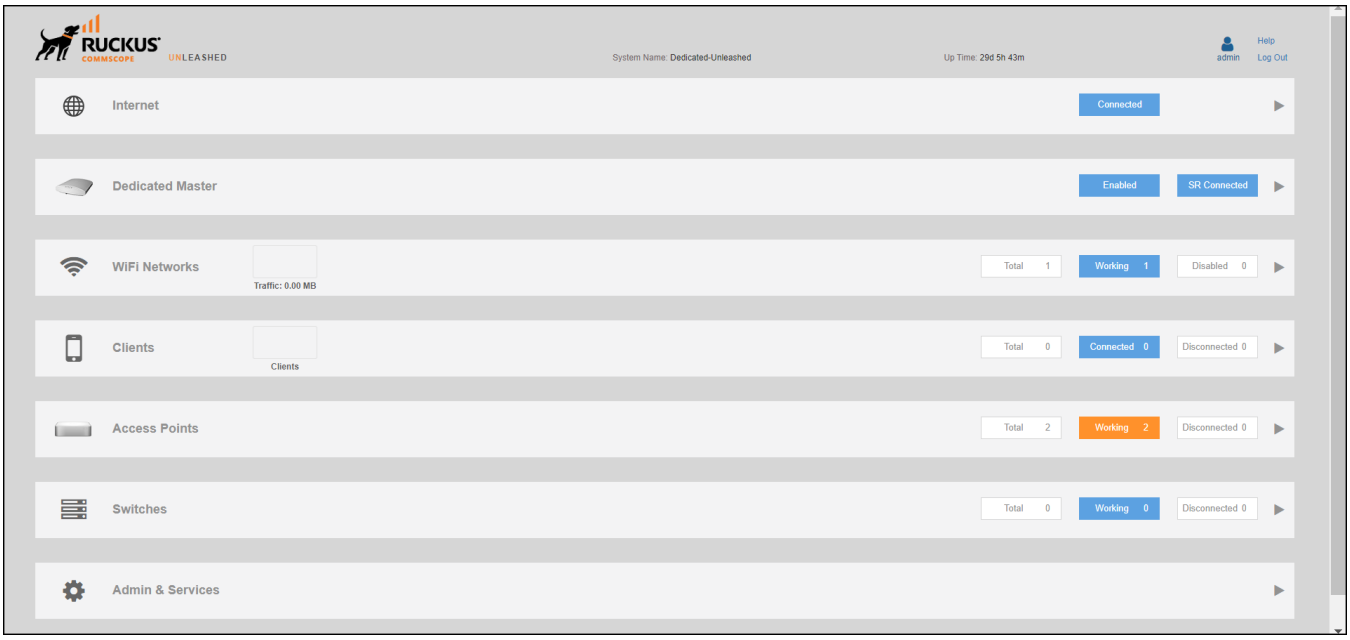
9. On the login page, enter your username and password, and click **Unleash**.

FIGURE 44 Login Page



After a successful login, the **Unleashed Dashboard** displays an overview of your RUCKUS Unleashed network.

FIGURE 45 Unleashed Dashboard



10. Continue to Step 3: Customize Your Wireless LANs on page 158.

UMM Install

If an Unleashed Multi-Site Manager (UMM) server is available, you can allow automatic Unleashed deployment configuration by running a configuration template from the UMM server to the Unleashed Master AP during setup.

To enable UMM easy deployment:

1. On the second page of the installation wizard, select **UMM Install**.
2. Enter the **UMM Domain/IP** address.
3. Enter the **Config Template Name** of the deployment configuration template configured on UMM for the Unleashed network.
4. Click **Next**. The Unleashed AP attempts to connect to the UMM server to retrieve the configuration template.

5. If successful, the configuration template is pushed to the AP and the Unleashed deployment is configured according to the template.

FIGURE 46 UMM Install

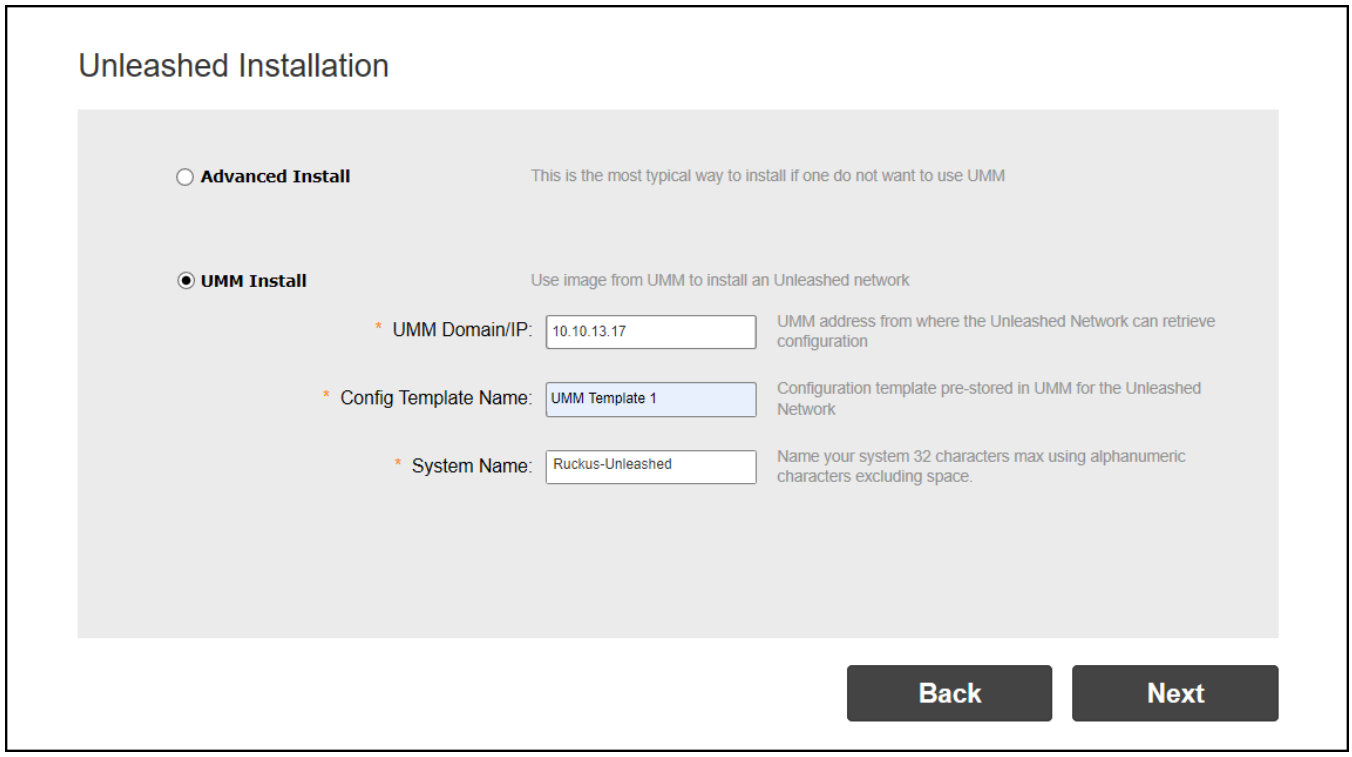
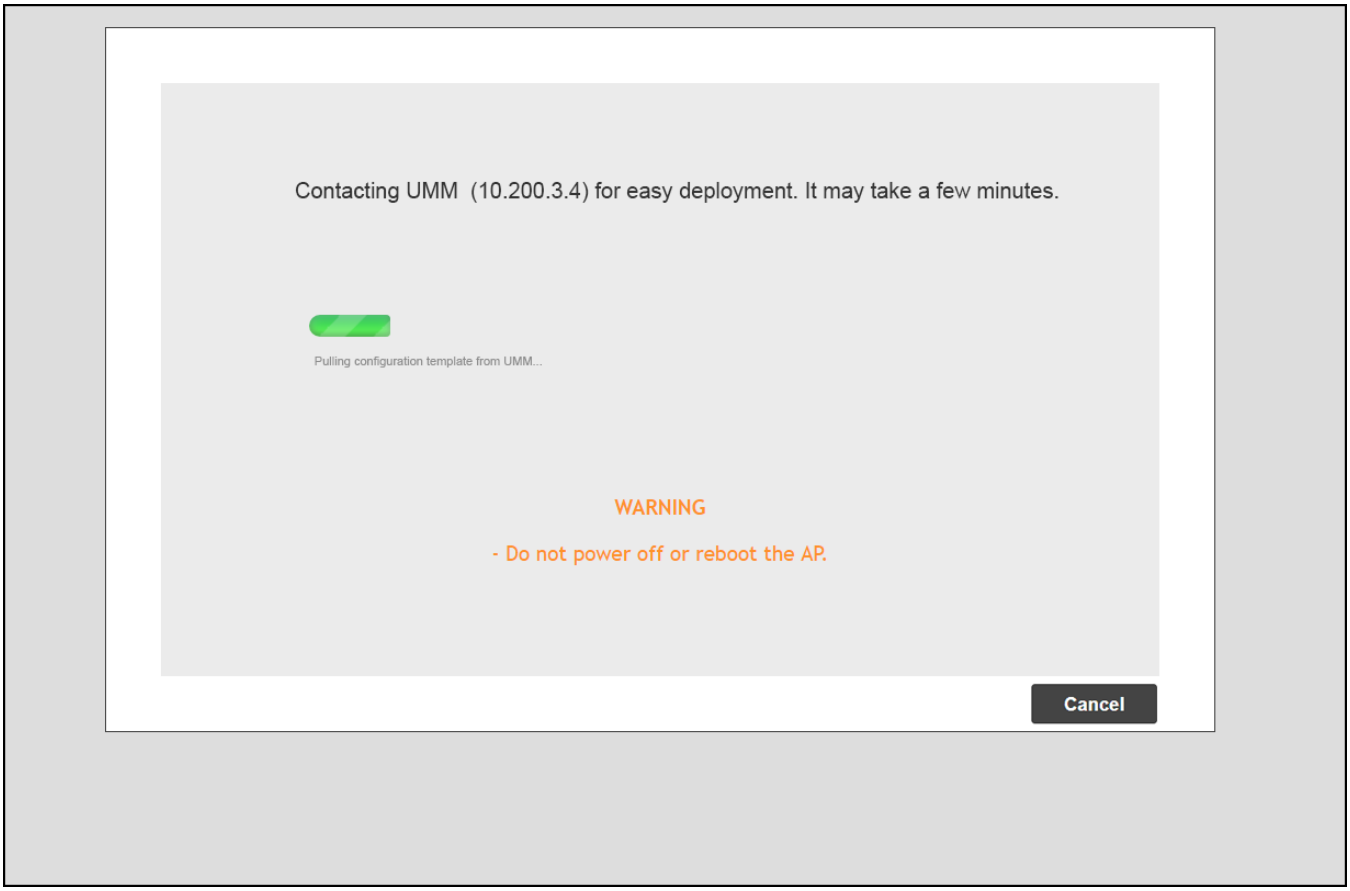


FIGURE 47 Contacting UMM for Easy Deployment



Installation with Local Upgrade

The Local Upgrade option during the installation settings allows the admin to upgrade the RUCKUS Unleashed firmware to a newer release build prior to deployment.

To perform a local upgrade before completing the RUCKUS Unleashed setup:

1. On the first page of the setup wizard, select **Local Upgrade**. The *Local Upgrade* page appears.
2. Click **Choose File** and select the locally stored RUCKUS Unleashed image file.
3. Click **Upgrade**.

4. When complete, click **Reboot** to reboot the AP and restart the installation process using the new firmware.

FIGURE 48 Local Upgrade - Installation Page

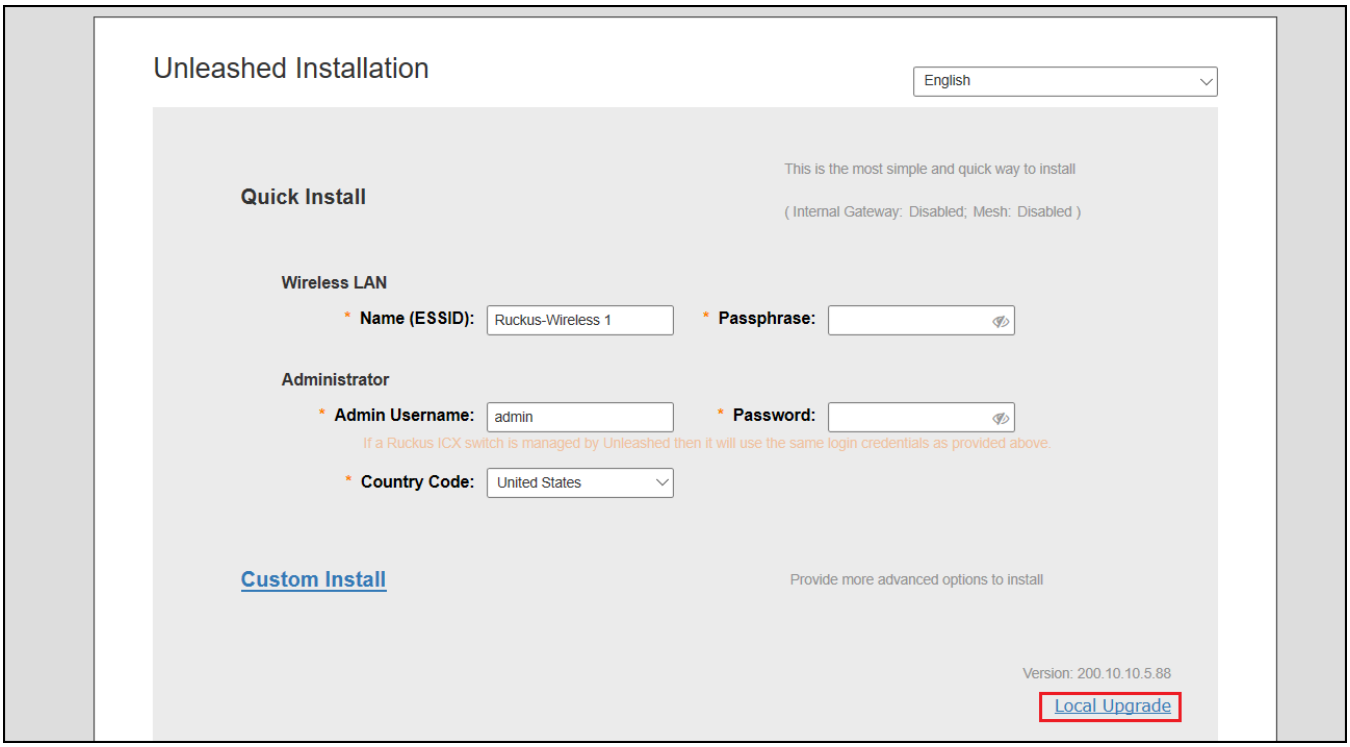
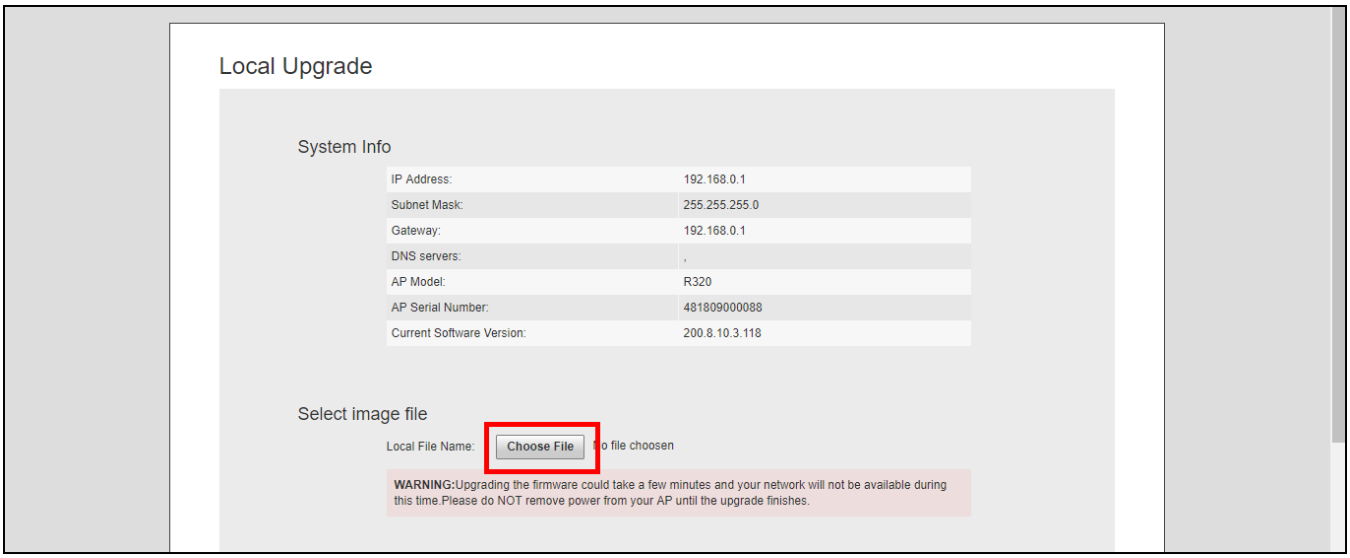


FIGURE 49 Choose Local Image File to Upgrade



Step 2c: Setup Using the Command Line Interface

The CLI setup wizard allows you to quickly configure your Unleashed Master AP with basic settings using a short series of CLI commands.

To perform Unleashed setup using CLI commands, use the following procedure:

1. When the Unleashed AP is in factory default state, associate to the "Configure.Me-xxxxxx" WLAN and connect to the Unleashed CLI using SSH (default IP address: **unleashed.ruckuswireless.com** or **10.154.231.125**), and log in using the default user name and password:
   - Please login: **super**
   - Password: **sp-admin**

     NOTE
     For information on using the Unleashed CLI, see the *Unleashed Command Line Interface Reference Guide*, available from *support.ruckuswireless.com*.

   The Unleashed CLI Wizard Configuration Tool starts automatically.

2. Follow the instructions in the setup wizard to configure your Unleashed Master AP. The following are two examples.

Configure Unleashed AP to Bridge Mode

```
Please login: super
Password: ********


Welcome to Ruckus Wireless Unleashed CLI Setup Wizard


Would you like to start the Setup Wizard? [yes/no]: yes

Enter the way of installation. 1. easy-deployment installation 2. local wizard [1/2] 2

Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****

Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed

Enter Country Code (or 'help' to show the list) [US]: US

Enable Mesh [yes/NO]? no

Enable Gateway Mode [yes/NO]? no

Enable Dedicated Master [yes/NO]? no

Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
1

Enter Access VLAN [1]: 1

Enable WLANs [YES/no]? yes

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Unleashed-SSID
Is it an Open WLAN [yes/NO]? no
Enter the WPA2 Passphrase (8-63 characters): ********
Re-enter the WPA2 Passphrase (8-63 characters):
********

Please review the following settings:
System Name=                Unleashed
Administrator Name=         admin
Country Code=               US
Mesh Supported=             Disable
Gateway Mode Supported=     Disable
Dedicated Master Supported= Disable
IPv4 Mode=                  DHCP
Access VLAN=                1
WLAN ESSID=                 Unleashed-SSID
Wireless Authentication=    WPA2_PSK


Done with the Setup Wizard [yes/no]? yes

Save the configuration ...


It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface
```

```
ruckus>
```

Configure Unleashed AP in Dedicated Mode

```
Please login: super
Password: ********


Welcome to Ruckus Wireless Unleashed CLI Command Line Interface


Would you like to start the Setup Wizard? [yes/no]: yes

Enter the way of installation:

1. easy-deployment installation.(Warning: The configuration costs about 15 seconds to store in
system, and in flash empase the device may be damaged if power-off. So please avoid rebooting device
after 60 seconds if network is reachable)

2. local wizard

please enter 1 or 2:
2

Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****

Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed

Enter Country Code (or 'help' to show the list) [US]: US

Enable Mesh [yes/NO]? yes

Enable Gateway Mode [yes/NO]?

Enable Dedicated Master [yes/NO]? yes

Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
1
Enter Access VLAN [1]: 1

Enable WLANs [YES/no]?

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Dedicated-SSID
Is it an Open WLAN [yes/NO]?
Enter the WPA2 Passphrase (8-63 characters):
********
Re-enter the WPA2 Passphrase (8-63 characters):
********

Please review the following settings:
System Name=                Unleashed
Administrator Name=         admin
Country Code=               US
Mesh Supported=             Enable
Gateway Mode Supported=     Disable
Dedicated Master Supported= Enable
    IPv4 Mode=              DHCP
    Access VLAN=            1
WLAN ESSID=                 Dedicated-SSID
Wireless Authentication=    WPA2_PSK
```

```
Done with the Setup Wizard [yes/no]? yes


Save the configuration ...


It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface
ruckus>
```

Configure Unleashed AP to Gateway Mode

```
Please login: super
Password: ********


Welcome to Ruckus Wireless Unleashed CLI Setup Wizard


Would you like to start the Setup Wizard? [yes/no]: yes

Enter the way of installation. 1. easy-deployment installation 2. local wizard [1/2] 2

Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****

Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed-Gateway

Enter Country Code (or 'help' to show the list) [US]: US

Enable Mesh [yes/NO]? no

Enable Gateway Mode [yes/NO]? yes

Enter AP R510 WAN Port:
    1: port1, eth0, UP:
    2: port2, eth1, DOWN:
1

Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
     3: PPPOE Mode;
1

Enter LAN & WLAN IP Address [10.106.0.1]:
192.168.1.1
Enter LAN & WLAN IP Netmask [255.255.0.0]:
255.255.255.0
Enter Client Starting IP Address [10.106.0.2]:
192.168.1.2
Enter Client Ending IP Address [10.106.7.209]:
192.168.1.200

Enter Lease Time [2]:
    1: 6 hours;
    2: 12 hours;
    3: 1 day;
    4: 2 days;
    5: 1 week;
    6: 2 weeks;

1
```

```
Enable WLANs [YES/no]? yes

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Unleashed-SSID
Is it an Open WLAN [yes/NO]? no
Enter the WPA2 Passphrase (8-63 characters):
********
Re-enter the WPA2 Passphrase (8-63 characters):
********

Please review the following settings:
System Name=                Unleashed-Gateway
Administrator Name=         admin
Country Code=               US
Mesh Supported=             Disable
Gateway Mode Supported=     Enable
WAN Port=                   port1 eth0 UP
IPv4 Mode=                  DHCP
LAN Port IPv4 Address Info= 192.168.1.1/255.255.255.0
Client Starting IPv4=       192.168.1.2
Client Ending IPv4=         192.168.1.200
Lease Time=                 6 hours
WLAN ESSID=                 Unleashed-SSID
Wireless Authentication=    WPA2_PSK


Done with the Setup Wizard [yes/no]? yes

Save the configuration ...


It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface
ruckus>
```

Step 3: Customize Your Wireless LANs

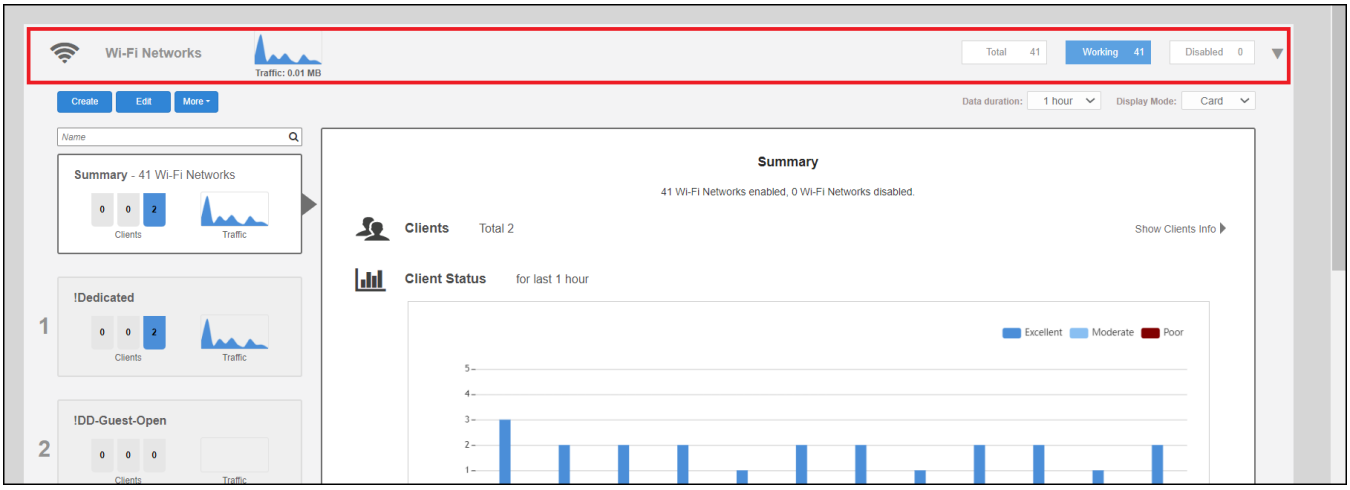
Once the Unleashed Master AP has been initialized, you can fine-tune the settings of your first WLAN (that you created during the setup wizard), and create any additional WLANs needed prior to attaching additional Unleashed member APs.

Then, when you deploy additional member APs in whatever order you prefer, they will automatically retrieve all WLAN configuration settings (and any other settings you have configured) from the Unleashed Master AP.

To customize an existing wireless LAN:

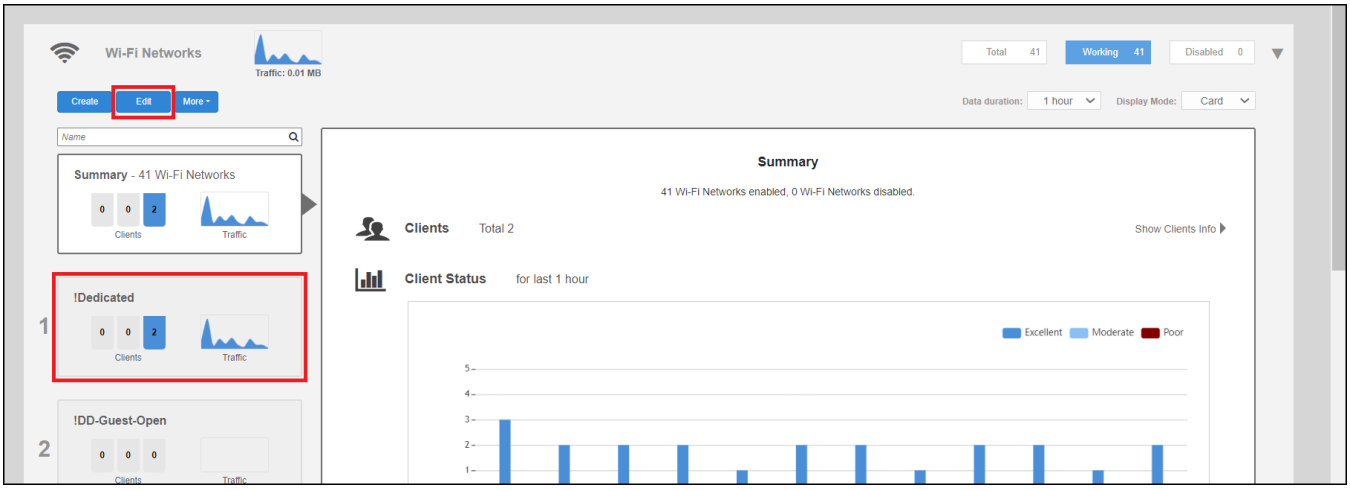
1. From the **Dashboard**, click anywhere in the **Wi-Fi Networks** section to expand the display of your deployed WLANs.

   FIGURE 50 Click the Wi-Fi networks section to expand



2. Select the WLAN box from the list on the left, and click the **Edit** button to edit the WLAN's settings.

   FIGURE 51 Select WLAN and click Edit to configure the WLAN settings

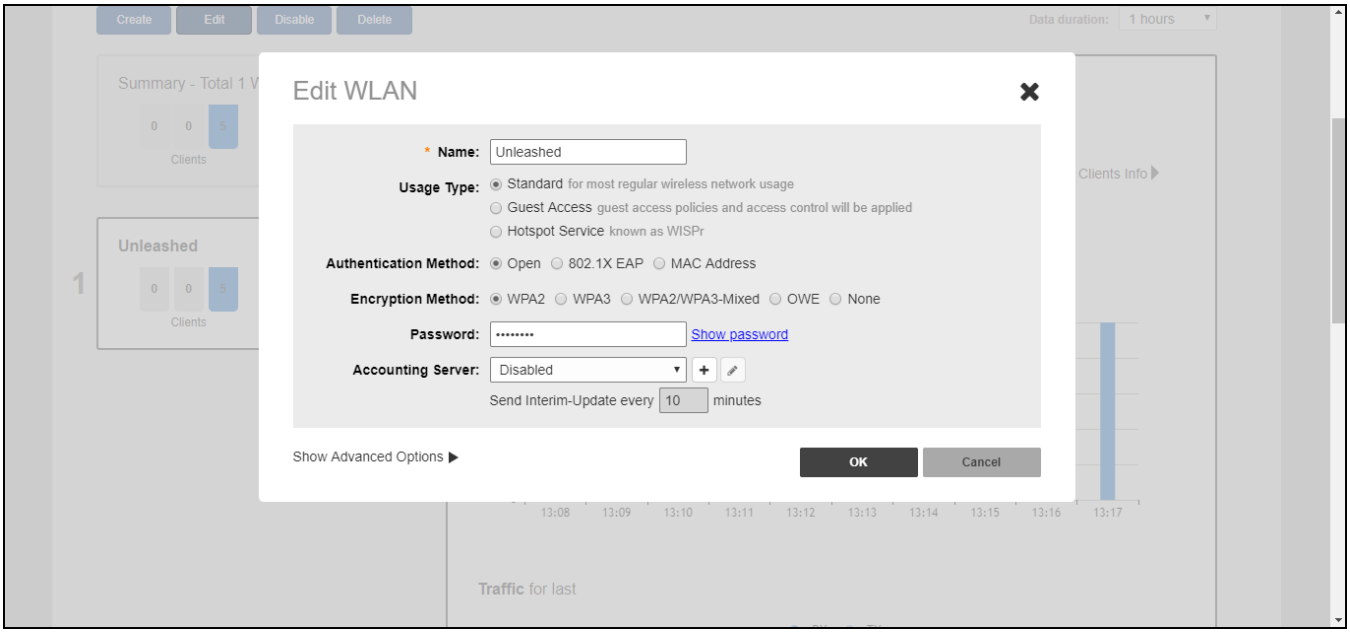


3. Configure the following WLAN settings:
   - **Name**: Enter a recognizable name for this WLAN.
   - **Usage Type**: Select Standard for most typical wireless network usage scenarios. Select Guest Access to create a Guest WLAN, or select Hotspot to create a Hotspot WLAN.
   - **Authentication**: Select Open, for open authentication, or authenticate users against an internal local database or an external authentication server using 802.1X or MAC address.
   - **Authentication Server**: Select an AAA server (or Local Database) to authenticate users when 8021.X or MAC authentication method is selected.
   - **Encryption Method**: Select WPA2 for standard wireless security. Select None for no encryption.
   - **Password**: Enter a WPA2 password for use when connecting to this WLAN if WPA2 is selected.

     NOTE
     For information on additional WLAN configuration options, see WLAN Configuration on page 189.

4. Click **OK** to save your changes.
5. Repeat for any additional WLANs you would like to create. All WLANs will be deployed to each new member AP as soon as it joins the Unleashed network.

FIGURE 52 Editing an existing WLAN



Congratulations! Your Unleashed network is now configured and ready for use. You may now proceed to Step 4: Deploy Additional Unleashed Member Access Points on page 161.

Step 4: Deploy Additional Unleashed Member Access Points

Deploying additional Unleashed member APs is simply a matter of connecting them via Ethernet to the same Layer 2 network and providing power. They will discover the Unleashed Master and join automatically. No additional steps are necessary.

The second and any additional APs that join an Unleashed network will automatically assume the role of Unleashed "member AP." Thereafter, if the Master AP goes offline, one of the member APs will become the new Master and assume control of the Unleashed network.

NOTE
When a member AP joins the Master for the first time, if it is running a different firmware version than the Master, it will automatically download and upgrade (or downgrade) itself to the correct firmware version to match that of the Master, reboot, and then rejoin the Unleashed network once the matching firmware is running.

Using the Admin Interface

- Unleashed Administration Interface Overview..... 163
- Navigating the Dashboard..... 163
- Using the Dashboard Components..... 164

Unleashed Administration Interface Overview

The Unleashed Admin Interface provides tools for use in managing all aspects of your Unleashed deployment.

It contains configuration pages for managing Internet connection status, Unleashed Access Points, ICX switches, wireless LANs, user accounts, system settings and administrator preferences.

Navigating the Dashboard

The RUCKUS Unleashed dashboard is the primary interface used for monitoring and configuring all aspects of your network. The RUCKUS Unleashed dashboard is divided into three main sections. These three main sections and their subsections are described in the following table.

FIGURE 53 RUCKUS Unleashed Dashboard

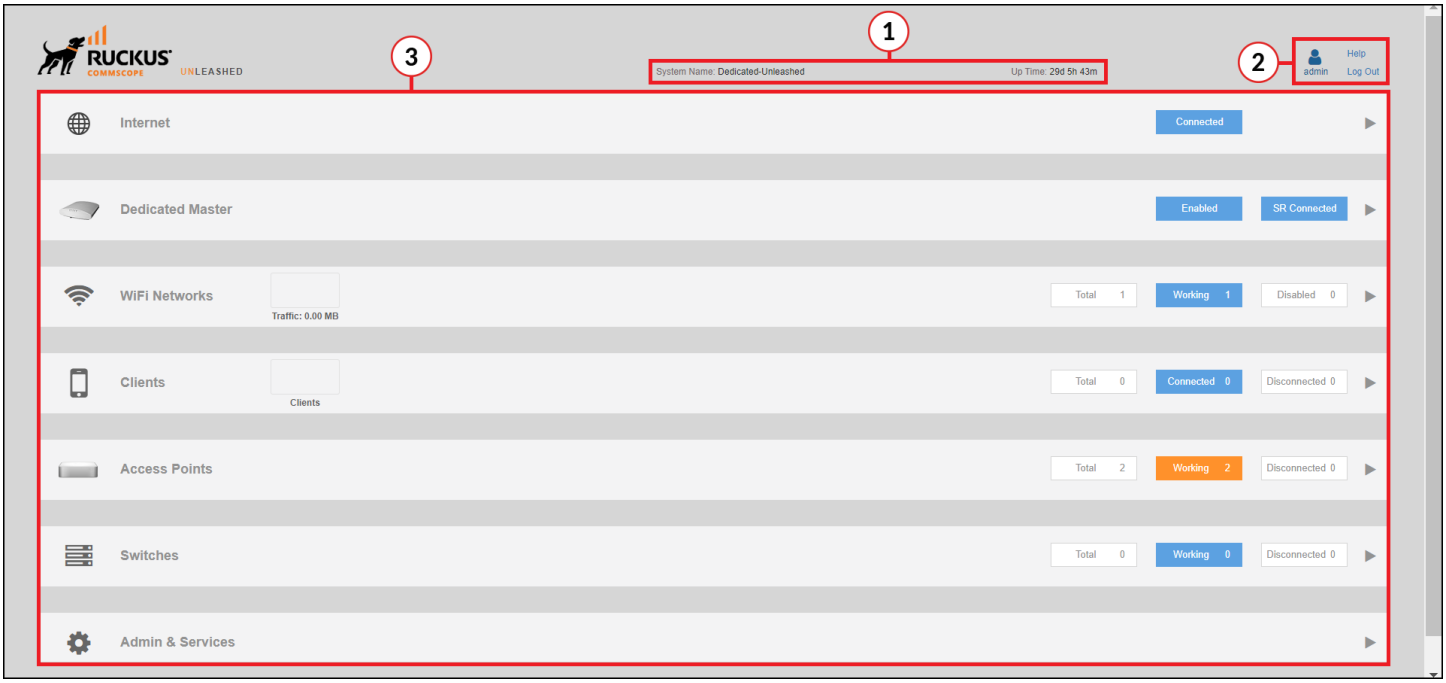


TABLE 29 Dashboard Components

Number	Component	Description
1	System Name and Uptime	Displays the system name that you configured and the uptime since the last reboot.
2	Admin Info	Displays currently logged-in Admin name, a link to this **Online Help**, and a **Logout** button.

TABLE 29 Dashboard Components (continued)

Number	Component	Description
3	Network Components	Provide general overviews of each component. Click any of the components to expand for more detailed information and configuration options. Refer to Using the Dashboard Components on page 164.

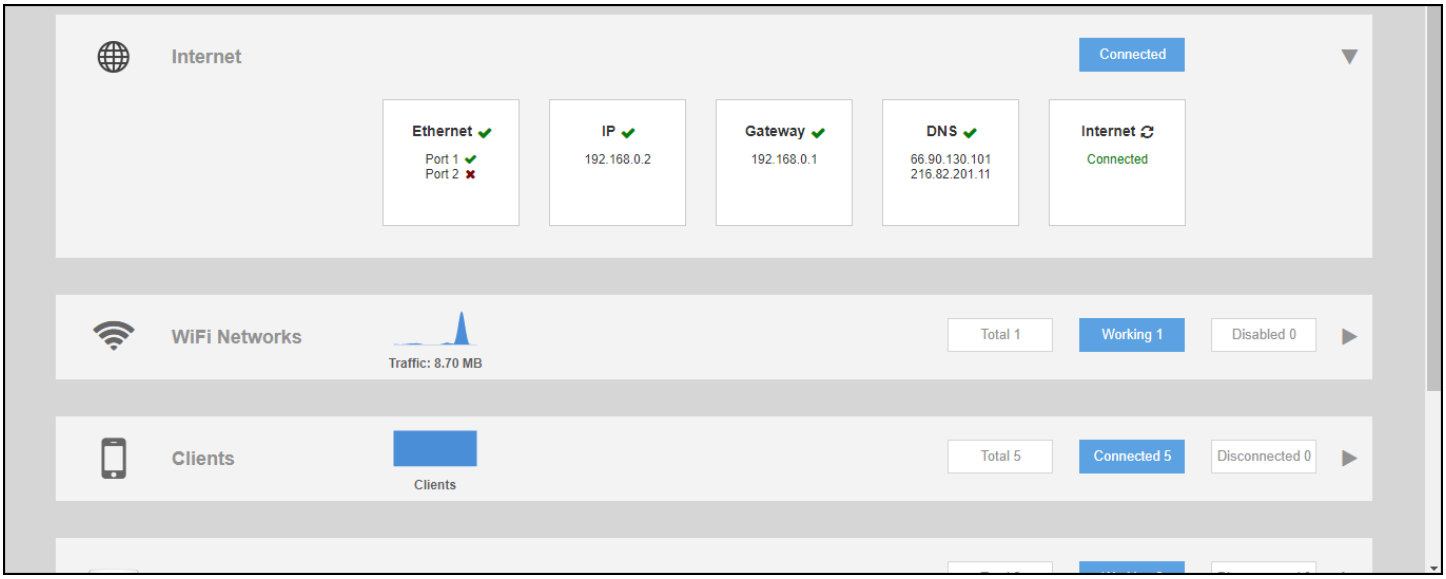
Using the Dashboard Components

Each of the Dashboard components can be expanded by clicking the component name to display more detailed information and links to configuration options for that component.

Internet

The **Internet** component provides details on the Master AP's upstream connection to the Internet, including IP address, DNS servers, Gateway address, and the Ethernet port being used as the WAN port.

FIGURE 54 Internet Component



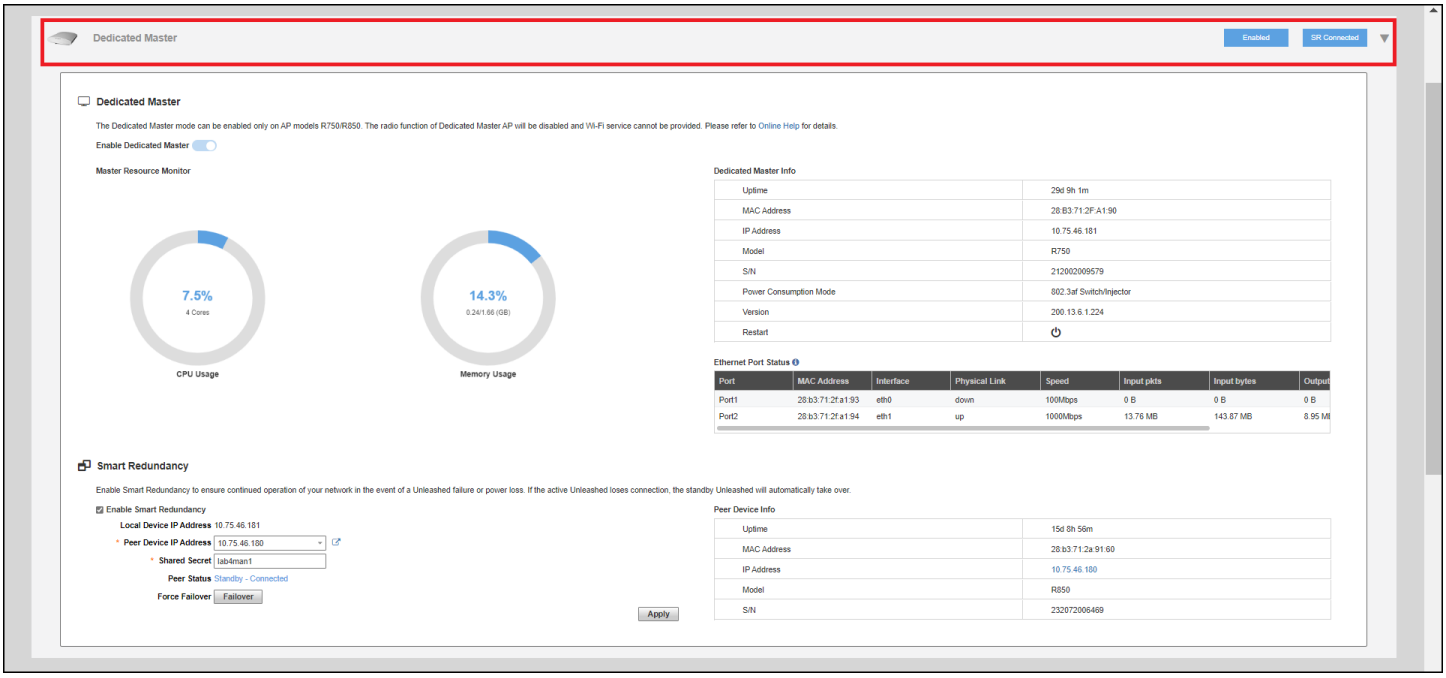
The Internet connection status indicator is not displayed if the "internet-check" feature has been disabled using a CLI command.

Dedicated Master

The **Dedicated Master** component displays status and information about Dedicated Master and Smart Redundancy.

> **NOTE**
> The **Enable Dedicated Master** option can be enabled only when the Master AP is an R750 AP or R850 AP.

FIGURE 55 Dedicated Master Component

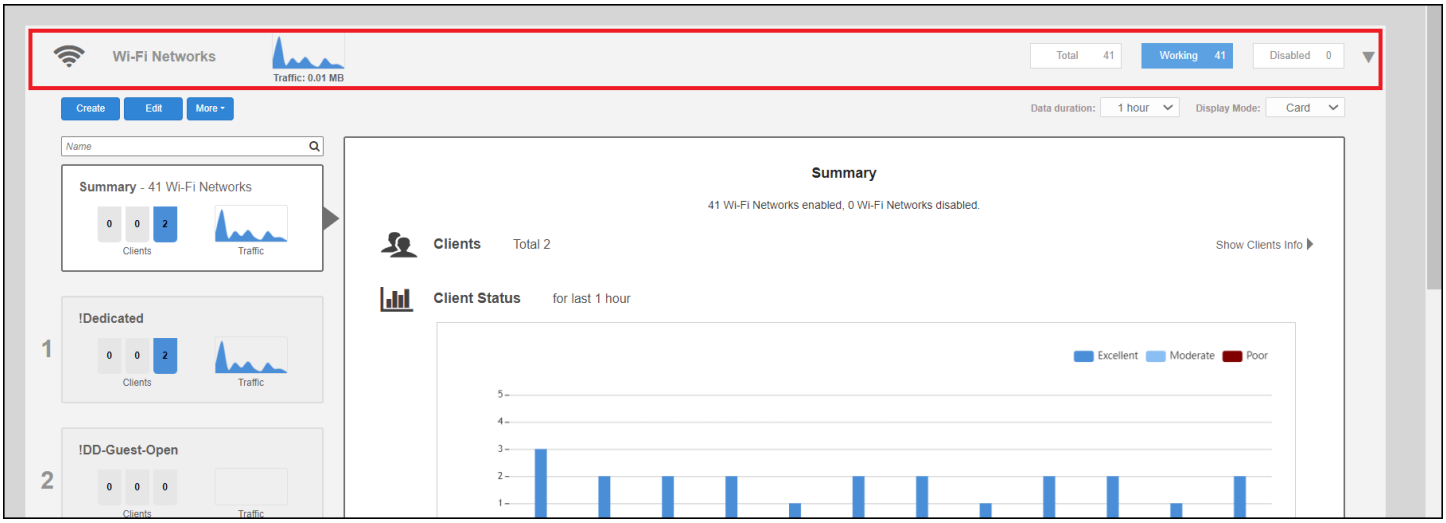


WiFi Networks

The **WiFi Networks** component displays an overview of the wireless LANs that you have deployed. It displays the total number of wireless LANs, the number that are currently in the Working state, and those that are in the Disabled state.

Each of the three categories can be selected to view a detailed list of the WLANs in the Total, Working, or Disabled category.

FIGURE 56 WiFi Networks Component

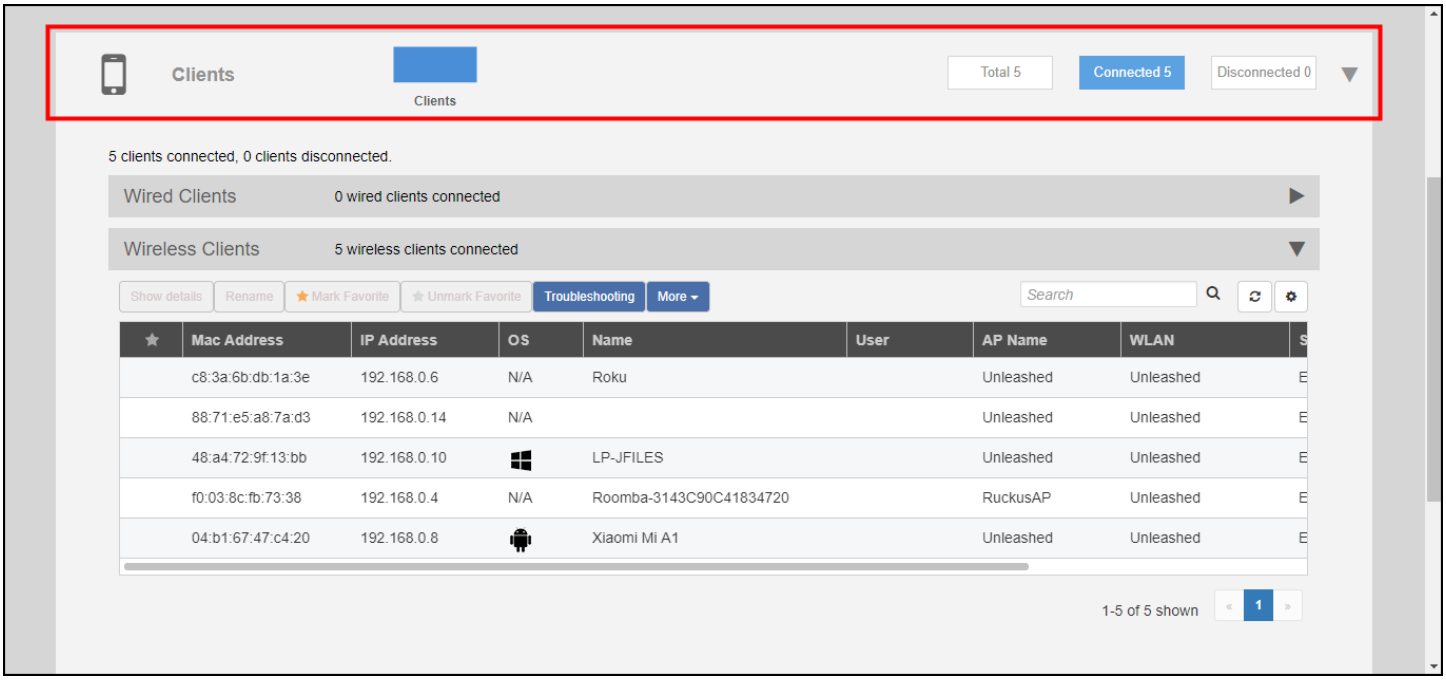


Clients

The **Clients** component provides an overview of the number of Total, Connected, and Blocked clients.

The Clients sub-component provides additional options to search for a client by MAC address, to show details on a client, to temporarily delete a client, or to permanently block a client.

FIGURE 57 Clients Component



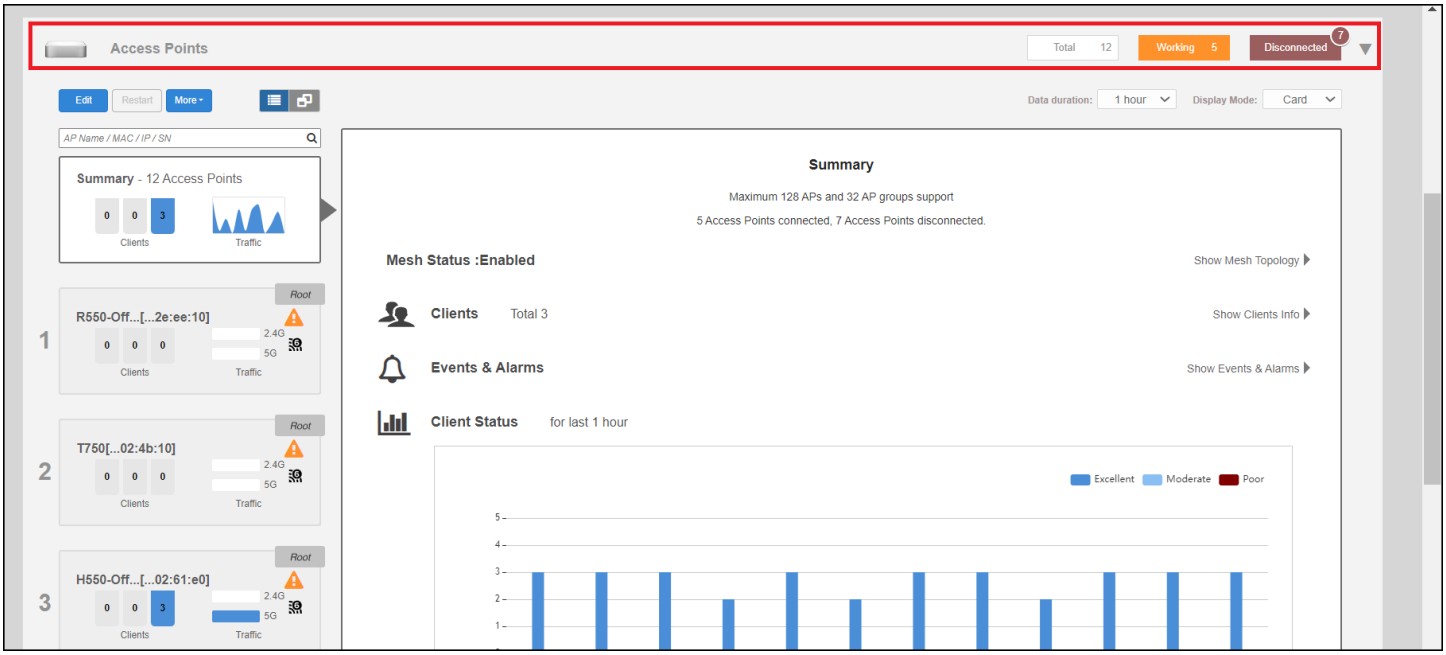
Access Points

The **Access Points** component provides an overview of the APs in your network, and is divided into three subsections: *Total*, *Working* and *Disconnected*. Click any of the three subsection buttons to expand the Access Points component and display a list of APs in that category.

The **Access Points** component displays a list of all of the APs being managed by your Master AP. The list includes all APs, including the Master AP itself, currently connected member APs, as well as any APs that have previously joined but are currently disconnected.

Each AP (whether working or disconnected) is represented by one of the large boxes on the left side of the screen. Click one of the AP boxes to display details about that specific AP.

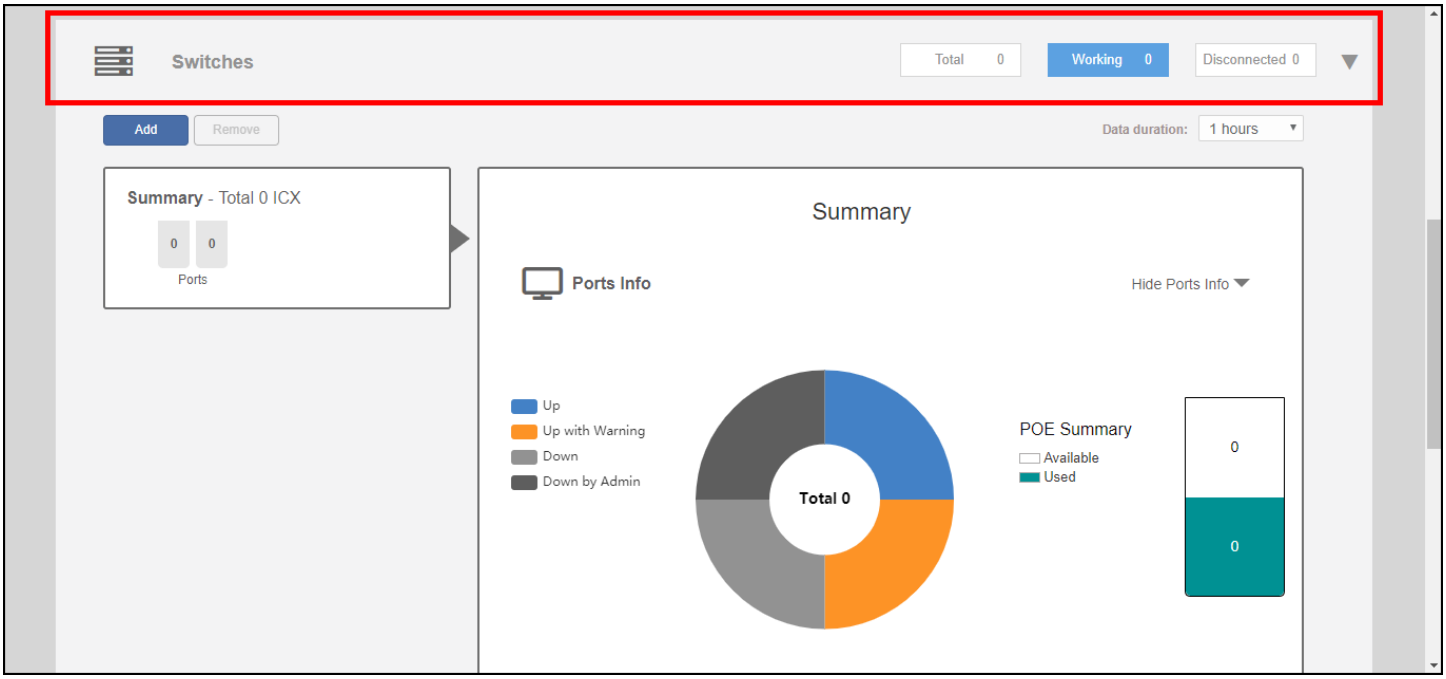
FIGURE 58 Access Points Component



Switches

The Switches component provides an at-a-glance overview of the status of any RUCKUS ICX switches managed by the RUCKUS Unleashed Master AP.

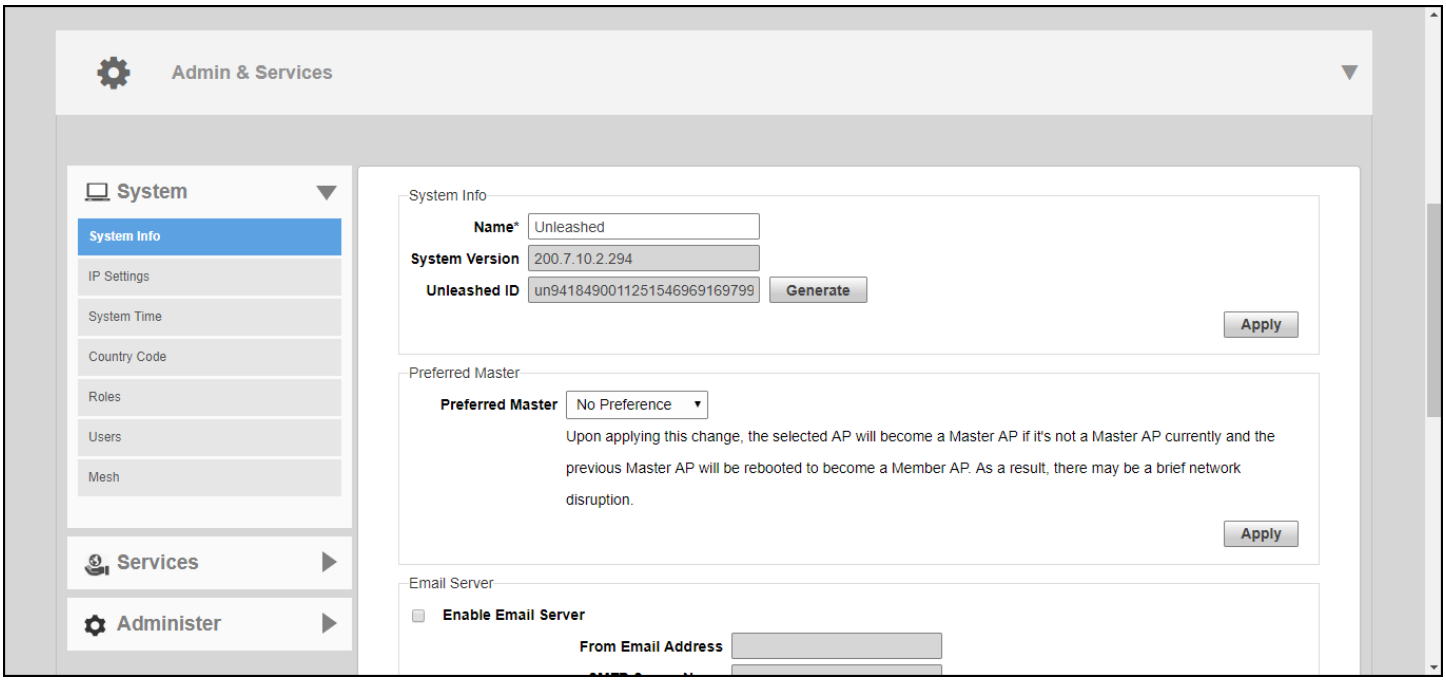
FIGURE 59 Switches Component



Admin & Services

The **Admin & Services** component provides options for configuring system settings and services, such as system IP address, Dynamic PSK, Bonjour Gateway, Application Recognition, Guest Access, Hotspot service, Radio Control settings and Wireless Intrusion Prevention Services (WIPS).

FIGURE 60 Admin & Services Component



Dedicated Master Configuration

- Dedicated Master Overview 169
- Converting an Unleashed Master AP to Dedicated Master 169
- Joining a Member AP to the Dedicated Master Network 171
- Dedicated Master AP or Member AP Behind NAT 174
- Checking Dedicated Master Status in the Unleashed Web Interface 175
- Smart Redundancy Configuration 176

Dedicated Master Overview

As a replacement for the ZoneDirector 1200, Dedicated Master is introduced in Unleashed 200.13.

NOTE
Only the R750 AP and the R850 AP can be elected as a Dedicated Master.

As compared to Unleashed bridge mode, the following features are supported in Dedicated Master mode:

- Cross-network segment networking
- Dedicated Master VLAN and AP VLAN
- Smart Redundancy
- Maximum capacity limit to 4,000 clients (compared to Unleashed bridge mode)
- Tunnel WLAN
- ZoneDirector AP migration to Unleashed network

Converting an Unleashed Master AP to Dedicated Master

Complete the following steps to convert an Unleashed Master AP to Dedicated Master:

- Checking Whether the Current Active Master AP is an R750 or R850
- Converting an Active Master AP to Dedicated Master

Checking Whether the Current Active Master AP is an R750 or R850

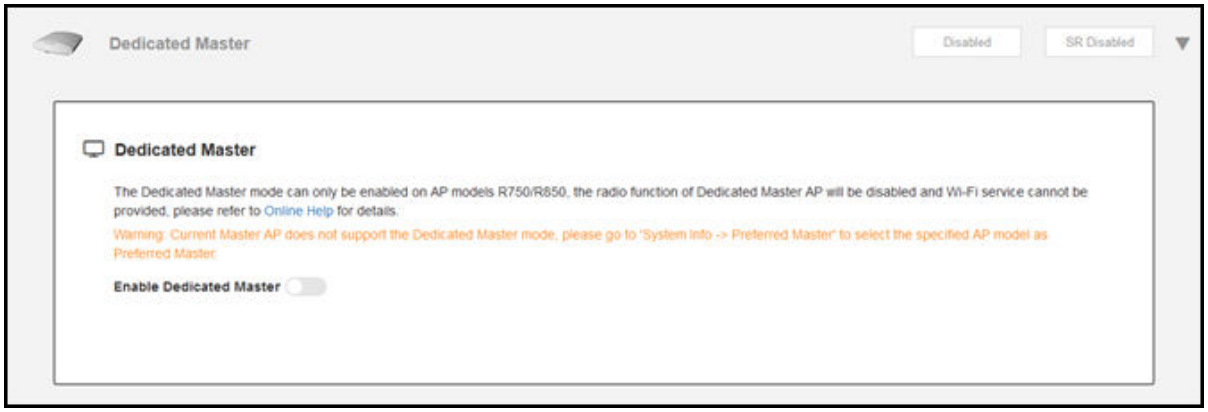
The **Enable Dedicated Master** option can be enabled only when the current Master AP is an R750 AP or an R850 AP. Otherwise, the system displays the following warning message:

Current Master AP does not support the Dedicated Master mode, please go to 'System Info -> Preferred Master' to select the specified AP model as Preferred Master.

For more information, refer to Designating a Preferred Master AP on page 368.

If the current Master AP is not an R750 AP or an R850 AP, the **Enabled Dedicated Master** option appears dimmed.

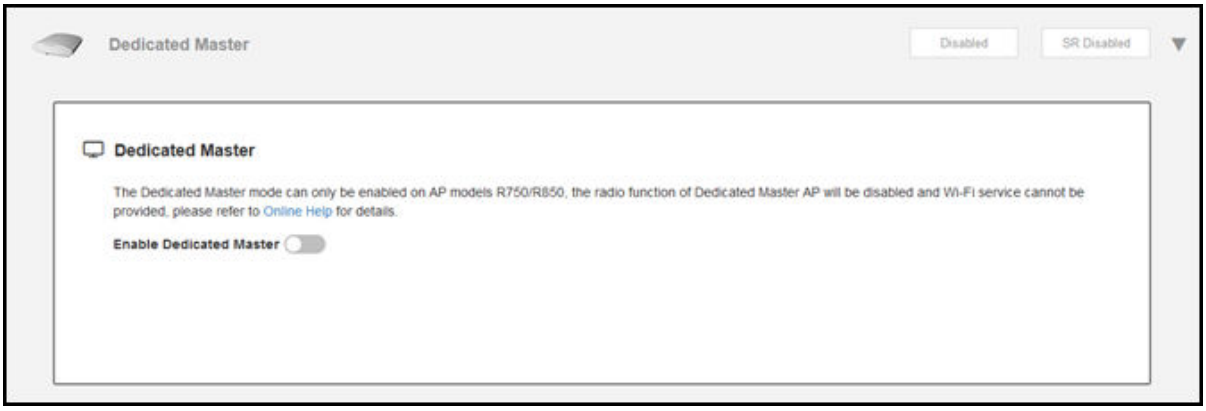
FIGURE 61 Warning Message



Converting an Active Master AP to Dedicated Master

1. From the Unleashed dashboard, select **Dedicated Master** and click the **Enable Dedicated Master** check box.

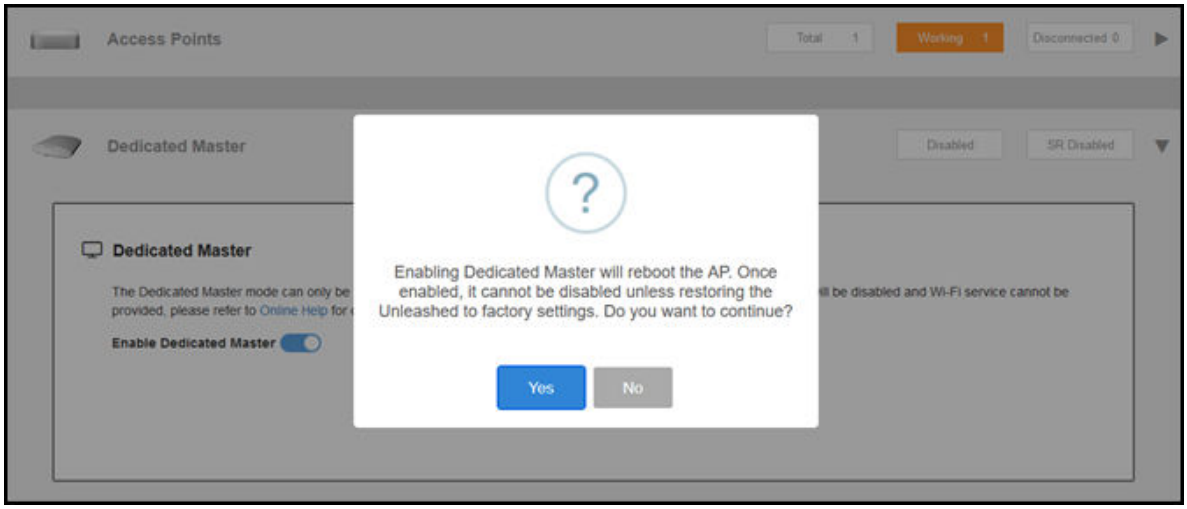
   FIGURE 62 Enabling Dedicated Master Mode



   The system displays the following warning message:

   Enabling Dedicated Master will reboot the AP. Once enabled, it cannot be disabled unless restoring Unleashed to factory settings. Do you want to continue?

FIGURE 63 Warning Message: Enabling Dedicated Master



2. Click **Yes** to reboot the AP.

Joining a Member AP to the Dedicated Master Network

You can use the following ways to join a member AP to the Dedicated Master network:

- Joining a Member AP to Dedicated Master Using Option 43 (Recommended) on page 171
- Placing a Member AP in the Same Network as Dedicated Master on page 172
- Setting the Dedicated Master IP Address in the Member AP CLI on page 173

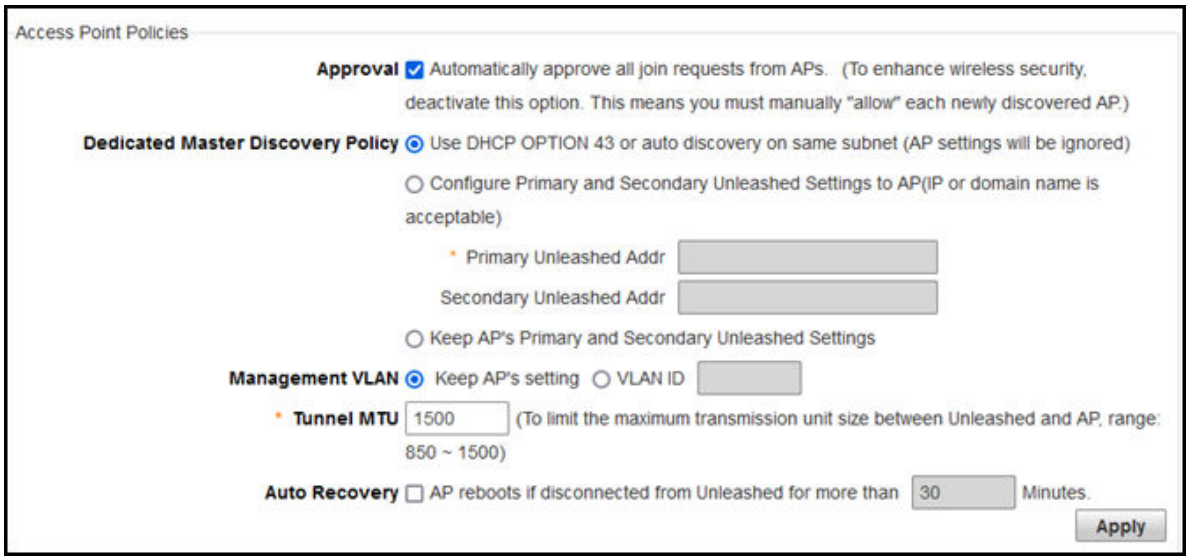
Joining a Member AP to Dedicated Master Using Option 43 (Recommended)

NOTE
Before you begin, ensure that Dedicated Master setup has been completed.

1. Select **Admin & Services** > **System** > **System Info** > **Access Point Policies**.
2. Select the **Approval** check box.

3. For **Dedicated Master Discovery Policy**, select **Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored)**.

   FIGURE 64 Member AP Joining Dedicated Master Using Option 43



4. Add the Option 43 setting under DHCP server in the Linux DHCP server.

```
#Ruckus Option 43 configuration as below:
option space ruckus_info;
option ruckus_info.zdiplist code 3 = text;
vendor-option-space ruckus_info;
option ruckus_info.zdiplist "10.223.26.121";
```

5. Power on the member AP to retrieve the IP address from DHCP.

   The member AP automatically joins Dedicated Master.

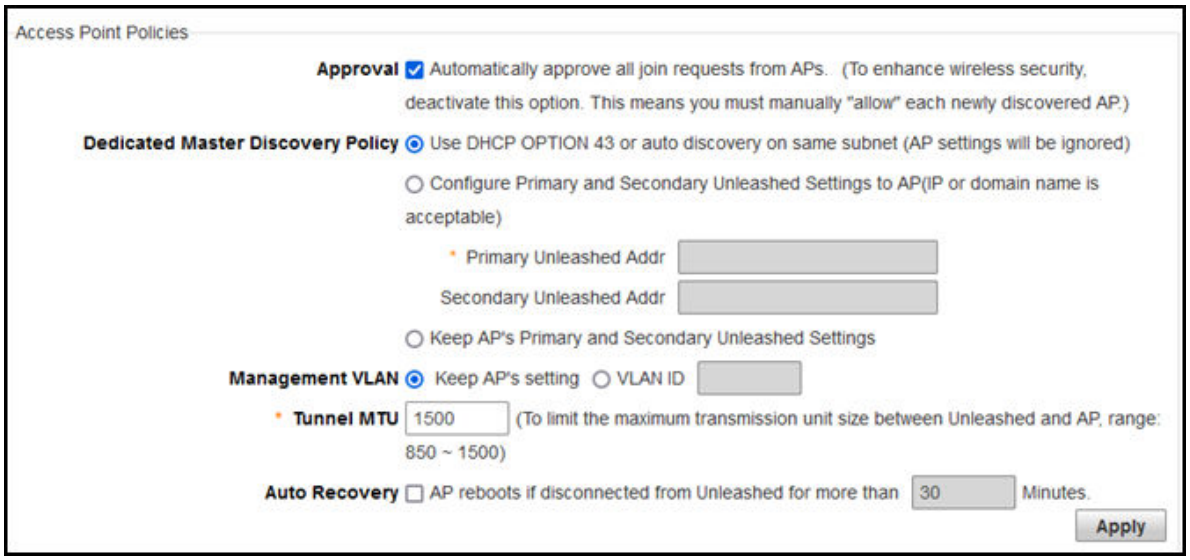
Placing a Member AP in the Same Network as Dedicated Master

NOTE
Before you begin, ensure that Dedicated Master setup has been completed.

1. Go to **Admin & Services** > **System** > **System Info** > **Access Point Policies**.
2. Select the **Approval** check box.

3. Under **Dedicated Master Discovery Policy**, select **Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored)**.

FIGURE 65 Placing Member AP in Same Network as Dedicated Master



4. Place the member AP in the same network as Dedicated Master and power on the AP.

   The member AP automatically joins the Dedicated Master.

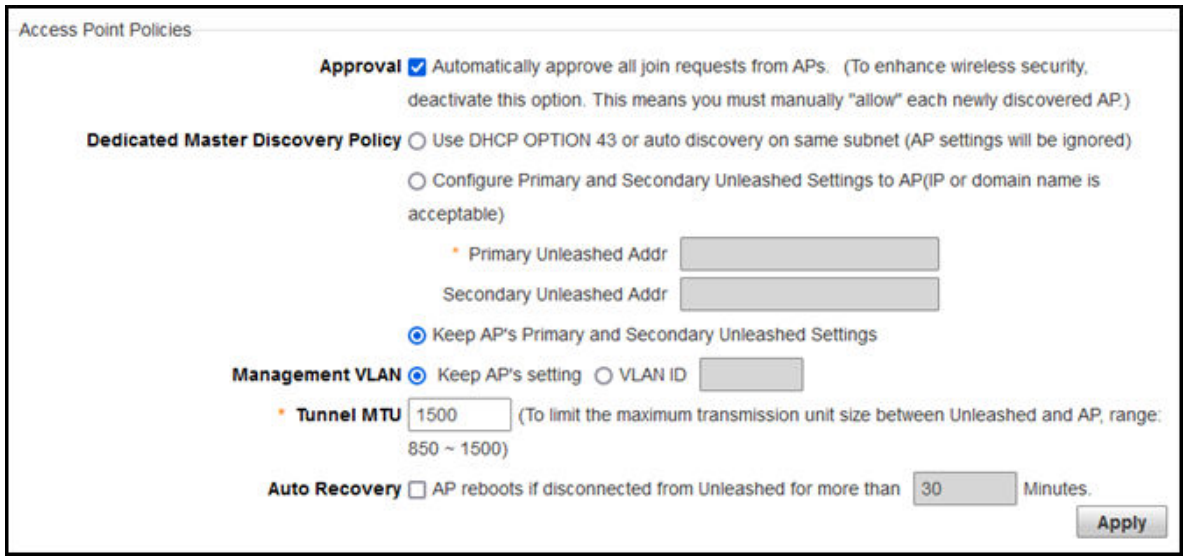
Setting the Dedicated Master IP Address in the Member AP CLI

NOTE
Before you begin, ensure that Dedicated Master setup has been completed.

1. Go to **Admin & Services** > **System** > **System Info** > **Access Point Policies**.
2. Select the **Approval** check box.

3. For **Dedicated Master Discovery Policy**, select **Keep AP's Primary and Secondary Unleashed Settings**.

   FIGURE 66 Maintaining the Unleashed Settings of the AP



4. Power on the AP and set the Dedicated Master IP address in the member AP CLI.

```
ruckus>
ruckus> en
ruckus#
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
ruckus(ap-mode)# set director ip 2.2.2.2
** Please reboot for this change to take effect
OK
ruckus(ap-mode)#
```

   After reboot, the member AP automatically joins Dedicated Master.

Dedicated Master AP or Member AP Behind NAT

In the Dedicated mode, a Dedicated Master AP or member AP working behind NAT is supported.

Basic NAT Topologies

You can follow three basic NAT topologies:

- Member AP behind NAT
- Dedicated Master AP behind NAT
- Both Dedicated Master AP and member AP behind NAT

Configuration Requirements for Ports or IP Addresses for NAT Topologies

You must configure the following port mapping for the service to work properly for NAT topologies:

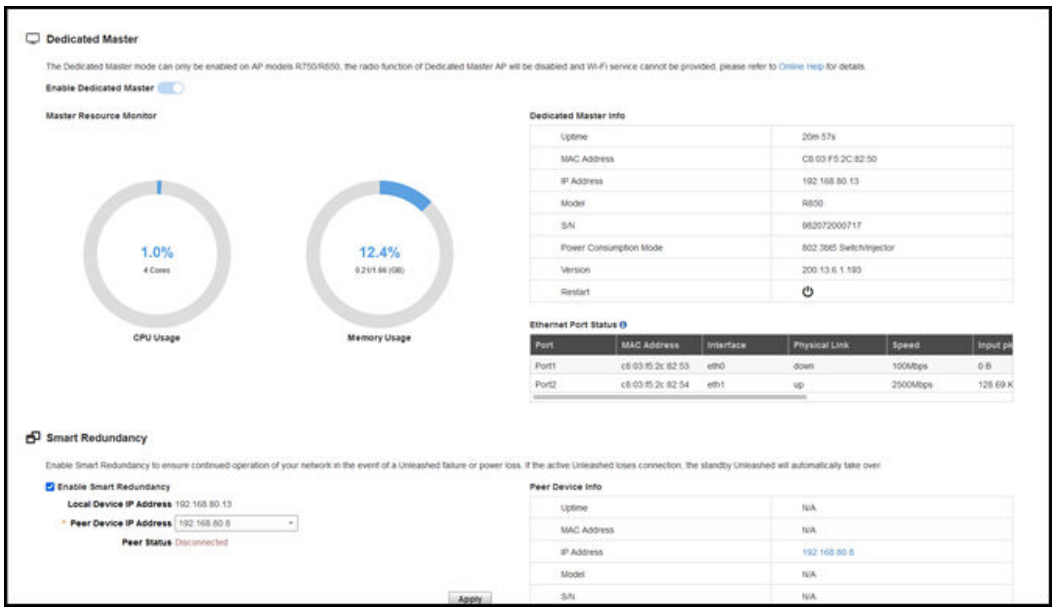
- Member AP behind NAT: Port configuration is not required.
- Dedicated Master AP behind NAT:
  - UDP port 12222, 12223, 60000 and TCP port 443 are configured to the private IP address of the Dedicated Master AP in the NAT mapping table.
  - The member AP must connect to the WAN IP address of NAT by Layer 3 (that is, the public IP address in the NAT mapping table of the Dedicated network).
- Both Dedicated Master AP and Member AP behind NAT:
  - UDP port 12222, 12223, 60000 and TCP port 443 are configured to the private IP address of the Dedicated Master AP in the NAT mapping table.
  - The member AP must connect to the WAN IP address of NAT by Layer 3 (that is, the public IP address in the NAT mapping table of the Dedicated network).

Checking Dedicated Master Status in the Unleashed Web Interface

Complete the following steps to check the Dedicated Master status after the wizard setup or conversion of Unleashed to Dedicated Master.

1. Log in to the Unleashed web interface by entering the administrator username and password. Click **Unleash**.
2. Under **Dedicated Master**, check the status and information about Dedicated Master and Smart Redundancy.

FIGURE 67 Dedicated Master and Smart Redundancy Information



Smart Redundancy Configuration

When Unleashed is switched to Dedicated Master mode, Unleashed supports Smart Redundancy ability as ZoneDirector.

Smart Redundancy feature allows configuration of two Dedicated Masters as a redundant pair, with one unit actively managing your network while the other serving as a backup in the standby mode and ready to take over if the first unit fails or loses power.

Each Dedicated Master will either be in an active or standby state. If the active Dedicated Master fails, the standby device becomes active. When the original active device recovers, it automatically assumes the standby state as it discovers an already active Dedicated Master on the network.

The Dedicated Master in an active state manages all the APs and client connections. The Dedicated Master in the standby state is responsible for monitoring the health of the active unit and periodically synchronizing its settings to match that of the active device. The Dedicated Master in the standby state will not respond to discovery requests from the APs, and changing from an active to standby state will release all the associated APs.

When a failover occurs, all the associated APs will continue to provide wireless service to the clients during the transition, and will associate to the newly active Dedicated master within approximately one minute.

When two Dedicated Masters are connected in a Smart Redundancy configuration, the standby Dedicated Master will send heartbeats and the active Dedicated Master will send discovery messages at 6-second intervals. After 15 seconds, if there is no response, each controller will assume disconnection from its peer, and the standby Dedicated Master will change to an active state. At this point, both the devices are in an active state and will accept join requests from the APs.

When the two Dedicated Masters are communicating again, one active Dedicated Master will change to the standby state and an auto-synchronization process will be started. A timestamp is used to determine which Dedicated Master is active and synchronizes its latest configuration changes to its peer.

Smart Redundancy Setup Overview

Complete the following steps to set up Smart Redundancy.

1. Install the Dedicated Unleashed Master AP. Refer to Setting Up an Unleashed Wi-Fi Network on page 131.
2. Configure the Dedicated Unleashed Master AP. Refer to Configuring Dedicated Master for Smart Redundancy on page 176.
3. Set up Smart Redundancy with the following components:
   - Member R750 AP or R850 AP
   - Other Dedicated Master
4. Check Smart Redundancy status. Refer to Checking the Standby Dedicated Master on page 184.

Configuring Dedicated Master for Smart Redundancy

You can set up Smart Redundancy on Dedicated Master using the following options:

- Smart Redundancy Setup Through Auto Mode on page 176
- Smart Redundancy Setup Through Manual Mode on page 179
- Smart Redundancy Setup Through the Command Line Interface on page 183

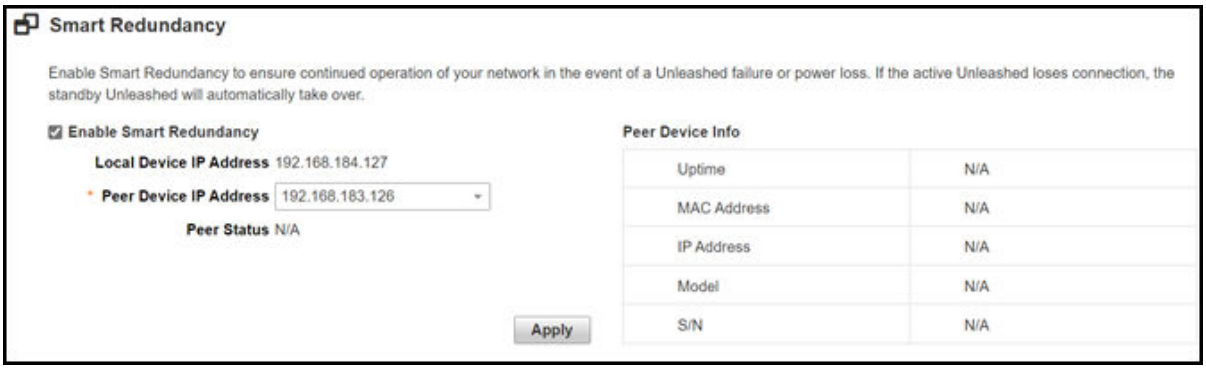
Smart Redundancy Setup Through Auto Mode

Complete the following steps to set up Smart Redundancy through auto mode.

1. Connect the member R750 AP or R850 AP to the Dedicated Master network.
2. Log in to the web interface of Dedicated Master.

3. On the **Dedicated Master** page under **Smart Redundancy**, select the **Enable Smart Redundancy** check box.

FIGURE 68 Enabling Smart Redundancy: Auto Mode

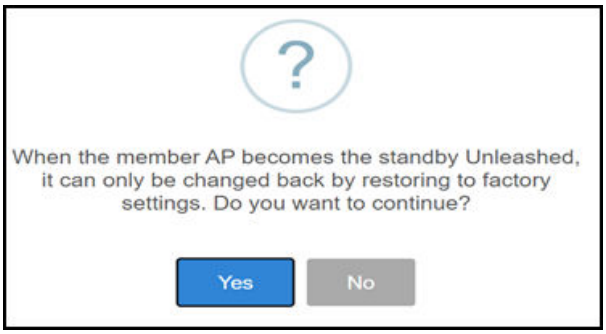


4. From the **Peer Device IP Address** list, select the IP address of the member R750 AP or R850 AP.

NOTE
Only an online root R750 AP or R850 AP can be selected as a peer device.

5. Click **Apply**. A confirmation message is displayed.

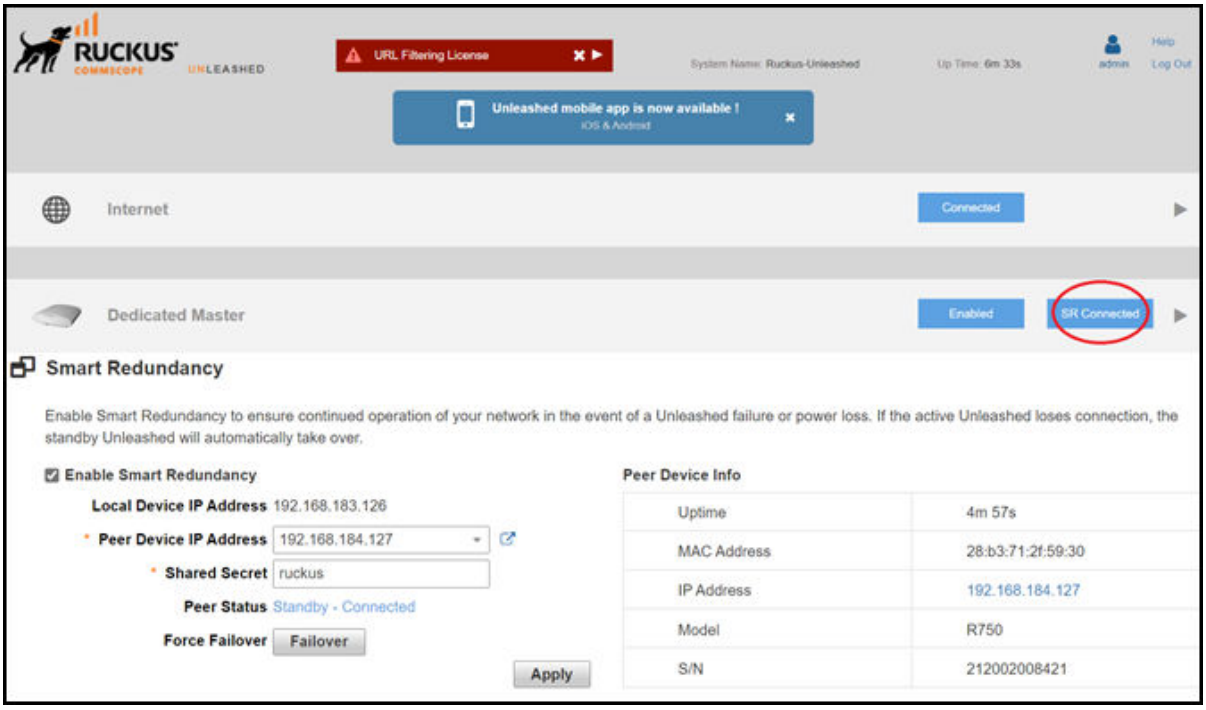
FIGURE 69 Confirmation Message for Selecting Peer Device



The selected member R750 AP or R850 AP syncs the configuration from Dedicated Master and changes to the standby Master AP after reboot.

If Smart Redundancy is established successfully, the peer status shows **SR Connected** and the details of the peer device are displayed in the **Peer Device Info** table.

FIGURE 70 Checking Smart Redundancy Status



NOTE
If the active and standby Dedicated Master APs are on different IP subnets, the APs must know the IP addresses of both Master APs to quickly find the active Master AP after a Smart Redundancy failover. You can configure the IP addresses of both devices. Go to **Admin & Services** > **System** > **System Info** > **Dedicated Master Discovery Policy**. For **Dedicated Master Discovery Policy**,

specify one Dedicated Master AP as primary and the other as secondary. Alternatively, you can also specify the IP addresses of both Dedicated Master APs using DHCP Option 43.

NOTE
If you disable Smart Redundancy after it has been enabled, both Dedicated Master APs will revert to the active state, which could result in unpredictable network topologies. Therefore, it is recommended to reset the standby Dedicated Master AP to factory settings before disabling Smart Redundancy.

NOTE
Smart Redundancy supports synchronization of SSL certificate.

NOTE
If an active or standby Master with Smart Redundancy enabled is deployed on different subnets, management IP address must be on a separate management VLAN and both the Masters must be the members of this management VLAN.

NOTE
The member R750 AP or R850 AP is removed from the AP list when it changes to standby Dedicated Master.

Smart Redundancy Setup Through Manual Mode

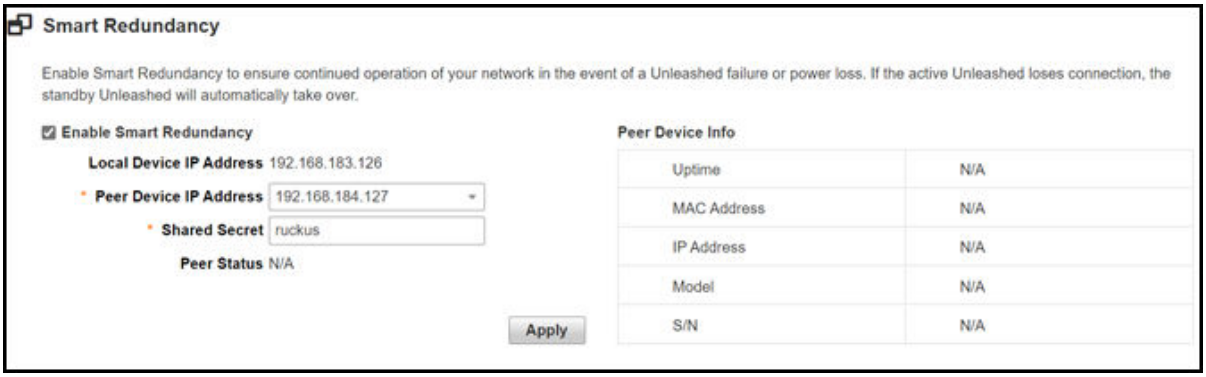
Complete the following steps to set up Smart Redundancy through manual mode.

1. Install two Dedicated Master networks in the same subnet or different subnets.
2. Log in to the web interface of the primary Dedicated Master (preferred as the primary).
3. From the **Dedicated Master** page under **Smart Redundancy**, select the **Enable Smart Redundancy** check box.
4. For **Peer Device IP Address**, enter the IP address of the secondary Dedicated Master.
5. For **Shared Secret**, enter a password for two-way communication between the two Dedicated Master networks.

   The password can contain up to a maximum of 15 characters and cannot include "`" (grave accent) or "$(".

   NOTE
   A dollar sign ($) and an opening parenthesis (() can be used separately in the password.

FIGURE 71 Enabling Smart Redundancy: Manual Mode



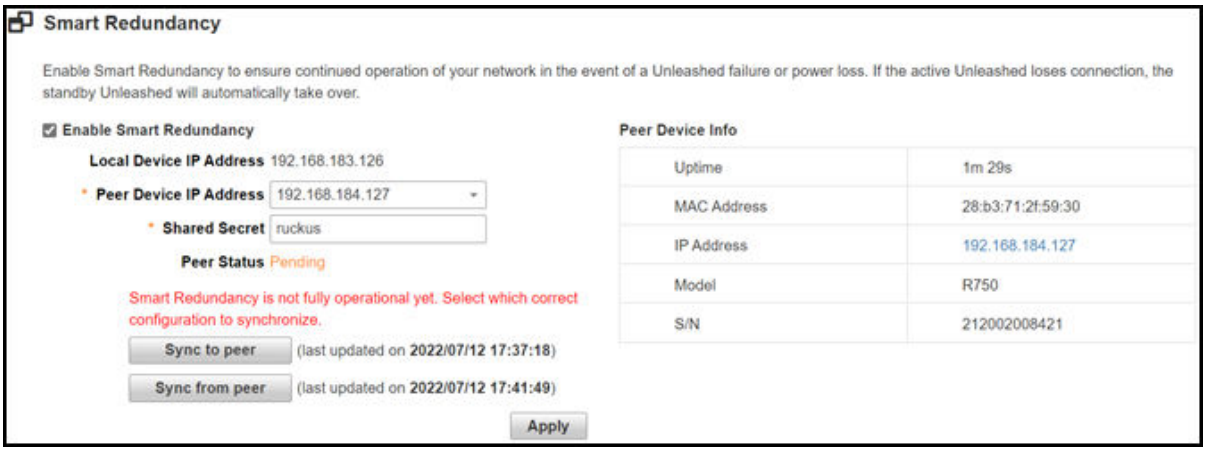
6. Click **Apply** to save changes.

   NOTE
   The versions of local and peer devices must match.

7. Log in to the web interface of the secondary Dedicated Master (preferred as the backup).
8. On the **Dedicated Master** page under **Smart Redundancy**, select the **Enable Smart Redundancy** check box.
9. For **Peer Device IP Address**, enter the IP address of the primary Dedicated Master.
10. For **Shared Secret**, enter the same password as entered in Step 5.
11. Click **Apply** to save changes.

    If an active Dedicated Master is discovered, the secondary Dedicated Master assumes the standby state. The **Sync to peer** and **Sync from peer** buttons are displayed on both Dedicated Masters to prompt configuration synchronization between local and peer devices.

    FIGURE 72 Syncing Configuration Between Local and Peer Devices

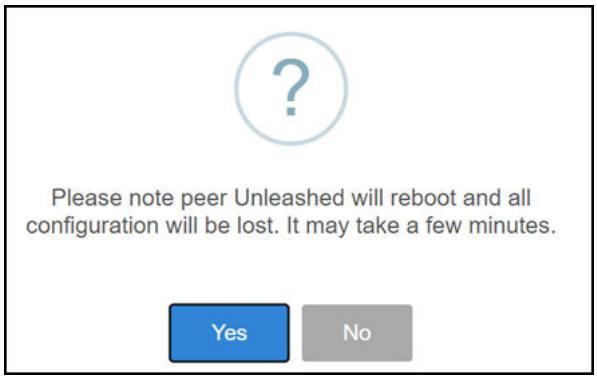


12. Choose one of the following options:

- Click **Sync to peer** on the primary Dedicated Master.

  A confirmation message is displayed.

  FIGURE 73 Confirmation Message: Sync to Peer



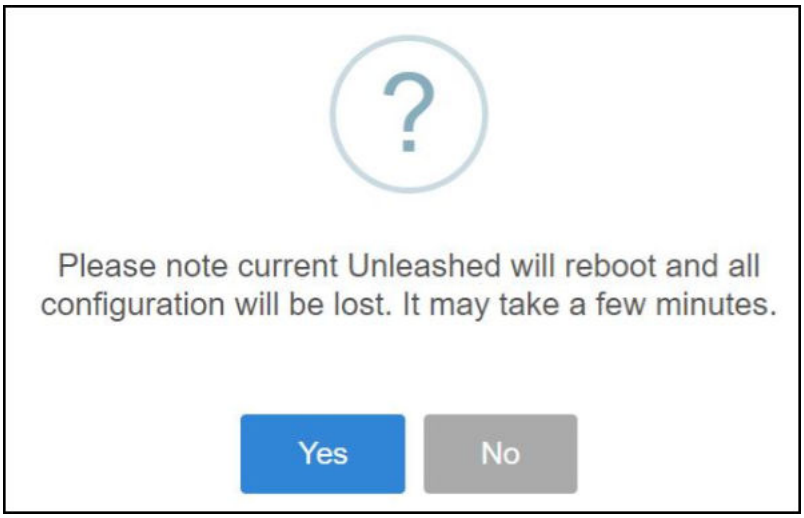
  Click **Yes** to proceed.

  The primary Dedicated Master syncs the configuration to the peer. The secondary Dedicated Master reboots and all its configuration is lost.

- Click **Sync from peer** on the primary Dedicated Master.

  A confirmation message is displayed.

  FIGURE 74 Confirmation Message: Sync from Peer



  Click **Yes** to proceed.

  The primary Dedicated Master syncs the configuration from the peer. The current Dedicated Master reboots and all its configuration is lost. The primary Dedicated Master and secondary Dedicated Master switch roles.

  NOTE

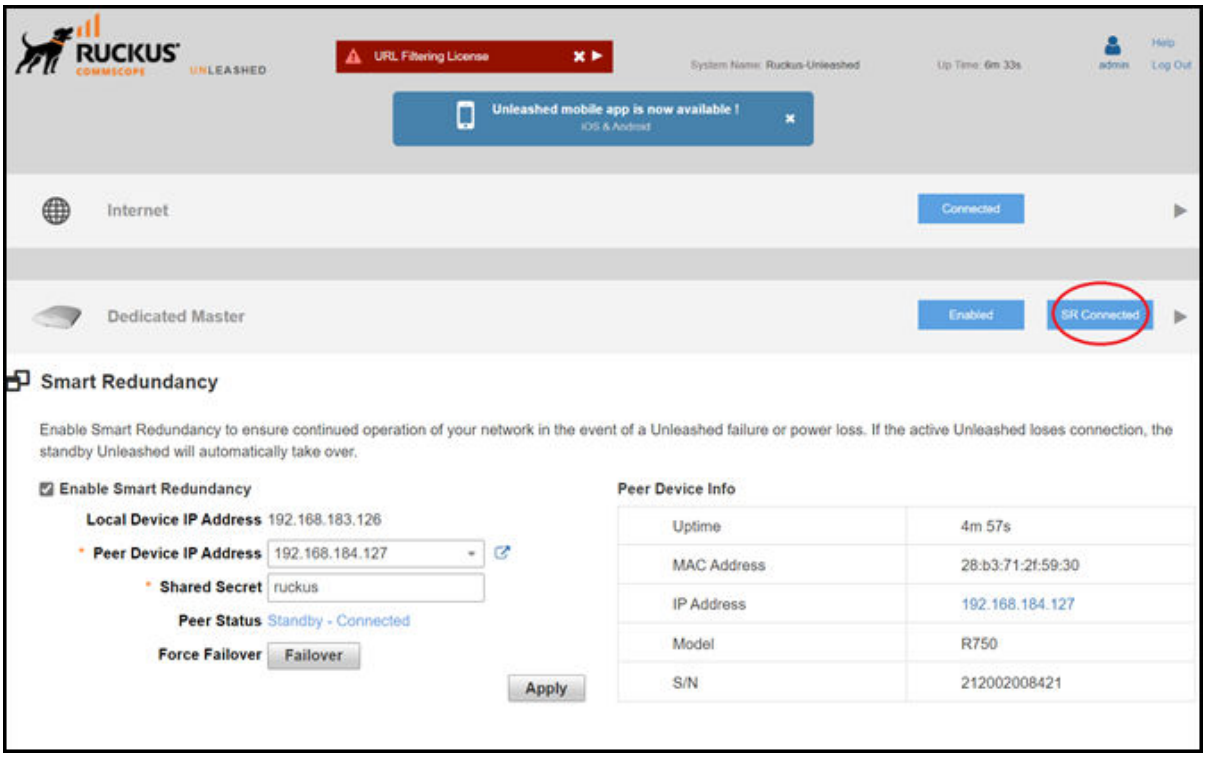
To avoid a primary Dedicated Master reboot and the switch from the primary Dedicated Master to the secondary Dedicated Master, it is recommended to select the **Sync to peer** option on the primary Dedicated Master and synchronize the configuration from the local to the peer device.

13. Log in to the standby Dedicated Master web interface after it boots up.

    The secondary Dedicated Master enters the standby mode.

14. Check the Smart Redundancy status on the primary Dedicated Master.

FIGURE 75 Checking the Status of Smart Reducdancy



NOTE
Smart Redundancy fails to establish a connection if the Unleashed versions are not the same.

NOTE
Use the **Force Failover** option to switch the active and standby states.

NOTE
If the active and standby Dedicated Master APs are on different IP subnets, the APs must know the IP addresses of both Master APs to quickly find the active Master AP after a Smart Redundancy failover. You can configure the IP addresses of both devices. Go to **Admin & Services** > **System** > **System Info** > **Dedicated Master Discovery Policy**. For **Dedicated Master Discovery Policy**, specify one Dedicated Master AP as primary and the other as secondary. Alternatively, you can also specify the IP addresses of both Dedicated Master APs using DHCP option 43.

NOTE
If you disable Smart Redundancy after it has been enabled, both the Dedicated Master APs will revert to the active state, which could result in unpredictable network topologies. Therefore, it is recommended to reset the standby Dedicated Master AP to factory settings before disabling Smart Redundancy.

NOTE
Smart Redundancy supports synchronization of SSL certificate.

NOTE
If an active or standby Master that is enabled with Smart Redundancy is deployed on different subnets, the management IP address must be on a separate management VLAN and both the Masters must be the members of this management VLAN.

NOTE
Active and standby Master APs are not displayed on the AP list; they are displayed in the AP table of the **Admin & Services** > **Administration** > **Upgrade** page.

Smart Redundancy Setup Through the Command Line Interface

Complete the following steps to set up Smart Redundancy through CLI.

1. Use SSH to access the CLI of Dedicated Master preferred as the primary.
2. Enable Smart Redundancy, and configure the peer device IP address and the shared secret.

FIGURE 76 Enabling Smart Redundancy Through the CLI for the Primary Dedicated Master

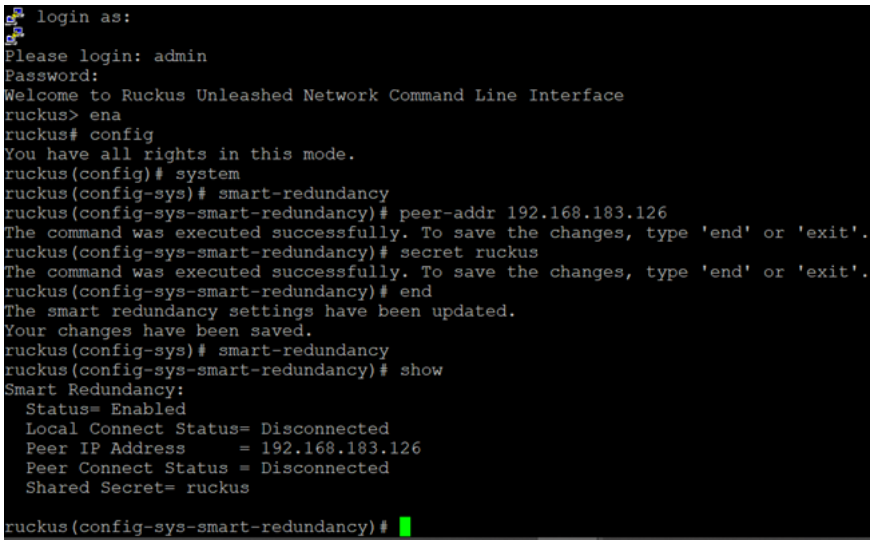
```
Please login:
Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> ena
ruckus# config
You have all rights in this mode.
ruckus(config)# system
ruckus(config-sys)# smart-redundancy
ruckus(config-sys-smart-redundancy)# peer-addr 192.168.184.127
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys-smart-redundancy)# secret ruckus
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys-smart-redundancy)# show
Smart Redundancy:
  Status= Disabled
  Peer IP/IPv6 Address=
  Shared Secret=

ruckus(config-sys-smart-redundancy)# end
The smart redundancy settings have been updated.
Your changes have been saved.
ruckus(config-sys)# smart-redundancy
ruckus(config-sys-smart-redundancy)# show
Smart Redundancy:
  Status= Enabled
  Local Connect Status= Disconnected
  Peer IP Address     = 192.168.184.127
  Peer Connect Status = Disconnected
  Shared Secret= ruckus
```

3. Use SSH to access the CLI of the Dedicated Master preferred as the secondary.

4. Enable Smart Redundancy, and configure the peer device IP address and the shared secret.

FIGURE 77 Enabling Smart Redundancy Through the CLI for the Backup Dedicated Master



5. Log in to the primary Dedicated Master web interface and click **Sync to peer** to synchronize the configuration from the local to the peer device (as shown in the *Smart Redundancy Setup Through Manual Mode*).

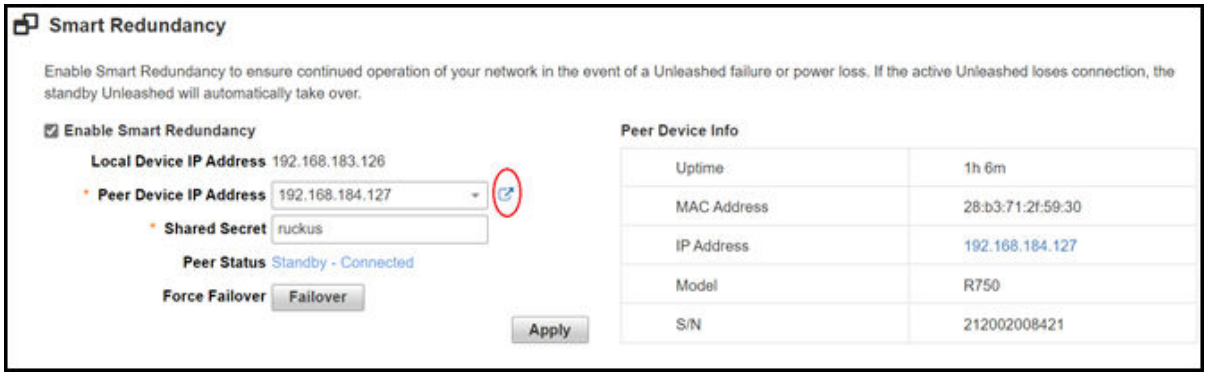
NOTE
Command line interface does not support Smart Redundancy setup through auto mode; only Smart Redundancy setup through manual mode is supported.

6. Check the Smart Redundancy status on the primary Dedicated Master.

Checking the Standby Dedicated Master

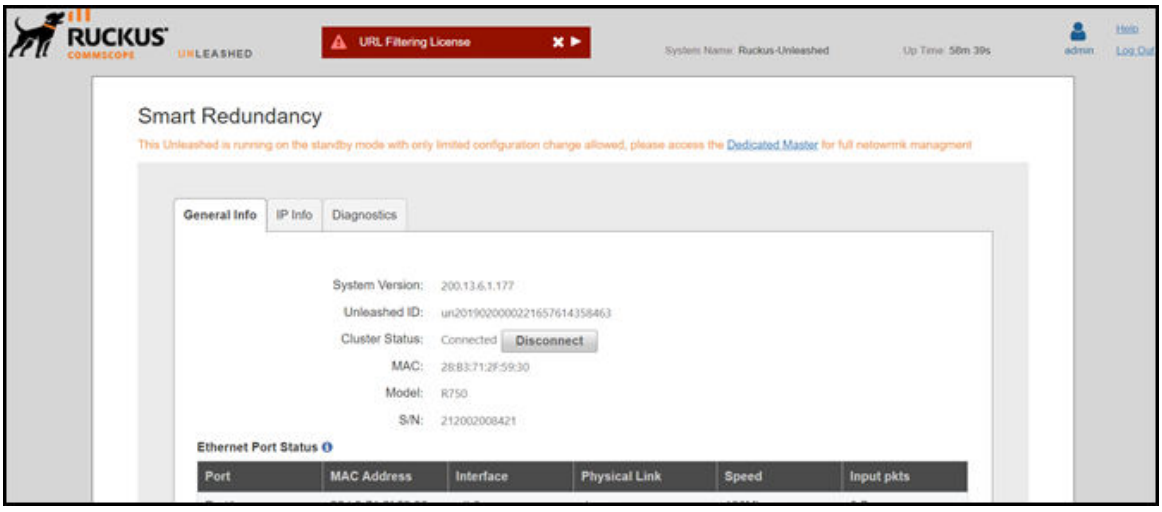
Log in to the standby Dedicated Master web interface using the device IP address https://StandbyMaster_ip or open the web interface of the standby Dedicated Master from the web interface of the primary Dedicated Master by clicking the icon next to **Peer Device IP Address**.

FIGURE 78 Opening the Standby Dedicated Master Web Interface



The standby mode information is displayed.

FIGURE 79 Standby Dedicated Master Information



Disabling Smart Redundancy

You can disable Smart Redundancy using the following options:

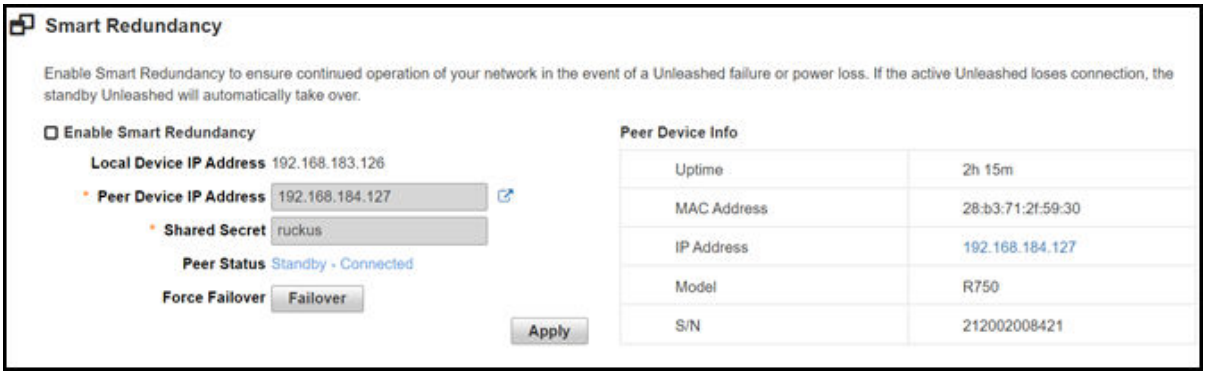
- Disabling Smart Redundancy from the Primary Dedicated Master on page 185
- Disabling Smart Redundancy from the Standby Dedicated Master on page 187

Disabling Smart Redundancy from the Primary Dedicated Master

Complete the following steps to disable Smart Redundancy from the primary Dedicated Master.

1. Clear the **Enable Smart Redundancy** check box.

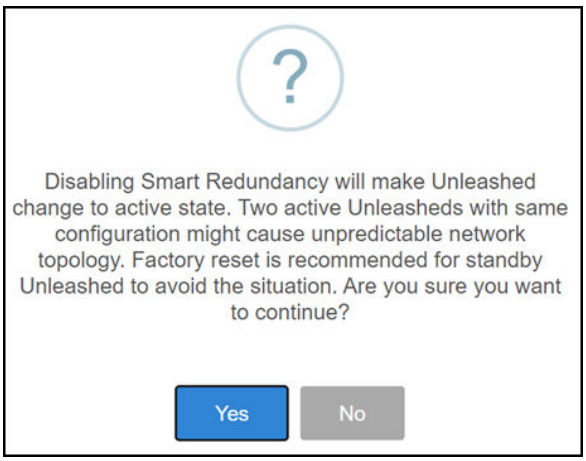
   FIGURE 80 Disabling Smart Redundancy from the Primary Dedicated Master



2. Click **Apply** to save the changes.

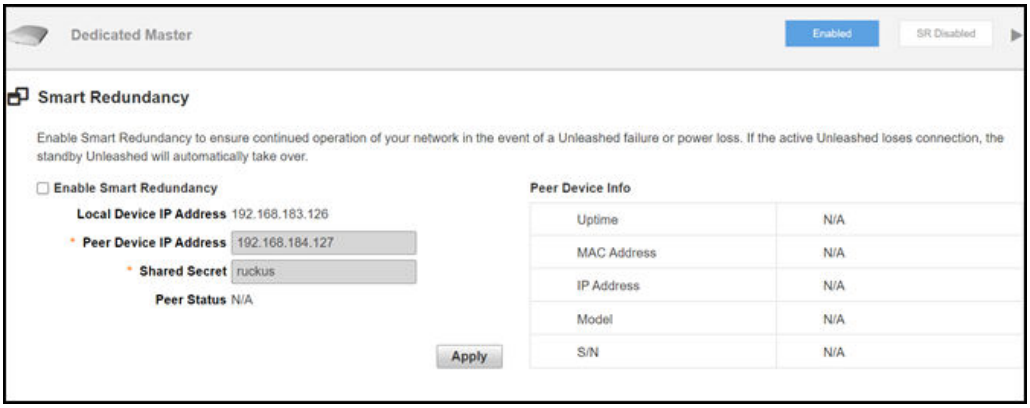
   A confirmation message is displayed.

   FIGURE 81 Confirmation Message: Disabling Smart Redundancy



3. Click **Yes** to confirm.
4. Check the Smart Redundancy status.

   FIGURE 82 Checking Smart Redundancy Status After Disabling

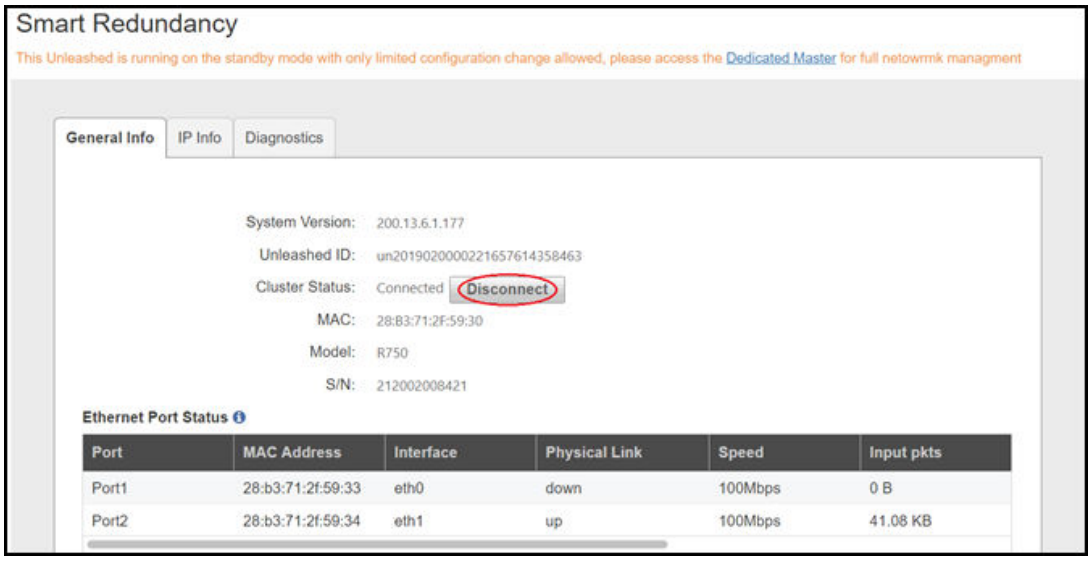


Disabling Smart Redundancy from the Standby Dedicated Master

Complete the following steps to disable Smart Redundancy from the standby Dedicated Master.

1. From the standby Dedicated Master web interface on the **General Info** tab, click the **Disconnect** button in **Cluster Status**.

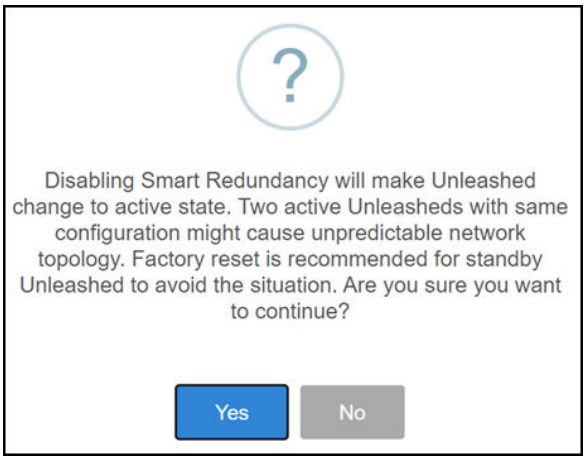
   FIGURE 83 Disabling Smart Redundancy from the Standby Dedicated Master



2. Click **Apply** to save the changes.

   A confirmation message is displayed.

   FIGURE 84 Confirmation Message: Disabling Smart Redundancy



3. Click **Yes** to confirm.

   The standby Dedicated Master web interface auto-refreshes and switches to active mode.

WLAN Configuration

- WLAN Configuration Overview....189
- WLAN Usage Types....191
- Creating a New WLAN....192
- 802.1X EAP WLANs....195
- Guest WLANs....198
- Hotspot WLANs....263
- Configuring Global WLAN Settings....264
- Editing an Existing WLAN....265
- Using a QR Code to Join a Wi-Fi Network....266
- Deleting a WLAN....267
- Disabling a WLAN Temporarily....268

WLAN Configuration Overview

The **Wi-Fi Networks** component of the RUCKUS Unleashed dashboard provides tools for managing all aspects of your RUCKUS Unleashed wireless local area networks (WLANs).

It contains options for creating new WLANs, modifying or deleting existing WLANs, and configuring global wireless settings for deployment on all WLANs.

The **Wi-Fi Networks** component offers two display modes:

- Card display mode
- Table display mode

The **Wi-Fi Networks** component offers the following options:

- Search field: Search WLANs in card or table display mode.
- **Summary** Wi-Fi Network box: Click this box to view a summary of all WLAN clients, signal quality, and traffic statistics.
- Individual Wi-Fi network boxes: Click any of these boxes to view details specific to the indicated WLAN.
- **Data Duration**: Select the duration of time interval (10 minute, 1 hour, and 12 hours) to view the client status and traffic information of the indicated WLAN.
- **Display Mode**: Switch between card and table display modes. If there are more than 20 WLANs, they are displayed in table mode automatically. The display mode returns to the default (card mode) when the web interface is refreshed.

  NOTE
  You can configure 64 WLANs in Dedicated mode and 16 WLANs in local bridge mode from the web interface, CLI, and mobile app.

- **Show Clients Info**: Click this link to view a table of currently connected clients.
- **Client Status** bar chart: This chart displays the number of connected clients and the client signal quality across all connected WLANs at one-minute intervals (over the last 10 minutes), 5-minute intervals (over the last one hour), and one-hour intervals (over the last 12 hours) respectively.
- **Traffic** graph: This graph displays the Received (Rx), Transmitted (Tx), and Total traffic values as per the time interval selected for **Data Duration**.

FIGURE 85 Wi-Fi Networks Component: Card Display Mode

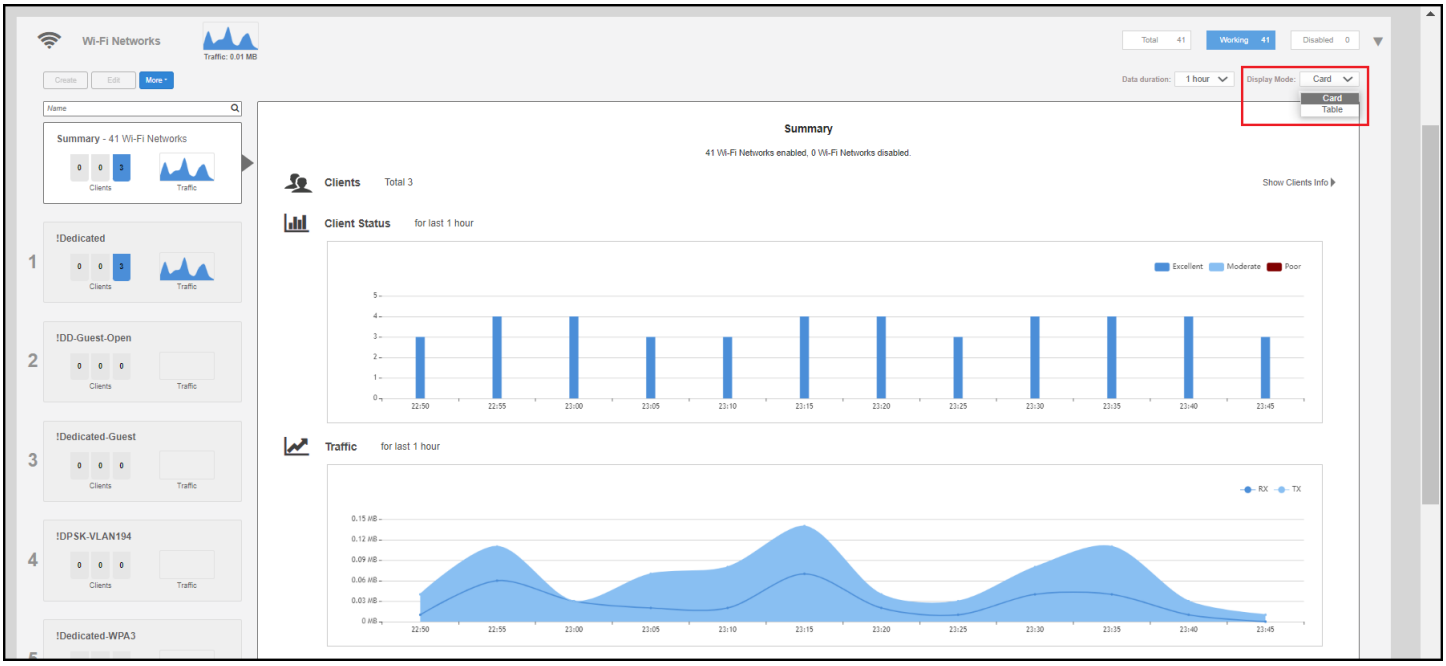
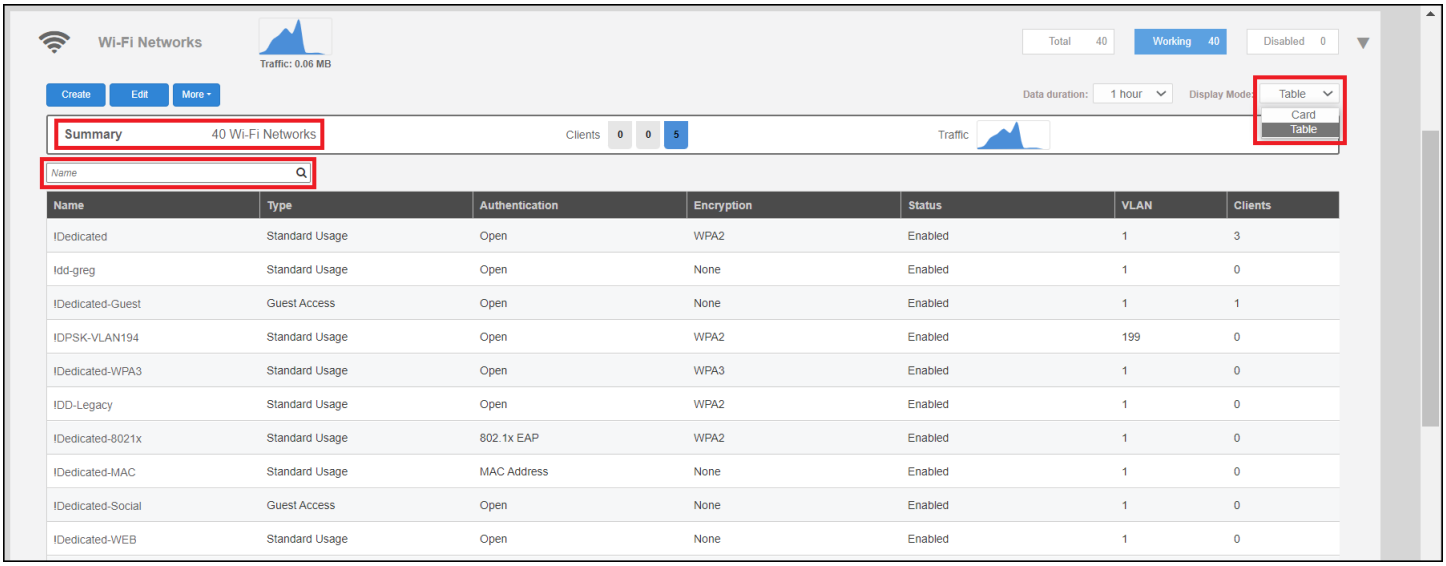


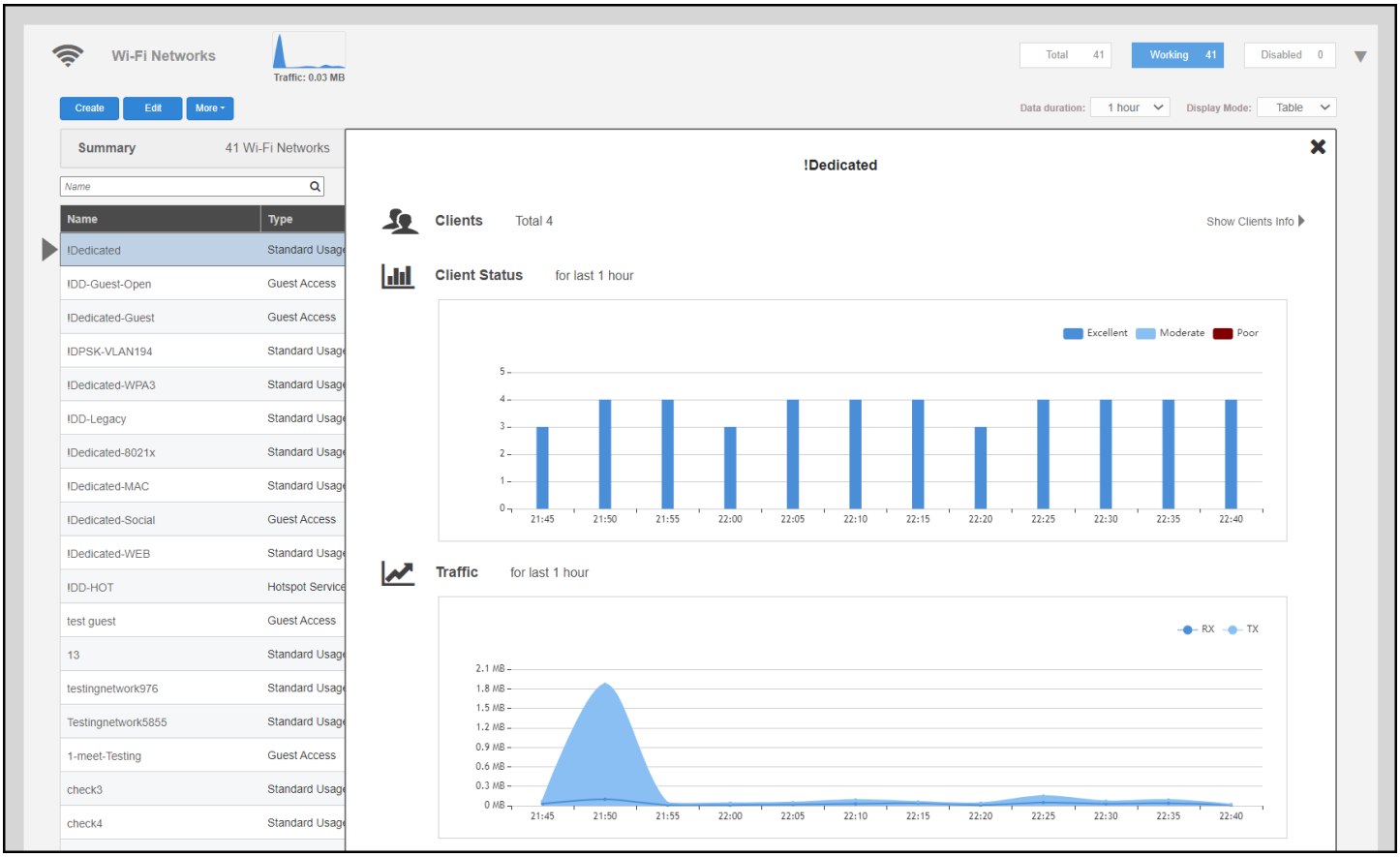
FIGURE 86 Wi-Fi Networks Component: Table Display Mode



You can sort the items in the table by clicking the **Name**, **Type**, **Authentication**, **Encryption**, **Status** column headings.

In the table display mode, you can click individual rows to view information about the clients and traffic associated with the selected WLAN.

FIGURE 87 Viewing Individual WLAN Information in Table Display Mode



WLAN Usage Types

Each WLAN must be configured as one of the following usage types:

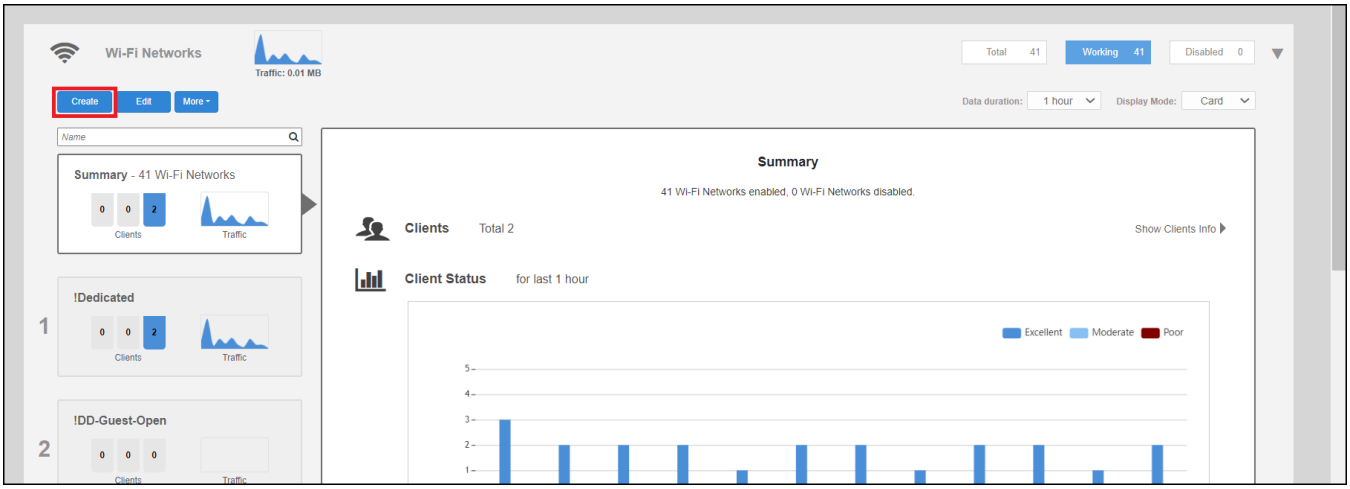
- **Standard Usage**: To create a WLAN with specific options, choose "Standard Usage."
- **Guest Access**: Use this WLAN type for a guest WLAN. Guest access policies and access controls will be applied. For more information, see Guest WLANs on page 198.
- **Hotspot Service**: Use this WLAN type for a Hotspot (aka, WISPr) WLAN. If Hotspot is used, a Hotspot Service must first be configured on the **Admin & Services > Services > Hotspot Service** page (or from the **Wi-Fi Networks > Create WLAN> Create Service** page). For more information, see Hotspot Services on page 436.

Creating a New WLAN

In addition to the initial WLAN you created during the setup process, you can create new WLANs using the **WiFi Networks** component.

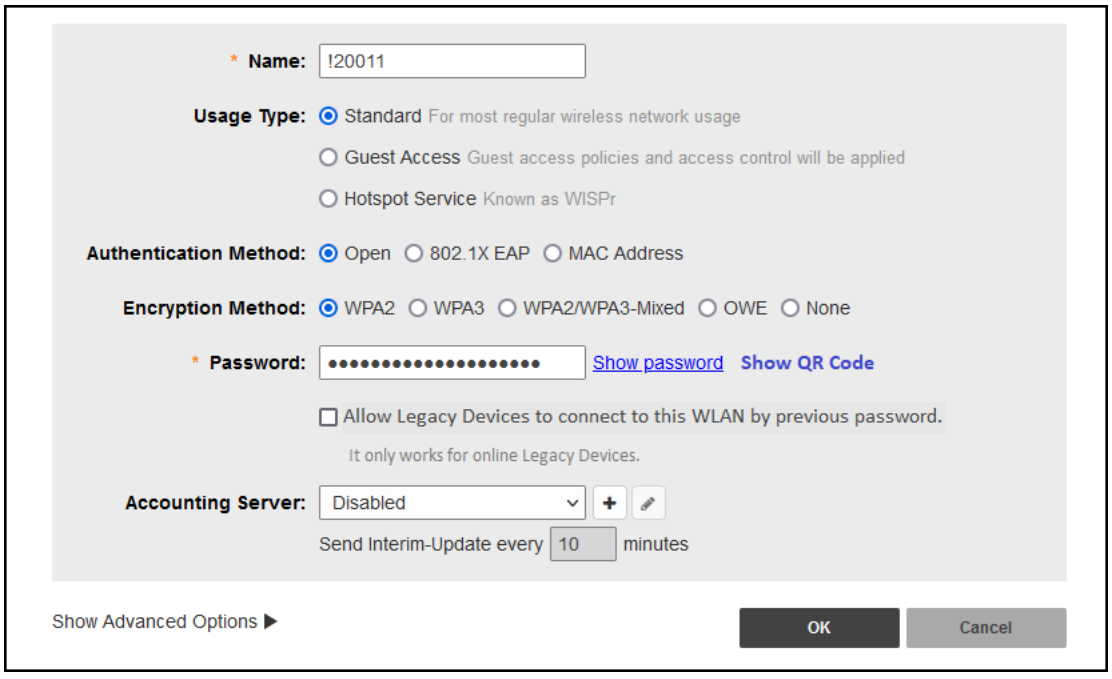
1. In the **WiFi Networks** component, click **Create**.

FIGURE 88 Creating a New WLAN



The **Create WLAN** page is displayed.

FIGURE 89 New WLAN Settings



2. Enter a **Name** for this wireless network.

3. Select the WLAN **Usage Type** from the following options:
   - **Standard**: Use this WLAN type for most regular wireless network usage.
   - **Guest Access**: Guest access policies and access controls will be applied. For more information, refer to Guest WLANs on page 198.

     NOTE
     As of Unleashed 200.7, Social Media WLANs are a subset of guest WLANs, and are configured using the guest WLAN settings. Social Media WLANs require a visitor to log in using a social media account before being granted Internet access. For more information, refer to Social Media WLANs on page 242.

   - **Hotspot Service**: Use this WLAN type for a Hotspot (also known as WISPr) WLAN. To deploy a Hotspot WLAN, you must first configure a Hotspot Service. For more information, refer to Hotspot Services on page 436.
4. For **Authentication Method**, select one of the following options:

   NOTE
   Unless using an external authentication server (RADIUS server), select Open authentication, and combine with **WPA2** encryption for secure Wi-Fi access.

   - **Open**: No authentication method is used. Open authentication allows the use of WPA2, WPA3, WPA2/WPA3-Mixed, OWE, or None encryption. Open authentication and WPA2 encryption (also known as WPA-PSK) is the most common type of WLAN encryption method and should be the default configuration if there are no special requirements for authentication or encryption.
   - **802.1X EAP**: Authenticates against either the internal database or an external RADIUS server. The 802.1X EAP authentication method (also known as WPA2-Enterprise) provides effective authentication regardless of the encryption method, and requires a back-end (RADIUS) authentication server. WPA2-Enterprise provides secure connectivity by ensuring that every device must authenticate to an authentication server before it is allowed access to network resources. Authentication can be based on digital certificates, and granular policies can be designed to govern the level of access and to provide visibility and control over devices on the network. 802.1X EAP authentication allows the use of WPA2, WPA3, or WPA2/WPA3-Mixed encryption.
   - **MAC Address**: Authenticates using the client MAC address against an external RADIUS server or internal database.

     NOTE
     Beginning with Unleased 200.7, MAC address authentication using the local database is available.

5. For **Encryption Method**, select one of the following options:
   - **WPA2**: Encrypts traffic using the WPA2 standard. The WPA2 encryption method complies with the 802.11i security standard. Announced in 2004, WPA2 encryption remains mandatory for all new products that bear the Wi-Fi trademark.
   - **WPA3**: You can enable 802.11r FT roaming for open authentication and WPA3 encryption. Announced in January 2018, the WPA3 standard replaces WPA2 with several security enhancements.
   - **WPA2/WPA3-Mixed**: Allows mixed networks of WPA2- and WPA3-compliant devices. SAE FT and AKM PSK SHA256 is supported for Open authentication + WPA2/WPA3-Mixed encryption. **Enable 802.11r FT Roaming** is configurable for open authentication and WPA2/WPA3-Mixed encryption and 802.1X EAP authentication + WPA2/WPA3-Mixed encryption under **Advanced Options** > **Radio Control**. Refer to Radio Control Settings on page 284 for more information.
   - **OWE**: Opportunistic Wireless Encryption (OWE) provides encrypted communications for open networks.
   - **None**: No encryption; communications are sent in clear text.

6. For **Password**, enter a password (WPA2), an SAE Password (WPA3), or both for a WPA2/WPA3-Mixed WLAN. If the Encryption method is **OWE** or **None**, no password is required.

   Click **Show QR Code** to display the QR code page. The user can save or print the QR code.

   FIGURE 90 Displaying QR Code Page

   (Optional) Select the **Allow Legacy devices to connect to this WLAN by previous password** check box.

   This option is available only for wireless clients that are marked as legacy devices in the **Clients** > **Wireless Clients** page. For more information, refer to "Marking a Client as a Legacy Device". If the **Allow Legacy devices to connect to this WLAN by previous password** check box is selected, under **Advanced Options** > **Zero-IT & DPSK**, **Dynamic PSK** is selected as **Internal**. You can change the password and Unleashed generates DPSK keys for all connected legacy devices with the previous password of the WLAN. For more information about internal DPSK, refer to Enabling DPSK for a WLAN on page 273. You can view all the generated DPSK keys in the **Admin & Services** > **Services** > **Dynamic PSK** > **Generated Dynamic PSKs** page.

7. Choose whether a **Web Authentication** (**Captive Portal**) will be used for web-based authentication.
8. If **802.1X EAP**, **MAC Address**, or **Web Authentication** (**Captive Portal**) is chosen, select a server from the **Authentication Server** from list.

   If an external authentication server is to be used rather than the internal database, click **Create Service** to create an AAA server object to authenticate against.

   NOTE
   Alternatively, you can create AAA servers on the **Admin & Services** > **Services** > **AAA Servers** page. For more information, refer to AAA Servers on page 410.

9. Click **OK** to save your changes and deploy the new WLAN.

   NOTE
   For advanced WLAN configuration options, refer to Advanced WLAN Configuration on page 269.

802.1X EAP WLANs

802.1X EAP (Extensible Authentication Protocol), or "WPA-Enterprise," is an IEEE Standard that provides a flexible and extensible authentication mechanism for devices attempting to connect to wired and wireless LANs.

802.1X provides secure connectivity by ensuring that every device must authenticate to an authentication server before it is allowed access to network resources. Authentication can be based on digital certificates, and granular policies can be designed to govern the level of access, and provide visibility and control over devices on the network.

The RUCKUS 802.1X implementation provides a means for the controller to connect to the RADIUS server after entering the server's IP address and shared secret. Specific instructions for RADIUS server configuration vary depending on the RADIUS server software used, and are therefore beyond the scope of this document.

802.1X WLAN Survivability

The WLAN Survivability feature allows 8021X end users to continue to authenticate successfully and access the internet even when the external RADIUS server is unreachable for a configurable period of time.

With this feature enabled, the RUCKUS device caches the user's credentials for reuse in the event of disconnection from the AAA server.

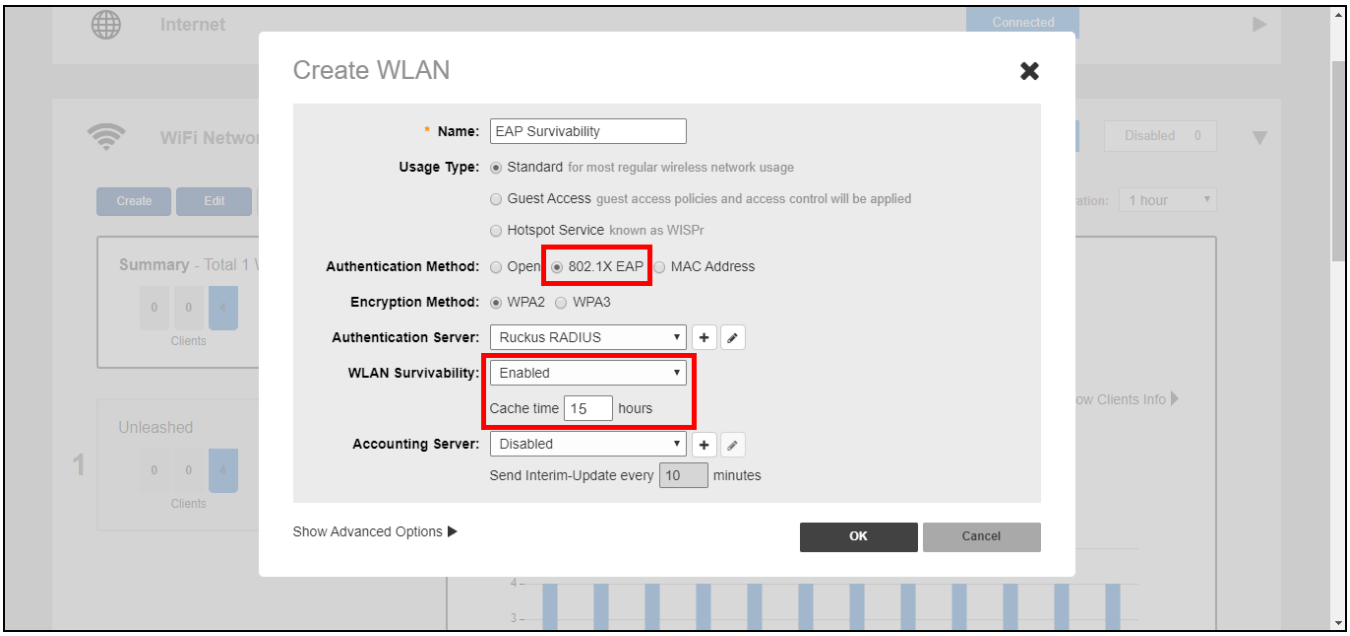
> **NOTE**
> Enabling this feature on the Unleashed web interface will not work unless the relevant configuration is also performed on the RADIUS server. This procedure assumes the reader has a high level of competence in RADIUS customization. Specifically, the user will need the ability to write scripts or code to recognize our RUCKUS RADIUS attributes and respond with the correct values by properly calculating the password and challenge strings.

To configure WLAN Survivability for 802.1X WLAN clients:

1. Go to **WiFi Networks > Create/Edit WLAN**.
2. In **Usage Type**, select **Standard**.
3. In **Authentication Method**, select **802.1X EAP**.
4. In **Authentication Server**, select or create a new RADIUS server to authenticate with.
5. In **WLAN Survivability**, select **Enabled**.
6. In **Cache Time**, enter a value in hours (1-128) to cache the user credentials.

7. Click **OK** to save your changes.

FIGURE 91 Enable 802.1X WLAN survivability



8. The RUCKUS controller will send the RADIUS request with the attribute: `RADIUS_RUCKUS_AUTH_SURVIVABILITY = 15` after enabling the survivability feature.
9. The RADIUS server must have the capability of recognizing the request and answering with the following attributes in the access-accept message: `RADIUS_RUCKUS_USER_NAME = 16 , /*Survivability-Usr-Name*/ RADIUS_RUCKUS_PASSWORD_NT_HASH = 17 /*Survivability-MD5-NT-Passwd*/.`

10. How the RADIUS server calculates the two new attributes:
    - `RADIUS_RUCKUS_USER_NAME`: This is the user name created in the RADIUS server.
    - `RADIUS_RUCKUS_PASSWORD_NT_HASH`: This is a 32 byte binary data value. RADIUS uses the following steps to create this attribute:
        a. The server generates a Windows NT hash of the user's password using the MS_CHAPv2 algorithm.
        b. It uses the first random 16 bytes as an authenticator and the shared secret to encrypt the data generated by the previous step via MD5 as a user password does (refer to RFC 2865, Chapter 5.2). The following is a code snippet of the user password encryption algorithm:

```
struct radius_attr_hdr *
radius_msg_add_attr_user_password(struct radius_msg *msg,
                  TAC_U8 *data, size_t data_len,
                  TAC_U8 *secret, size_t secret_len)
{
    TAC_U8 buf[128];
    int padlen, i, pos;
    MD5_CTX context;
    size_t buf_len;
    TAC_U8 hash[16];

    if (data_len > 128)
        return NULL;

    memcpy(buf, data, data_len);
    buf_len = data_len;

    padlen = data_len % 16;
    if (padlen) {
        padlen = 16 - padlen;
        memset(buf + data_len, 0, padlen);
        buf_len += padlen;
    }

    MD5Init(&context);
    MD5Update(&context, secret, secret_len);
    MD5Update(&context, msg->hdr->authenticator, 16);
    MD5Final(hash, &context);

    for (i = 0; i < 16; i++)
        buf[i] ^= hash[i];
    pos = 16;

    while (pos < buf_len) {
        MD5Init(&context);
        MD5Update(&context, secret, secret_len);
        MD5Update(&context, &buf[pos - 16], 16);
        MD5Final(hash, &context);

        for (i = 0; i < 16; i++)
            buf[pos + i] ^= hash[i];

        pos += 16;
    }

    return radius_msg_add_attr(msg, RADIUS_ATTR_USER_PASSWORD,
                   buf, buf_len);
}
```

        c. Replace `msg->hdr->authenticator` with that first 16 bytes of random data.
        d. Place the results into the second 16 bytes.

        NOTE
        This feature is unavailable when a Backup RADIUS server is configured.

Guest WLANs

By creating a guest WLAN, visitors to your organization can be allowed limited (or unlimited) access to your wireless network, with configurable guest access policies.

Visitors can be given the option to self-activate their devices using social media login, a self-service Guest Pass, or to self-authenticate to any of your internal WLANs using Zero-IT activation by way of the BYOD Onboarding Portal.

The following options are available for different types of guest WLANs:

- No authentication (open WLAN): Any client can connect, and no password is required.
- Social media login: Visitors log in using an existing social media account to access the wireless network.
- Authentication with shared key: Any client can connect using the same shared password.
- Authentication with unique key (Guest Pass): Guest Pass keys must be generated for each guest, either by an adminstrator (each Guest Pass must be generated by a Guest Pass operator), or using the self-service Guest Pass.

  Self-service Guest Pass users can self-authenticate their clients to the guest WLAN in one of two ways:

  - No sponsor approval: No restrictions. Any client can request a Guest Pass, and it will be provided immediately.
  - Sponsor approval: Guests are required to request a Guest Pass, which must be approved by a sponsor before being delivered to the user by way of email or SMS.

Deploying a Guest WLAN

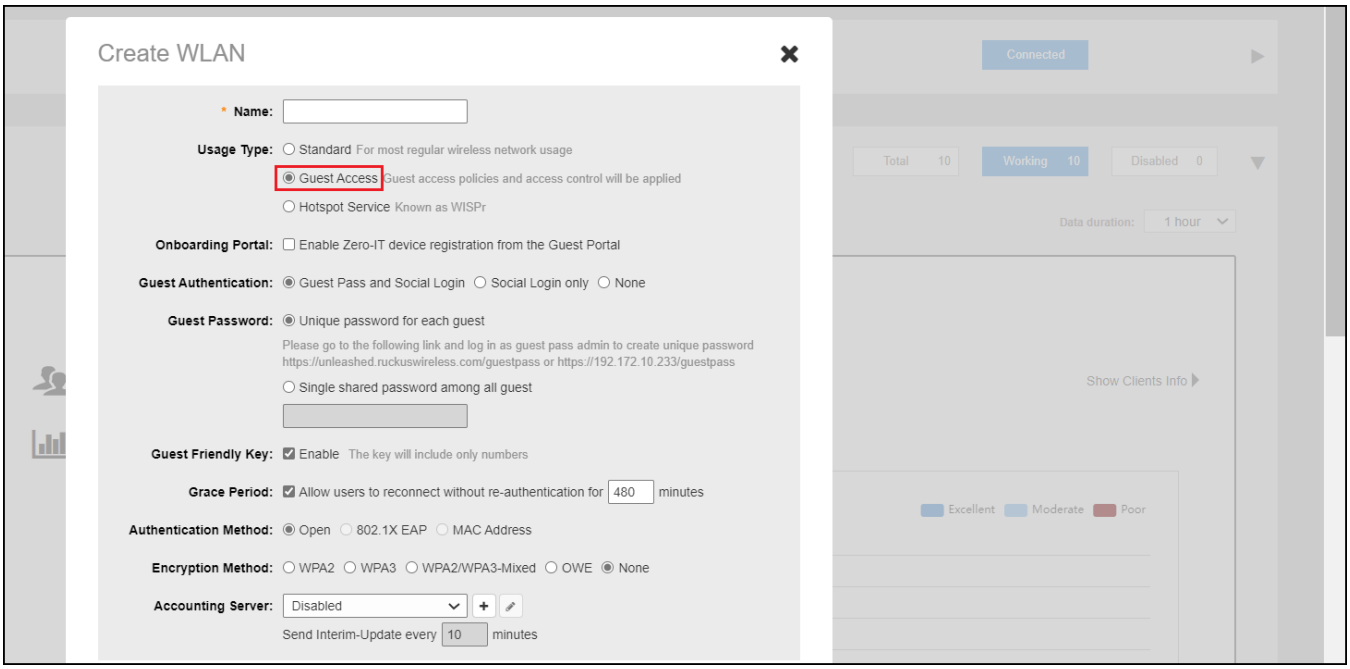
Extensive options are provided for customizing guest wireless networks, both in terms of how users connect, and what access privileges they are given once connected.

Complete the following steps to deploy a guest WLAN.

1. Go to **Wi-Fi Networks** > **Create**.

2. Enter a name for the guest WLAN.

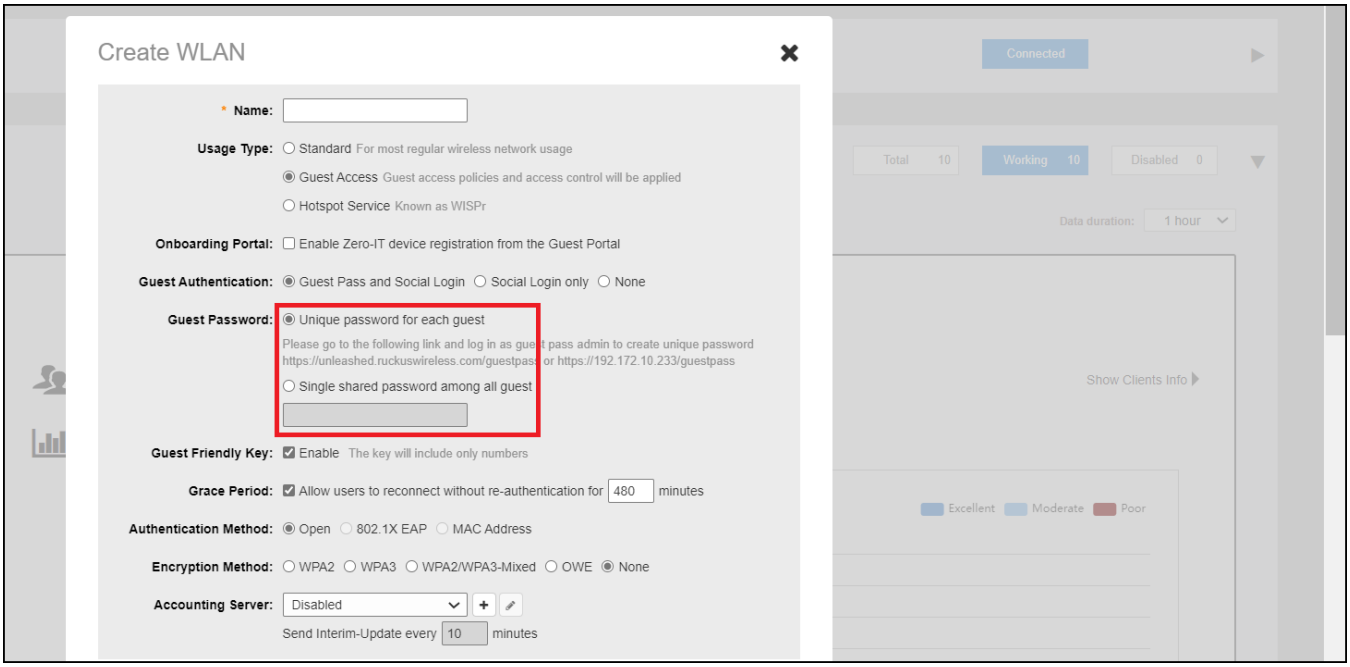
FIGURE 92 Creating a New Guest WLAN



3. For **Usage Type**, select **Guest Access**.
4. In **Onboarding Portal**, select whether to allow guests the option to register their devices on your internal (non-guest) WLANs using the Onboarding Portal. For more information, refer to Using the BYOD Onboarding Portal on page 211.
5. For **Guest Authentication**, select **Guest Pass and Social Login** (allows social media login and Guest Pass), **Social Login only** (social media login only), or **None** (no password required).

6. For **Guest Password**, if you selected **Guest Pass and Social Login** for **Guest Authentication**, select one of the following options:
   - **Unique password for each guest**: Guest Passes must first be generated, in batch or individually, for each visitor before they will be able to log in using a Guest Pass. For more information, refer to Working with Guest Passes on page 216.
   - **Single shared password among all guests**: This option allows you to skip the Guest Pass requirement, and simply provide a single password for all visitors.

   FIGURE 93 Selecting a Single Shared Password or Unique Password for Each Guest



7. For **Guest Friendly Key**, select **Enable** to include only numbers in the guest-friendly key.

   NOTE
   By default, the guest-friendly key is enabled when a user creates a new WLAN with guest access (**Guest Authentication** is set to **Guest pass** and **Social login**).

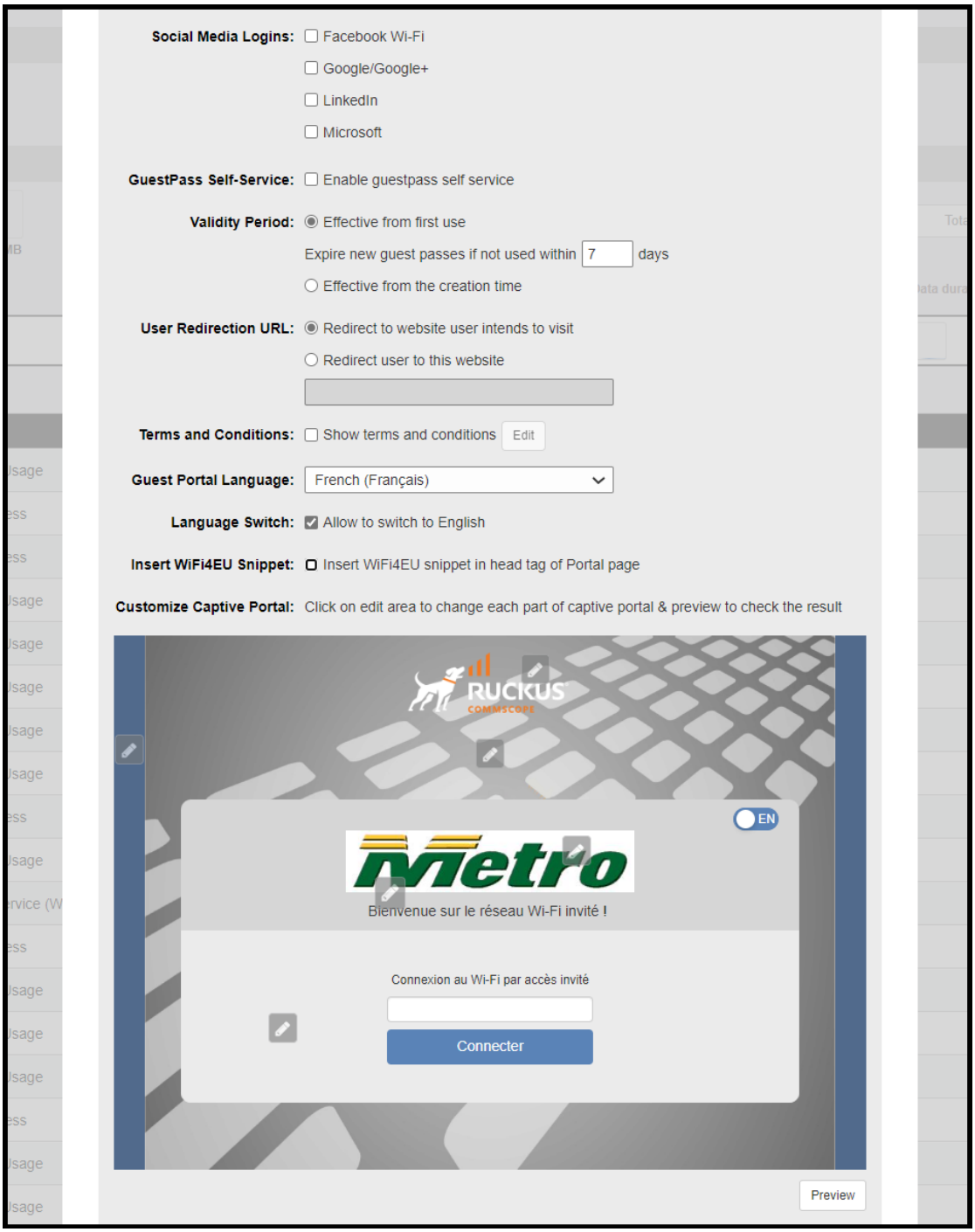
   NOTE
   The guest-friendly key is disabled in the guest access WLAN during migration.

8. For **Grace Period**, enter a value in minutes to allow users to reconnect without re-authentication. Clear the check box to disable the grace period.
9. For **Authentication Method**, **Open** is the only option available for Guest WLAN and is selected by Default.
   - **Open**: No authentication method is used. Open authentication allows the use of WPA2, WPA3, WPA2/WPA3-Mixed, OWE, or no encryption. Open authentication + WPA2 encryption (also known as WPA-PSK) is the most common type of WLAN encryption method and should be the default configuration if there are no special requirements for authentication or encryption.

10. For **Encryption Method**, select one of the following options:
    - **WPA2**: Encrypts wireless traffic with WPA2 encryption. If this option is selected, users will still be required to enter the WPA2 passphrase to access the open guest WLAN, even with **None** selected as the guest authentication type.
    - **WPA3**: Announced in January 2018, the WPA3 standard replaces WPA2 with several security enhancements.
    - **WPA2/WPA3-Mixed**: Allows mixed networks of WPA2- and WPA3-compliant devices.
    - **OWE**: Opportunistic Wireless Encryption (OWE) provides encrypted communications for open networks.
    - **None**: Without encryption, anyone can access this WLAN with no passphrase or Guest Pass login required. (Guests may still be required to visit a captive portal landing page, if configured.)
11. For **Accounting Server**, select an accounting server from the list or click the **+** icon to create a new RADIUS accounting server entry.
12. (Optional) Click **Show Advanced Options**, and configure any advanced options, such as restricted subnet access, WLAN priority, access controls, application visibility, and so on. Refer to Advanced WLAN Configuration on page 269 for more information.
13. Click **Next**.

14. Customize the guest WLAN by configuring the following options:

FIGURE 94 Configuring the Guest WLAN



- **Social Media Logins**: Allow users to log in using their social media accounts. Refer to Social Media WLANs on page 242.
- **Guest Pass Self-Service**: Allow users to self-authenticate their clients to your guest WLAN using a Guest Pass generated automatically for each guest user. For more information, refer to Guest Pass Self-Service on page 218.

- **Validity Period**: Click **Effective from first use** to make the Guest Pass valid on first use or click **Effective from the creation time** to make the Guest Passes valid from the time they are created. If you select **Effective from first time**, enter a value for the number of days after which the Guest Passes will expire if not used.
- **User Redirection URL**: Click **Redirect to website user intends to visit** to redirect to the website the user intended to visit after successful login or click **Redirect user to this website** to redirect the user to a specified URL. If you select **Redirect user to this website**, enter the URL of the website in the field.
- **Terms and Conditions**: Choose whether to display the terms and conditions before guests can access your network. You can also edit the default terms and conditions by clicking **Edit**, and replacing the default text with any text you choose.
- **Guest Portal Language**: Select your preferred guest portal language for guest WLAN configuration.

  NOTE
  The default language is the same as the system language. The guest portal preview page and the guest portal page will follow the guest portal language in the WLAN. The guest portal language will not work on customized text.

  NOTE
  The portal language is not applicable for the following two types of guest WLANs:

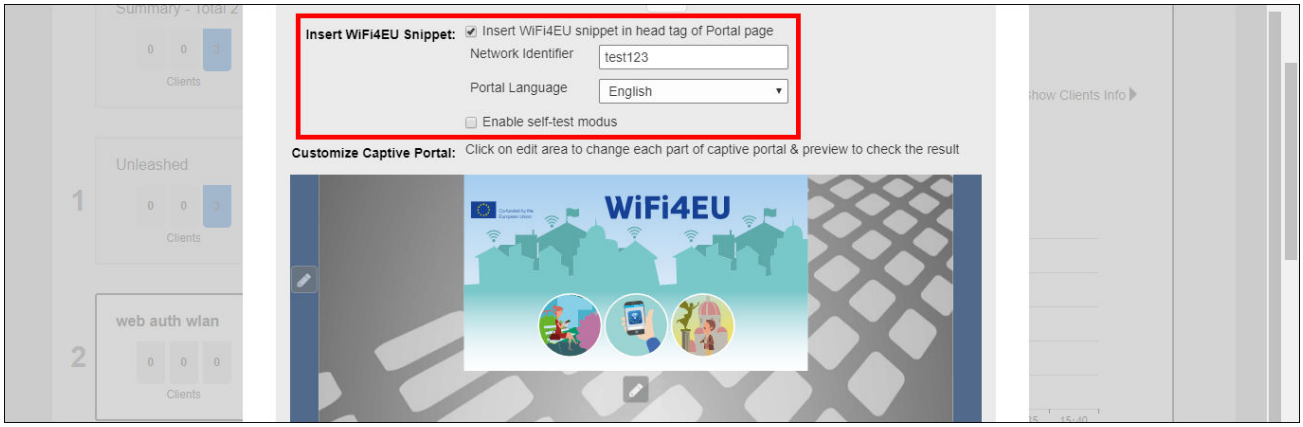
  - A Facebook login for the guest WLAN only.

    NOTE
    The portal language is supported if the Facebook login method is combined with other login options.

  - A no-authentication guest WLAN without **Terms and Conditions** and **Customize Captive Portal**.

- **Language Switch**: This option is available only when the selected guest portal language is not English and this option is selected by default. Only when the **Language Switch** option is selected, the **English (EN)** toggle switch will be displayed in the guest portal page. You can change the portal language between the default language and English.
- **Insert WiFi4EU Snippet**: Select the check box to insert a WiFi4EU snippet in the head tag of the web authentication portal page. This allows the WLAN to be used by members of the WiFi4EU "digital single market" for EU member states.

  FIGURE 95 Inserting a WiFi4EU Snippet



- **Customize Captive Portal**: Click the edit icons to customize the banner, background image, background color, logo, welcome message, and opacity level. Click **Preview** to preview your changes.

15. Click **OK** to save your changes.

16. The next screen prompts you to begin the configuration for email and SMS delivery of Guest Passes. Click **Yes** to configure email and SMS settings, or click **No** to skip this step.

    You can configure these settings later from the **Admin & Services** page, if you prefer. Refer to Configuring Email Server Settings on page 204 for more information.

    FIGURE 96 Configuring Email and SMS Delivery Settings

Configuring Email Server Settings

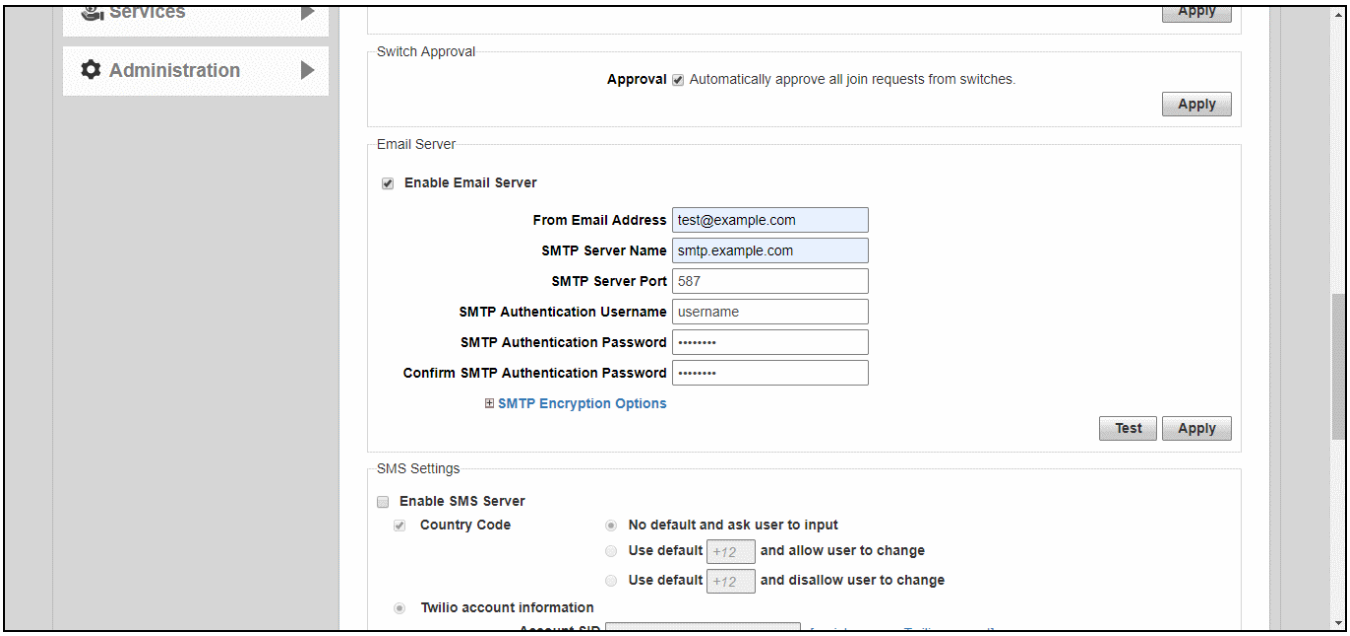
In order for Unleashed to send guest pass codes to guest users via email, it needs to have an email server configured.

To configure email server SMTP settings:

1. Go to **Admin & Services > System > System Info**.
2. In the **Email Server** section, enable the **Enable Email Server** check box, and then enter the following:
   - **From email address**: Type the email address from which Unleashed will send email messages.
   - **SMTP Server name**: Type the full name of the server provided by your ISP or mail administrator. Often, the SMTP server name is in the format smtp.company.com.
   - **SMTP Server port**: Type the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is 465 or 587. The default SMTP port value is 587.
   - **SMTP Authentication username**: Type the user name provided by your ISP or mail administrator. This might be just the part of your email address before the @ symbol, or it might be your complete email address. If you are using a free email service (such as Hotmail or Gmail), you typically have to type your complete email address.
   - **SMTP Authentication password**: Type the password that is associated with the user name above.
   - **Confirm SMTP Authentication password**: Retype the password you typed above to confirm.
   - **SMTP Encryption Options**: If your mail server uses TLS encryption, click the SMTP Encryption Options link, and then select the TLS check box. Additionally, select the STARTTLS check box that appears after you select the TLS check box. Check with your ISP or mail administrator for the correct encryption settings that you need to set.

3. To verify that Unleashed can send email messages using the SMTP settings you configured, click the **Test** button.
   - If Unleashed is able to send the test message, the message `Success!` appears at the bottom of the Email Notification page.
   - If Unleashed is unable to send the test message, the message `Failed!` appears at the bottom of the Email Notification page. Go back to the previous step, and then verify that the SMTP settings are correct.
4. Click **Apply**. The email server settings you configured become active immediately.

FIGURE 97 Email Server settings



Configuring SMS Server Settings

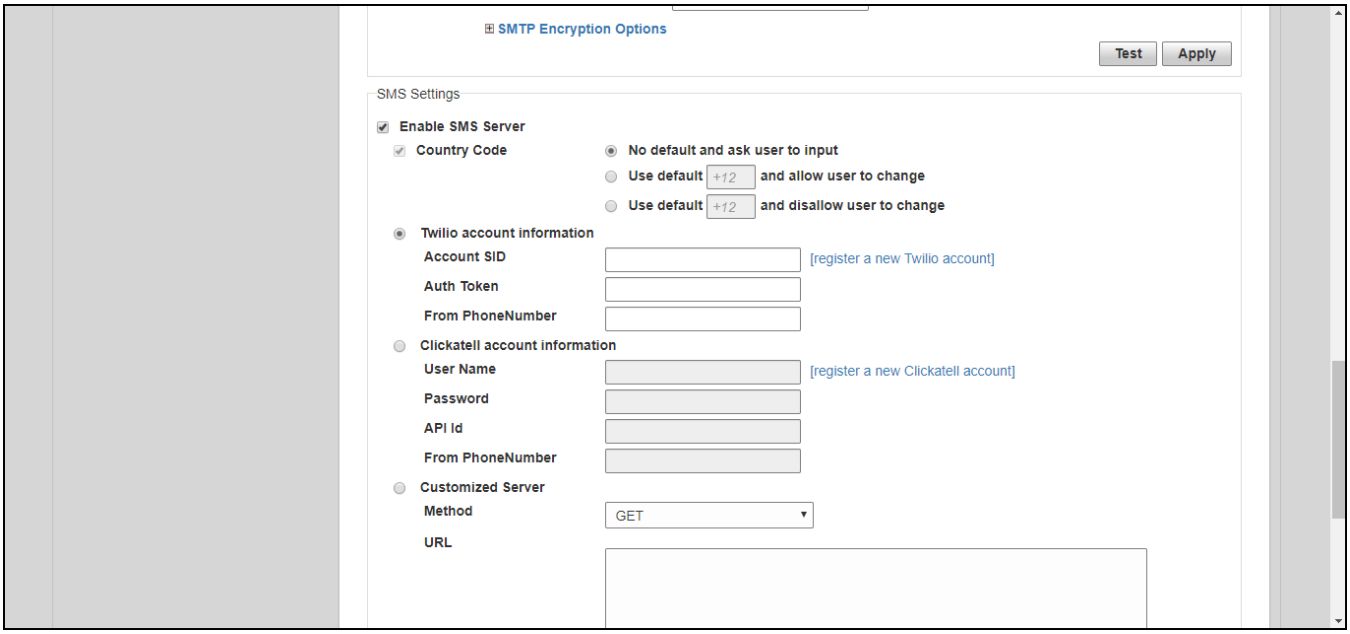
In order for Unleashed to send guest pass codes to guest users via SMS, it needs to have an SMS server configured.

To configure SMS server settings:

1. Go to **Admin & Services > System > System Info**.
2. In the **SMS Settings** section, enable the **Enable SMS Server** check box.
3. In **Country Code**, select one of the following options:
   - **CountryCode**: This option is only available with "Customized Server" SMS server type (for Twilio and Clickatell, the country code is mandatory and cannot be unchecked). When unchecked, the guest registration page does not support country code input.
   - **No default and ask user to input**: The guest registration page does not provide a default country code and the guest user is asked to input one.
   - **Use default and allow user to change**: The guest registration page provides a default country code and allows the guest user to change it.
   - **Use default and disallow user to change**: The guest registration page provides a default country code and the guest user is not allowed to change it.
4. Select **Twilio**, **Clickatell**, or **Customized Server**, depending on your SMS service provider.

5. Enter your **Account SID**, **Auth Token** and **From Phone Number** (Twilio) or your **User Name**, **Password** and **API ID** (Clickatell), or **Method** (Get or Post) and the URL for a custom SMS service provider.
6. Click the **Test** button to test your settings.
7. Once confirmed, click **Apply** to save your changes.

FIGURE 98 Configuring SMS settings



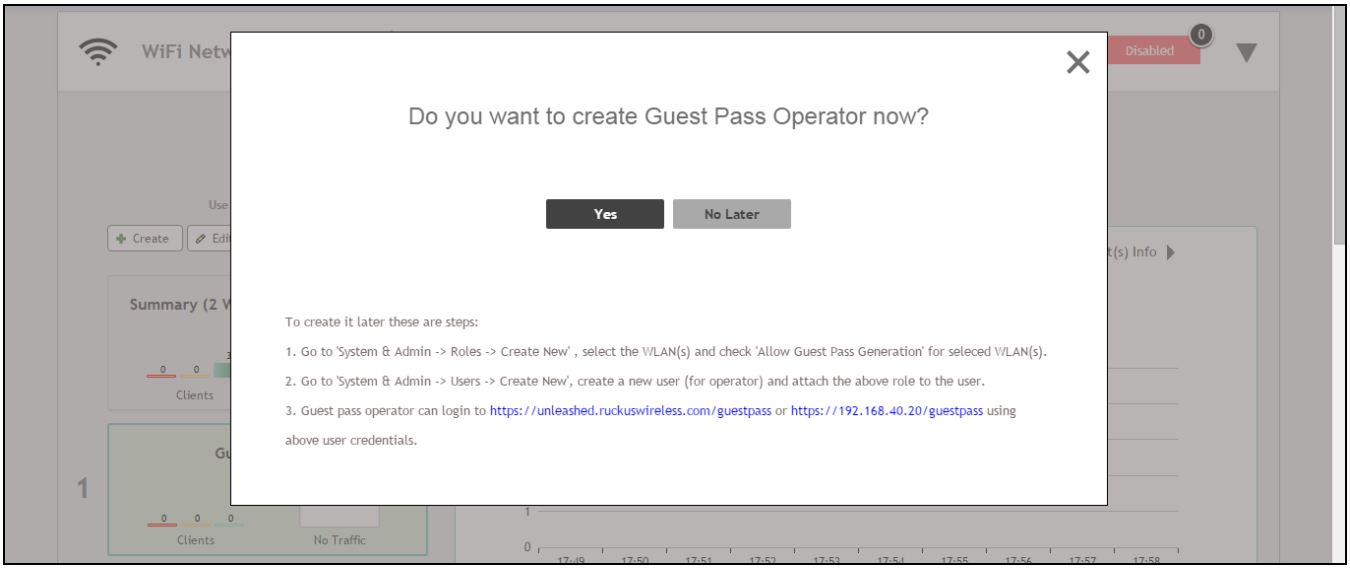
Creating a Guest Pass Operator

Guest Pass Operators are individuals within an organization who have the authority to generate guest passes for visitors.

This task describes how to create a user role for a category of user that is allowed to generate and manage guest passes.

1. After configuring Email and SMS settings, you will be prompted to configure a Guest Pass Operator.

   FIGURE 99 Optionally Configuring a Guest Pass Operator Now

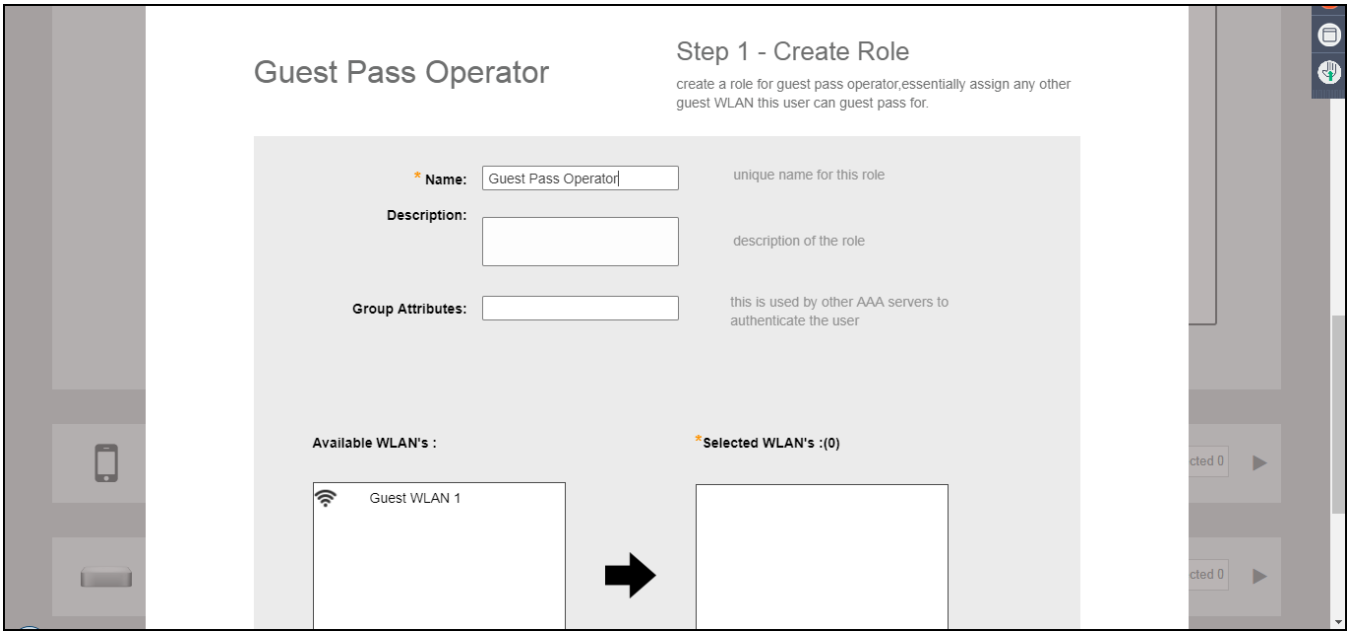


2. Click **Yes** to configure this role now. Or click **No Later** to configure these settings later.

   NOTE
   To configure additional operator roles, go to **Admin & Services > System > Roles > Create New**, select the guest WLAN(s) to allow, and check **Allow Guest Pass Generation** for the selected WLAN(s).

3. If you clicked **Yes**, you will be presented with the **Guest Pass Operator** configuration screen. Use this screen to configure the following options:
   - **Name**: Enter a unique name for the operator role.
   - **Description**: Optional description of the role.
   - **Group Attributes**: Used by AAA servers to authenticate the user.
   - **Available WLANs**: The list of available WLANs that the operator is allowed to choose from.
   - **Selected WLANs**: The list of WLANs for which the operator can issue guest passes.

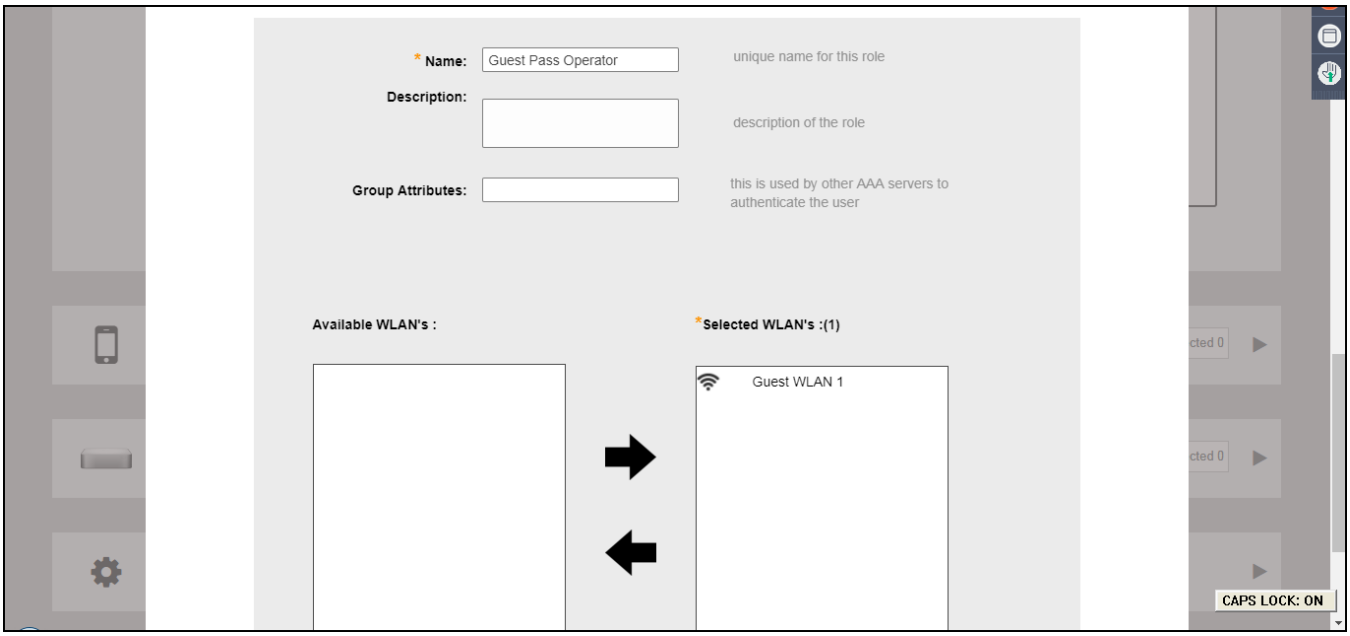
   FIGURE 100 Create Guest Pass Operator - Step 1



4. Use the arrows to move WLANs to/from the list of **Available WLANs** to **Selected WLANs** for which the Guest Pass Operator will be allowed to issue guest passes. (The list of available WLANs only includes unique password type guest WLANs.)

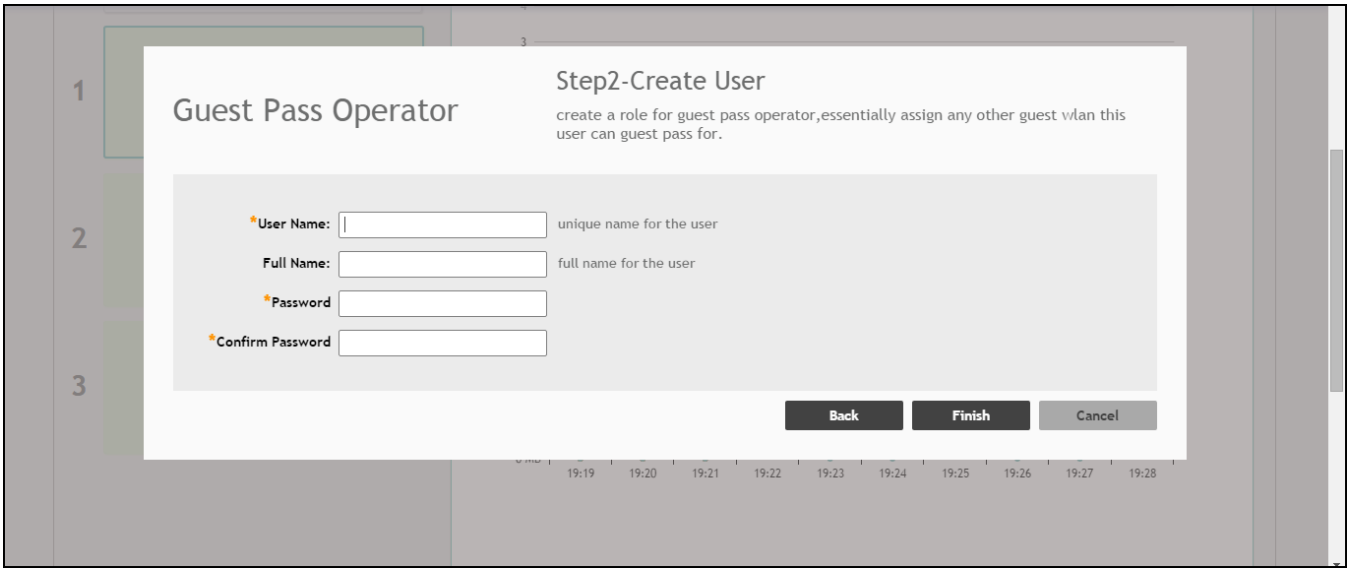
5. Click **Next** to continue.

FIGURE 101 Moving WLANs from Available to Selected



6. On the next screen that appears, **Guest Pass Operator - Step 2: Create User**, enter a user name and password to create a user with this role.

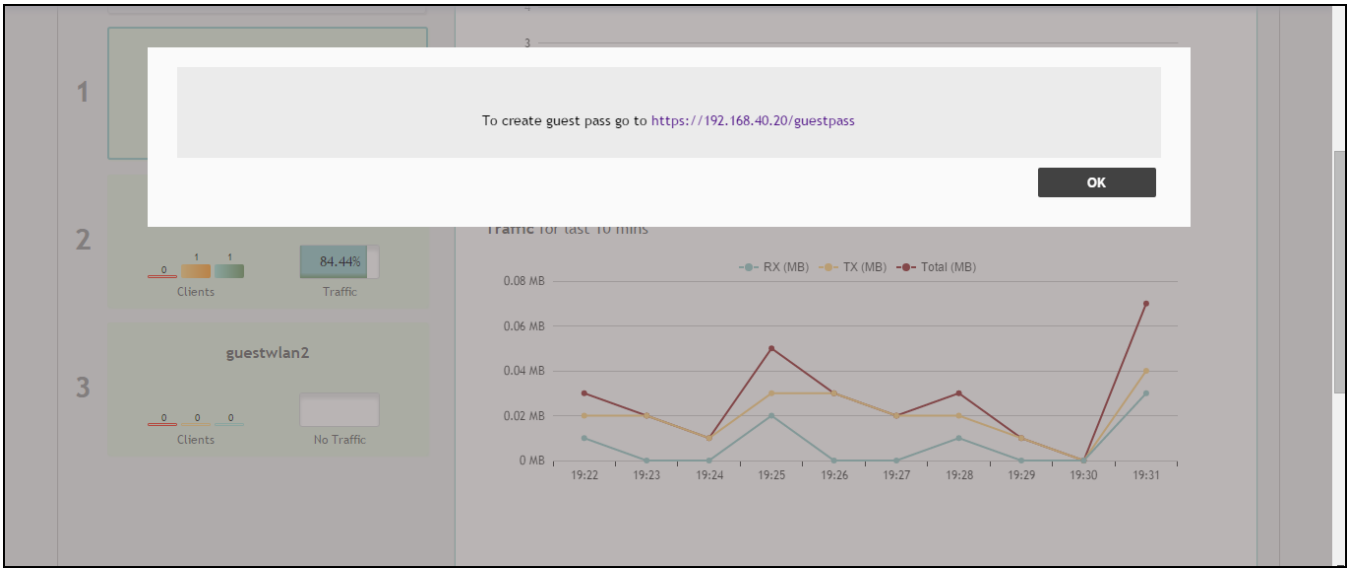
FIGURE 102 Create Guest Pass Operator - Step 2



7. You have completed creating a user with the Guest Pass operator role. The confirmation screen displays the URL where this user can create guest passes.

   NOTE
   Users with the Guest Pass operator role can login to *https://unleashed.ruckuswireless.com/guestpass* or *https://[host_ip_address]/guestpass* using the above user credentials.

   FIGURE 103 Guest pass operator created, to create a guest pass go to URL



8. To create additional users for the operator role, go to **Admin & Services > System > Users > Create New**, and attach the above role to the user.

Configuring Guest Subnet Restrictions

By default, guest pass users are automatically blocked from the Unleashed network subnet (format: A.B.C.D/M) and the subnet of the AP to which the guest user is connected.

If you want to create additional rules that allow or restrict guest users from specific subnets, use the **Restricted Subnet Access** section.

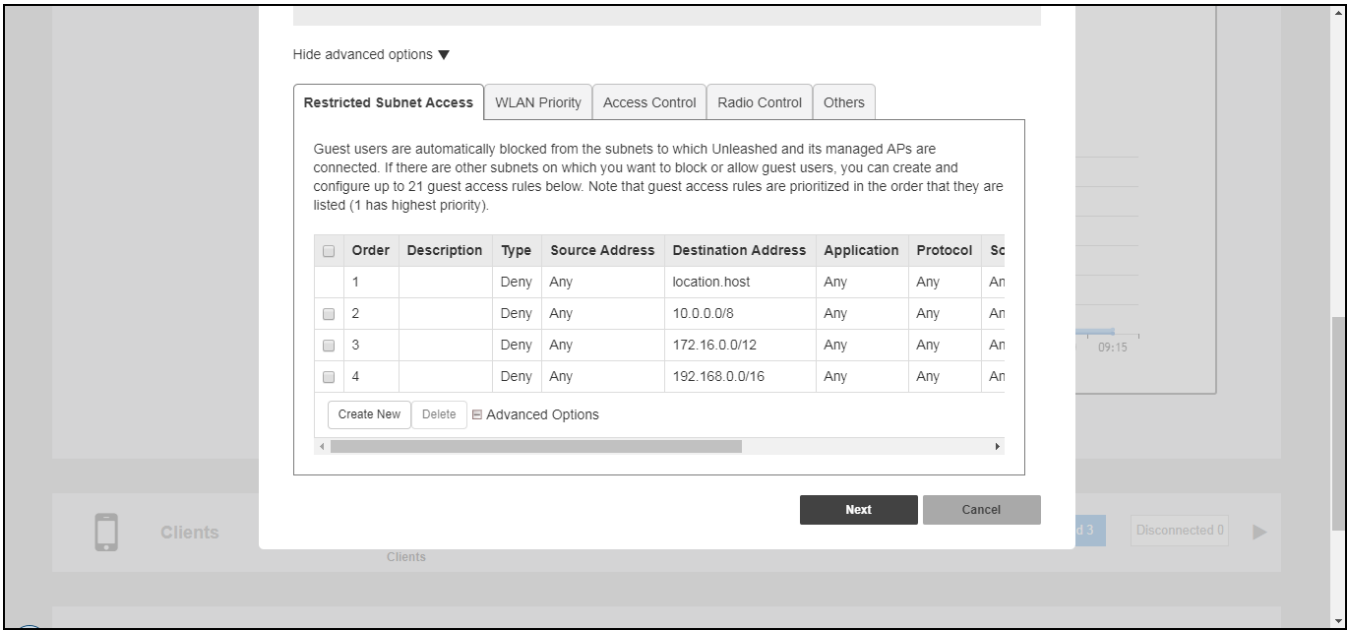
You can create up to 32 subnet access rules, which will be enforced both on both the Unleashed Master AP and all connected member APs.

To create a guest access rule for a subnet:

1. Go to **Wi-Fi Networks** and click **Create** to create a new guest WLAN, or **Edit** to modify an existing guest WLAN.
2. In **Usage Type**, ensure that **Guest Access** is selected.
3. Click the arrow next to **Show Advanced Options** to expand the advanced options section.
4. Click the **Restricted Subnet Access** tab.
5. Click **Create New** to create a new subnet restriction. Text boxes appear under the table columns in which you can enter parameters that define the access rule.
6. Under **Description**, type a name or description for the access rule that you are creating.
7. Under **Type**, select Deny if this rule will prevent guest users from accessing certain subnets, or select Allow if this rule will allow them access.

8. Under **Source Address**, type the IP address and subnet mask (format: A.B.C.D/M) from which you want to allow or deny users access.
9. Under **Destination Address**, type the IP address and subnet mask (format: A.B.C.D/M) to which you want to allow or deny users access.
10. If you want to allow or restrict subnet access based on the application, protocol, or source or destination port used, click the **Advanced Options** link, and then configure the settings.
11. Click **Save** to save the subnet access rule.
12. Repeat Steps 5 to 11 to create up to 22 subnet access rules.

FIGURE 104 Configuring guest Restricted Subnet Access



Using the BYOD Onboarding Portal

The Onboarding Portal feature provides a series of intuitive option screens allowing mobile users to choose whether to connect devices to a Guest WLAN or to self-configure their mobile devices to authenticate to an internal WLAN using Zero-IT activation.

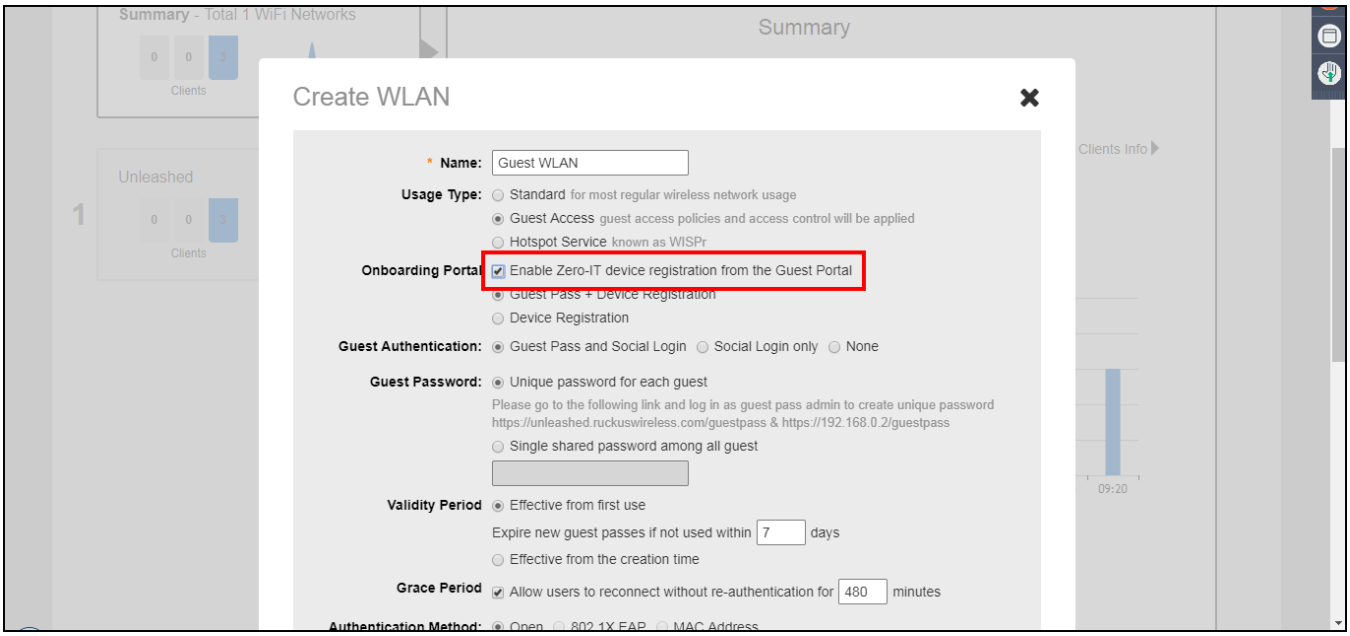
To enable the Onboarding Portal for mobile devices:

1. Expand the **Wi-Fi Networks** section of the Dashboard.
2. Select an existing guest WLAN and click **Edit** or click **Create** to configure a new guest WLAN.
3. Enable the check box next to **Onboarding Portal** to enable Zero-IT device registration from the Guest Portal.
4. Select one of the following options to display when connecting to the Onboarding Portal:
   - **Guest Pass + Device Registration**: Show both buttons.
   - **Device Registration**: Show Zero-IT Device Registration button only.
5. If **Guest Pass** is enabled, configure Guest Pass options as described in Working with Guest Passes on page 216.
6. Click **Next** to continue to the next guest WLAN configuration page.

7. Optionally, configure additional guest WLAN settings, and click **OK** to apply.

   NOTE
   For information on these settings, see Deploying a Guest WLAN on page 198.

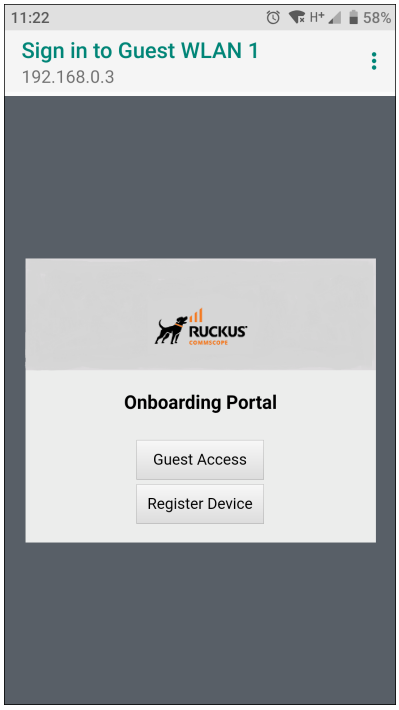
FIGURE 105 Enabling Onboarding Portal



When a client connects to the open Guest WLAN for the first time, the RUCKUS **Onboarding Portal** page is displayed. The screen displays one or both of the following options, depending on your choice in Step 4 above:

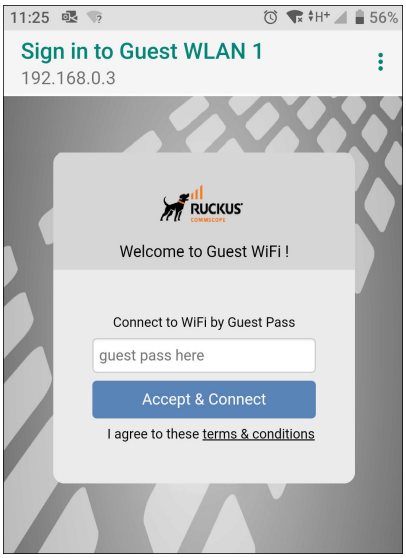
- **Guest Access**: Connect this device to a guest WLAN.
- **Register Device**: Download a Zero-IT activation file to register this device for access to one or more internal WLANs.

FIGURE 106 The Onboarding Portal for Mobile Devices



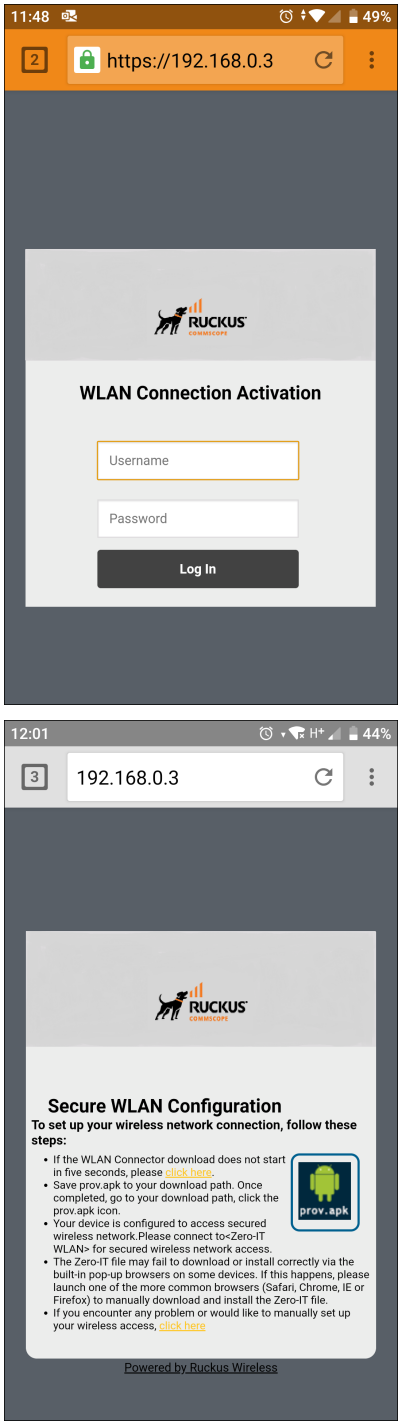
If the user clicks the **Guest Access** button, the process is the same as when connecting to a Guest WLAN and all settings on the **Guest Access** configuration page will be put into effect.

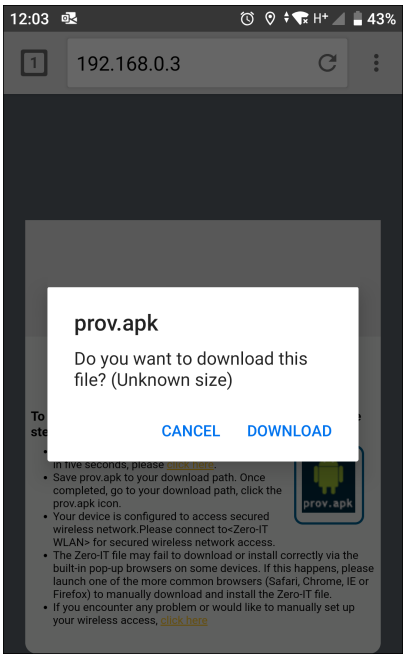
FIGURE 107 Guest Access Welcome Page



If the user clicks the **Register Device** button, the web page will be redirected to the **WLAN Connection Activation** page, from which the user can enter user name and password to activate this device. A Zero-IT activation file is generated for download once the client device is registered with Unleashed.

FIGURE 108 Activating the Device Using the WLAN Connection Activation Screen, and Downloading Activation File



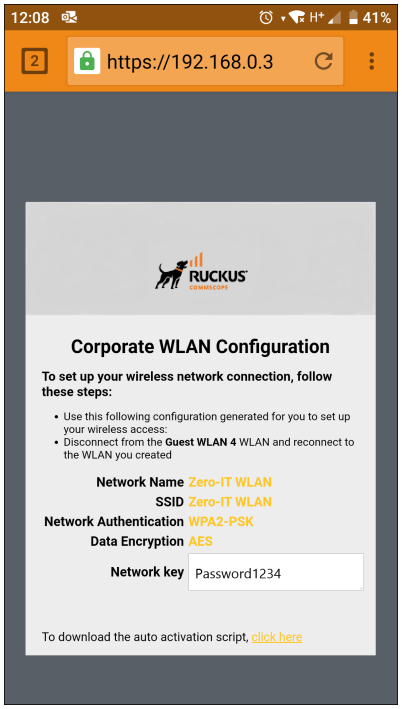


After running the downloaded Zero-IT file, the device will be configured with the settings to automatically connect to the secure internal/corporate WLAN.

NOTE
You may need to manually switch from the guest WLAN to the secure WLAN after activation (on some mobile devices).

NOTE
You may need to manually delete any previously installed Zero-IT activation files before a new one can be run. On some devices (including some Android versions), the activation file will not run if an older existing package of the same name with a conflicting signature is already installed.

FIGURE 109 If Zero-IT activation file cannot be run, manually copy/paste the Network Key



Working with Guest Passes

Guest passes are temporary privileges granted to guests to allow access your wireless LANs.

Unleashed provides many options for customizing guest passes, controlling who is allowed to issue guest passes, and controlling the scope of access to be granted.

With Guest Pass authentication enabled, guests are required to enter a guest pass code when connecting to a guest WLAN. Temporary guest passes can be issued for single users, multiple users, one-time login, time-limited multiple logins for a single guest user, or can be configured so that a single guest pass can be shared by multiple users. Additionally, they can be batch generated if many short-term guest passes need to be created at once.

Guest passes can be delivered in any of the following ways:

- Printout
- Send SMS with guest credentials
- Send email with guest credentials

NOTE
To enable guest pass delivery via email or SMS, you must first configure an email server or an SMS delivery account (Twilio or Clickatell) from the **Email** tab or the **SMS** tab.

Generating a Guest Pass

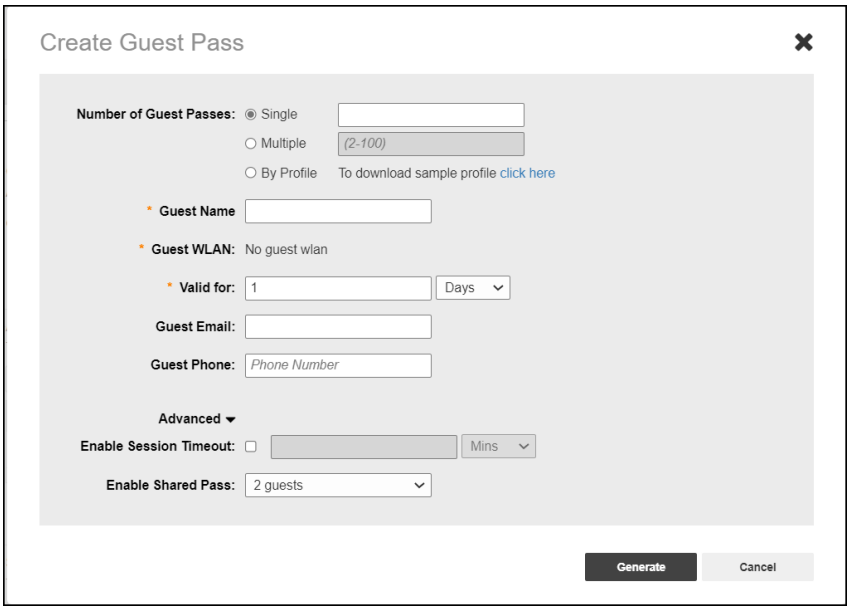
Using the **Guest Access Service > Admin Generated Guest Passes** page, Unleashed administrators can create guest passes from within the UI.

Complete the following steps to generate a guest pass.

1. From the dashboard, select **Admin & Services > Services > Guest Access Service**.

2. Under **Admin Generated Guest Passes**, click **Create** to create a guest pass.

FIGURE 110 Creating a Guest Pass



3. For **Number of Guest Passes**, select one of the following options:
   - **Single**: Generate a single guest pass. Refer to Generating and Delivering a Single Guest Pass on page 227.
   - **Multiple**: Generate multiple guest passes. Refer to Generating and Printing Multiple Guest Passes at Once on page 232.
   - **By Profile**: Import a guest pass profile. Refer to Creating a Guest Pass Profile on page 234.
4. Enter the guest name.
5. For **Guest WLAN**, select the WLAN for which the guest pass will be issued. To create a guest WLAN, refer to Deploying a Guest WLAN on page 198.
6. In **Valid For**, enter a number and select a time interval (**Hours**, **Days**, or **Weeks**) for which the guest pass will remain valid.
7. (Optional) Enter a guest email address and guest phone number. If these options are entered, and the email server and SMS delivery method have been configured (from **Admin & Services > System > System Info**), you can deliver the guest pass to the guest using email or SMS.
8. (Optional) Under **Advanced Options**, configure the following options:
   - **Enable Session Timeout**: Select the check box and select a time interval (**Minutes**, **Hours**, **Days**, or **Weeks**) after which guests are required to log in again. If **Session Timeout** is disabled, the connected users are not required to log in again until the guest pass expires.
   - **Enable Shared Pass**: Allow multiple users to share a single guest pass.
9. Click **Generate** to create the guest pass.

10. On the **Create Guest Pass** page, select a delivery method:
    - Single
      - **Print passes now using Default template**: Print the guest pass to a printer.
      - **Text the pass to [phone]**: Deliver the guest pass code by way of an SMS text message to the phone number entered.
      - **Email the pass to [email]**: Deliver the guest pass code by way of an email message to the email address entered.
    - Multiple
      - **Print the passes now**
      - **Download all passes now**
      - **Show me all passes and let me decide to print/SMS/email passes**

Guest Pass Self-Service

The Guest Pass Self-Service feature allows guests to your organization to self-activate their devices to access your guest WLANs.

The Guest Pass Self-Service feature allows guests to connect to a guest SSID and submit basic information (name, email address and mobile phone number) to receive a guest pass code. The guest then enters this code to gain access to the internet, with no IT involvement required.

Using the default settings, a guest user connects to a self-service guest WLAN and enters his contact information to receive a guest pass code. The user then activates the guest pass, and can now freely use the internet.

Additional configuration options allow the administrator to set the guest pass delivery method (either displayed directly on the device screen, or sent to the user via email, SMS, or both) to set session length and access duration, and to require "sponsor approval" prior to providing a guest pass to the new guest user.

Enabling Guest Pass Self-Service

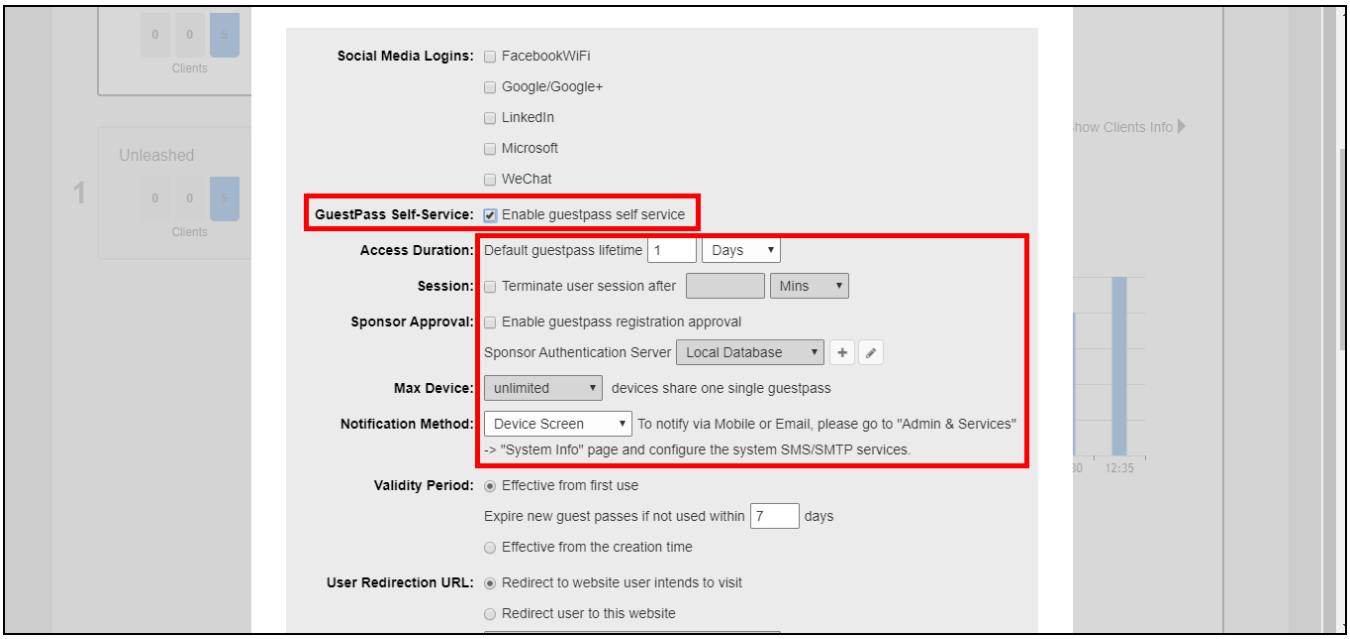
Use the following procedure to allow visitors to self-activate their devices to your Guest WLAN(s).

To enable Guest Pass Self-Service for a Guest WLAN:

1. Go to **Wi-Fi Networks**, and click **Create** to create a new guest WLAN, or **Edit** to edit an existing WLAN.
2. Enter a **Name** for the WLAN, and in **Usage Type**, select **Guest Access**.
3. Click **Next**. The second WLAN creation screen appears.

4. Locate the **Guest Pass Self-Service** option and select the **Enable guest pass self service** button. Additional options appear.

FIGURE 111 Select Enable Guest Pass Self Service



5. Configure the following options as required:
   - **Access Duration**: Select the default access time provided with one guest pass in days, hours or weeks. (Default is one day.)
   - **Session**: Optionally, enable the session limitation to require guest pass users to re-login after the specified time period.
   - **Max Device**: Allow multiple devices to share a single guest pass. (Default is unlimited.)
   - **Sponsor Approval**: Select this option to require email approval for issuing self-service guest passes. (See Requiring Sponsor Approval for Self-Service Guest Pass Authentication on page 219.)
   - **Notification Method**: Select whether the guest pass will be delivered via email, SMS, or displayed directly on the device screen. When Sponsor Approval is selected, the Device Screen option is not allowed.
6. Click **OK** to save your changes.

Requiring Sponsor Approval for Self-Service Guest Pass Authentication

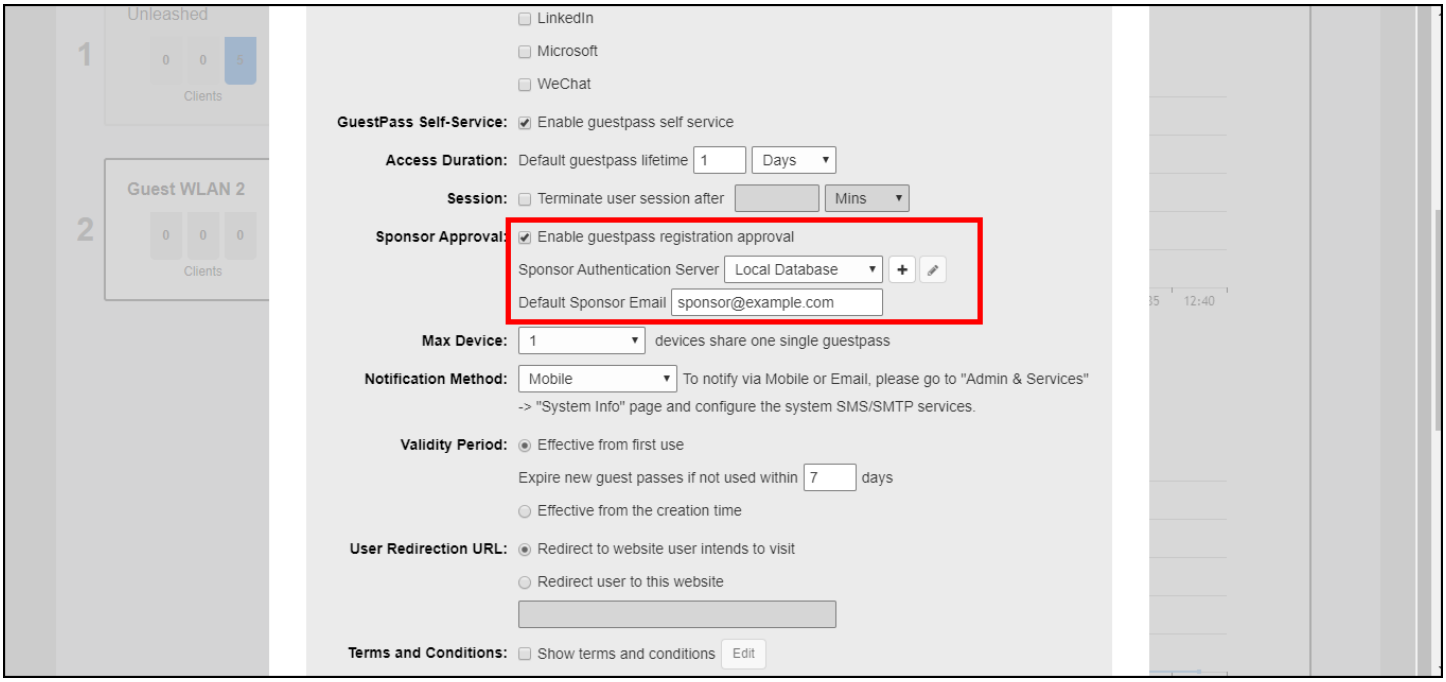
If the **Sponsor Approval** option is enabled, when the user connects to the WLAN, registration information must be submitted along with a sponsor's email address to await sponsor approval.

The Sponsor receives the email request and clicks a link to allow this user access to the guest WLAN. After the registration is approved, RUCKUS Unleashed generates a guest pass and sends it to the user through email or SMS (or both) using the contact information the user provided.

NOTE
If using sponsor approval, RUCKUS Unleashed must be configured with your SMTP settings for email delivery, or with a valid Twilio or Clickatell account to deliver guest passes through SMS. Refer to Customizing the Guest Pass Email Content on page 241 and Customizing the Guest Pass SMS Content on page 242 for more information.

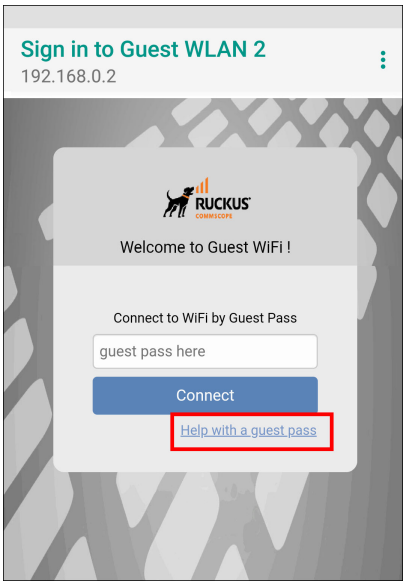
To configure sponsor approval, select the **Sponsor Approval** check box, select a sponsor authentication server (default is local database), and optionally enter a **Default Sponsor Email** address.

FIGURE 112 Enabling Sponsor Approval for Guest Pass Self-Service



When a user connects to a guest WLAN with Sponsor Approval enabled, the **Welcome to Guest WiFi** page allows the guest to request a self-service guest pass by clicking the **Help with a guest pass** link.

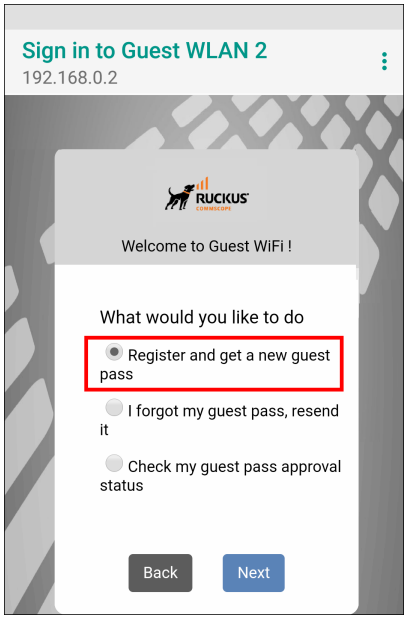
FIGURE 113 Requesting Help with a Guest Pass



Complete the following steps to request, approve, and activate a sponsor-approved guest pass:

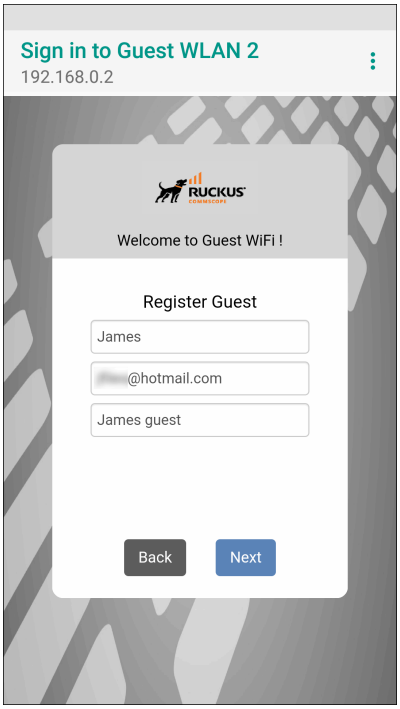
1. On the **What would you like to do** screen, select **Register and get a new guest pass**, and click **Next**.

   FIGURE 114 Requesting a New Guest Pass



2. Enter a username, an email address or phone number to which the guest pass key will be sent, and the sponsor's email address, and click **Next**.

   FIGURE 115 Registering as a Guest



   A guest pass request email is sent to the sponsor's address, and a message that the guest access request has been submitted is displayed.

FIGURE 116 Guest Pass Request Submitted Message

The sponsor will then receive an email requesting approval for guest pass activation.

FIGURE 117 Sponsor Accept Email

Dear Sponsor/Admin,

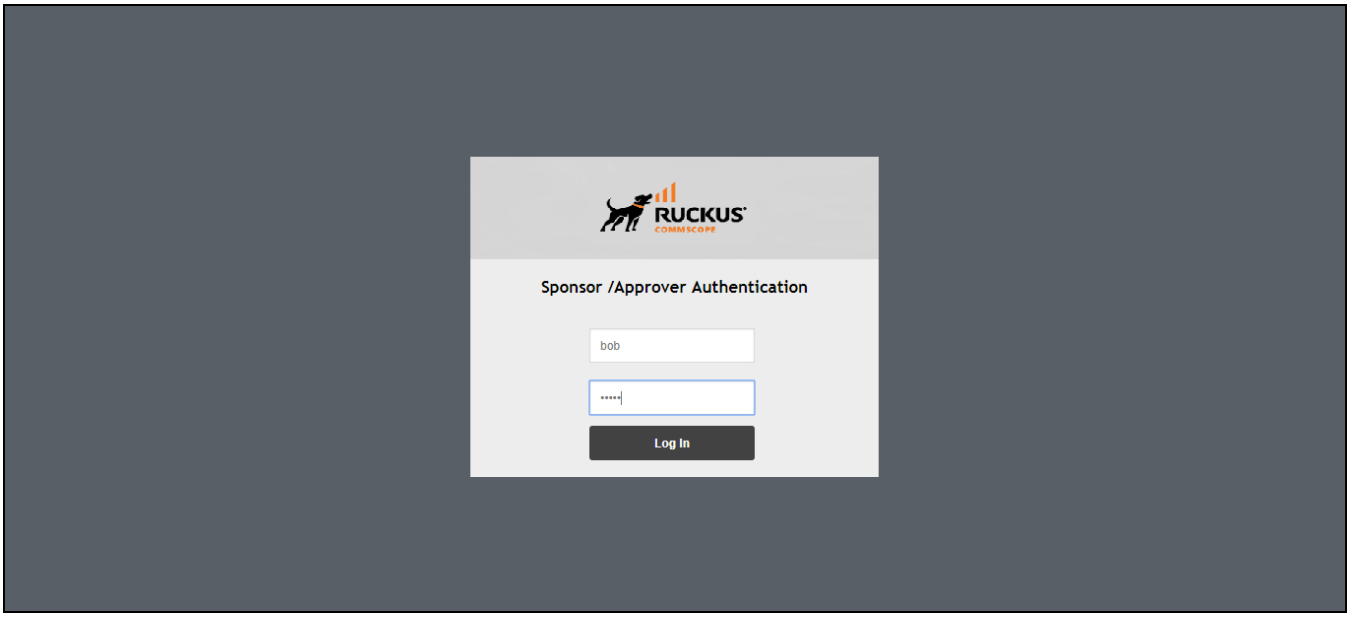
You are a designated approver for @hotmail.com's WiFi access. Click link below to approve or reject the request.
https://192.168.0.2/user/sponsor_login.jsp?email=GKGGGJGMGFHDEAGIGPHEGNGBGJGMCOGDGPGN&user=HDGMGJGOGHHDGBGOGEGBHCHCGPHHHDDBDAEAGIGPHEGNGBGJGMCOGDGPGN&ssid=EHHFGFHDHECAFHEMEBEOCADC
Name: @hotmail.com
Mobile No:
Email: @hotmail.com
SSID: Guest WLAN 2

3. As the sponsor opens the email and clicks the link to open the **Sponsor/Approver Authentication** page.

4. On the **Sponsor/Approver Authentication** page, enter a valid **User Name** and **Password** and click **Log in** to continue.

   NOTE
   This username and password must exist on the authentication server (Local Database, Active Directory, or RADIUS) configured for this guest access service.

FIGURE 118 Sponsor/Approver Login Page



5. Upon successful login, the **Guest Pass Approval** page displays the name, phone number, and email addresses of all pending guest pass requests. Select the check box next to each guest pass you wish to approve, set the **Duration** for each, and click **Approve** to approve them.

FIGURE 119 Guest Pass Approval

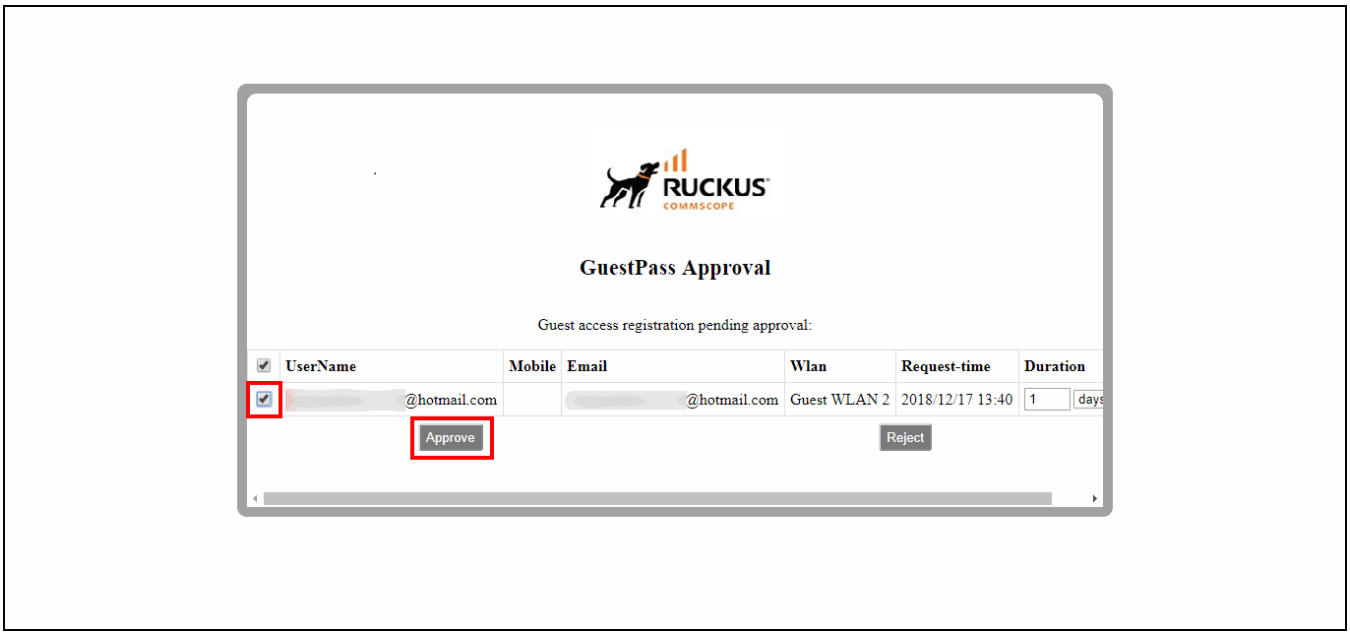
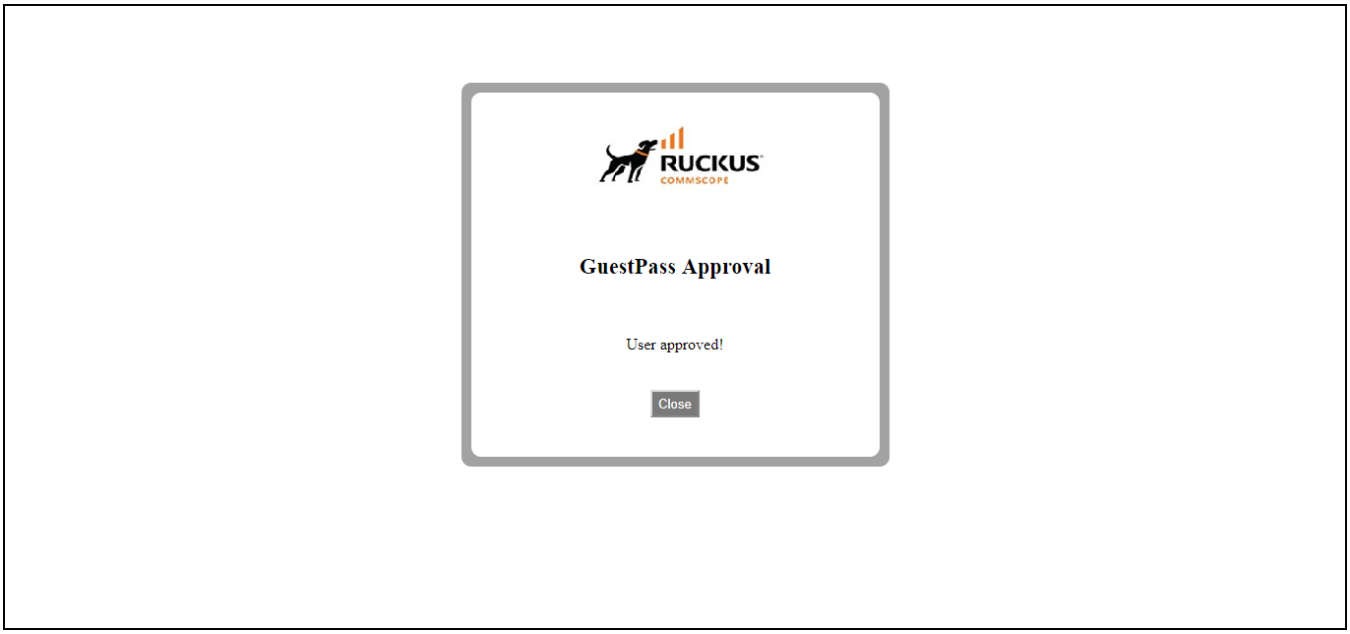


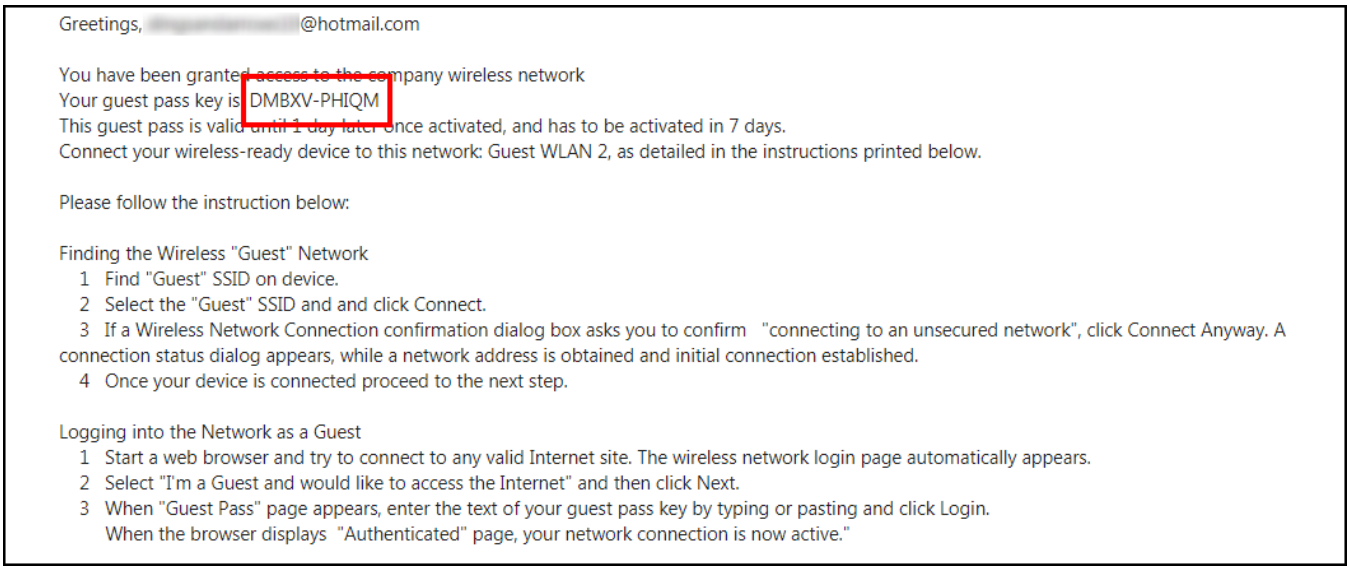
FIGURE 120 Guest Pass Approved Message



Approving a guest pass triggers delivery of an email or SMS (or both) message containing the guest pass code to the guest.

6. As a guest user, open the guest pass activation email message email and copy the Guest Pass code to the clipboard.

FIGURE 121 Guest Pass Activation Email Message



7. Launch a web browser and browse to any URL. You will be redirected to the **Welcome** login page.
8. Enter the Guest Pass code received in the activation email (or SMS), and click **Connect**.

FIGURE 122 Entering Guest Pass Code

You have successfully authenticated to this guest network using the guest pass provided.

Controlling Guest Pass Generation Privileges

By default, guest pass generation privileges are given to all authenticated users in the Default user role.

In order to change the guest pass generation privileges for a group of users, refer to Configuring User Roles on page 392.

For more information on creating a Guest Pass Operator role, refer to Creating a Guest Pass Operator on page 207.

Generating and Delivering a Single Guest Pass

The following instructions apply to users with guest pass generation privileges.

A single guest pass can be used for one-time login, time-limited multiple logins for a single guest user, or configured so that a single guest pass can be shared by multiple users.

> **NOTE**
> For instructions on how to generate multiple guest passes, refer to Generating and Printing Multiple Guest Passes at Once on page 232.

> **NOTE**
> If printing the guest pass, make sure that your computer is connected to a local or network printer before starting.

Complete the following steps to generate a single guest pass.

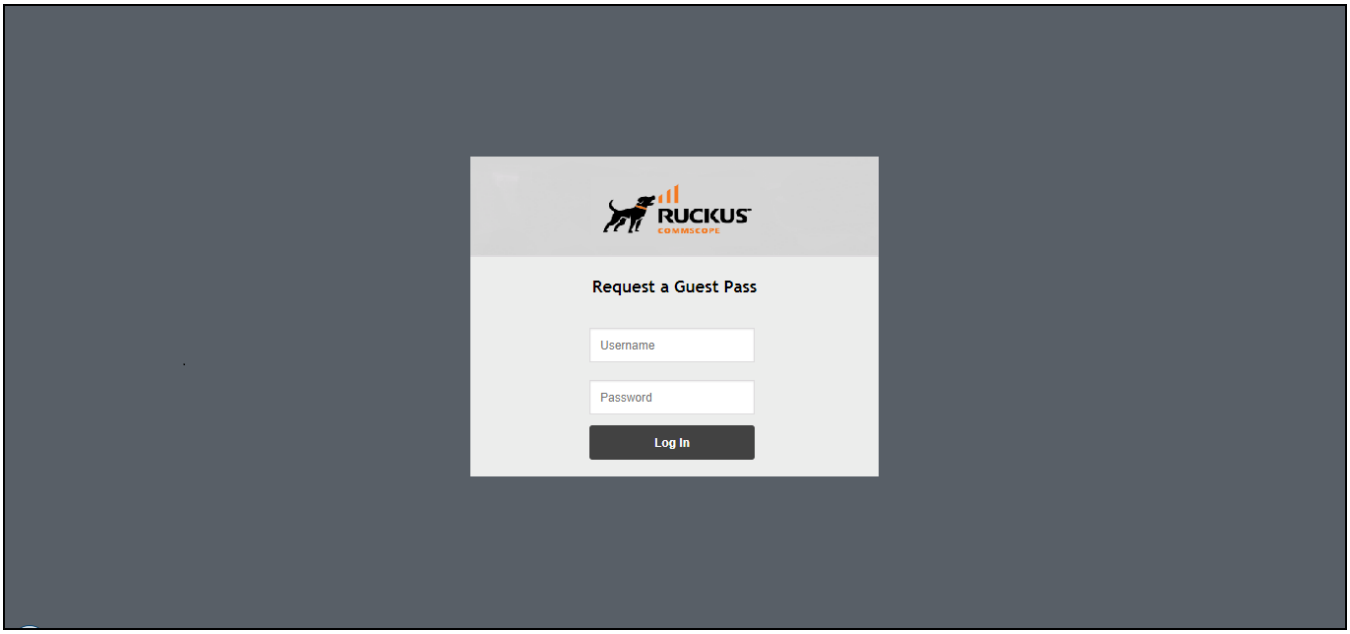
1. Enter the URL of the **Guest Pass Generation** page in your web browser.

   ```
   https://{unleashed-hostname-or-ipaddress}/guestpass
   ```

2. Enter your username and password and click **Log in**.

   NOTE
   The user generating the guest pass must have guest pass generation privileges, as described in Controlling Guest Pass Generation Privileges on page 227.

FIGURE 123 Requesting a Guest Pass



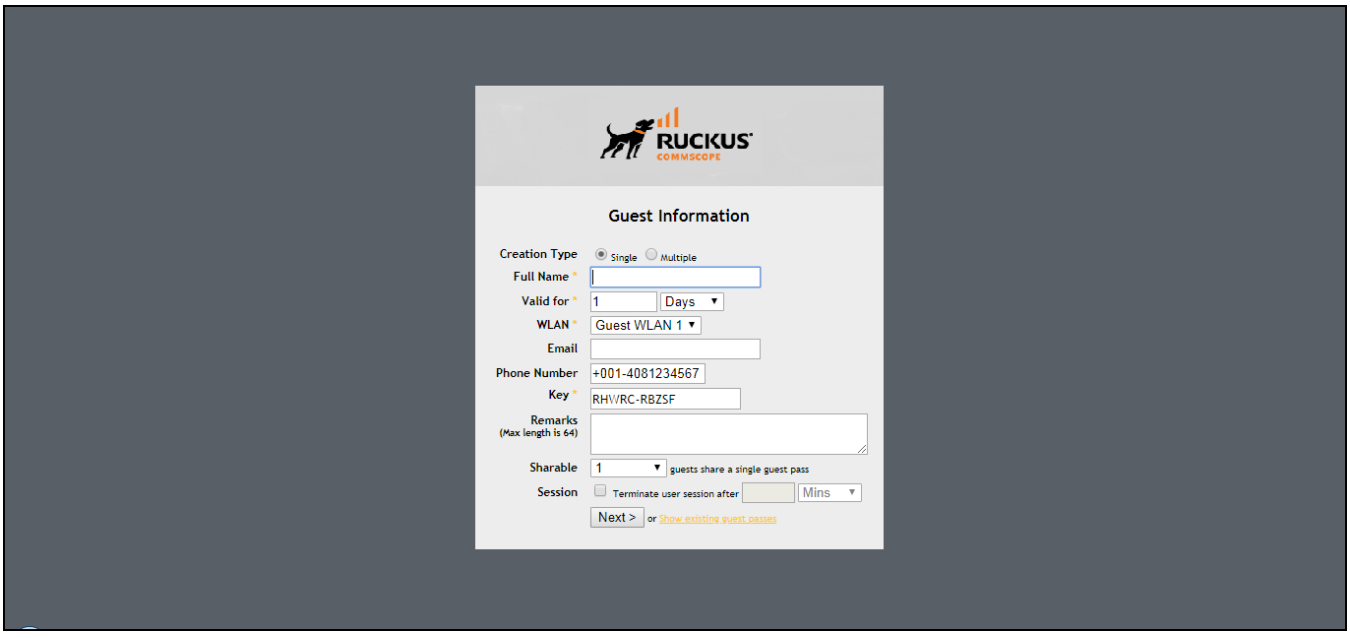
The **Guest Information** page appears. On this page, you need to provide information about the guest user to enable RUCKUS Unleashed to generate the guest pass.

3. On the **Guest Information** page, fill in the following options:
   - **Creation Type**: Click **Single** to generate a single guest pass. To generate multiple guest passes in batch, refer to Generating and Printing Multiple Guest Passes at Once on page 232.
   - **Full Name**: Enter the name of the guest user for whom you are generating the guest pass.
   - **Valid for**: Enter a number in the **Valid for** field and select a time unit (**Hours**, **Days**, or **Weeks**) to specify the time period when the guest pass will be valid.
   - **WLAN**: Select the WLAN for this guest (typically, a guest WLAN).
   - **Email**: (Optional) Enter the email address for this user.
   - **Phone Number**: (Optional) Enter a phone number for this user.
   - **Key**: Leave as is if you want to use the random key that RUCKUS Unleashed generates. If you want to use a key that is easy to remember, delete the random key, and enter a custom key. For example, if RUCKUS Unleashed generated the random key OVEGS-RZKKF, you can change it to "joe-guest-key". Customized keys must be from 1 through 16 ASCII characters in length.

     NOTE
     Each guest pass key must be unique and is distributed on all guest WLANs. Therefore, you cannot create the same guest pass for use on multiple WLANs.

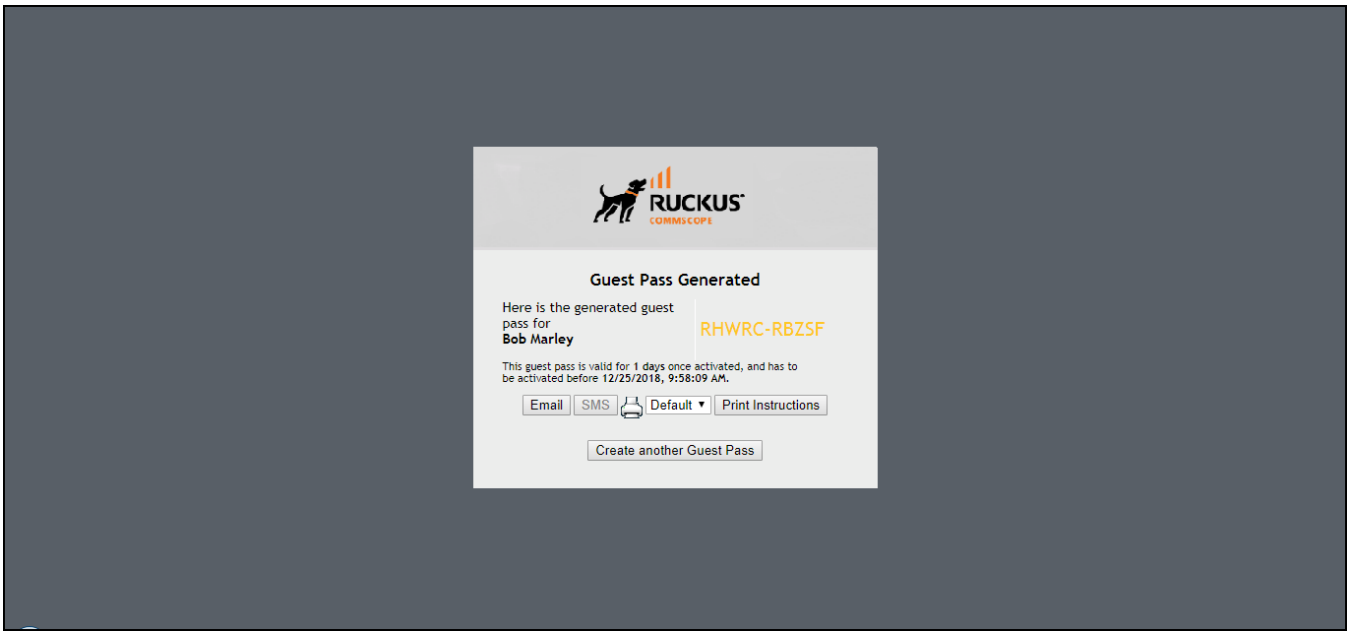
   - **Remarks**: (Optional) Enter any notes or comments. For example, if the guest user is a visitor from a partner organization, you can enter the name of the organization.
   - **Sharable**: Use this option to allow multiple users to share a single guest pass.
   - **Session**: Select the check box and enter an increment of time after which guests must log in again. If the **Session** check box is not selected, connected users will not be required to log in again until the guest pass expires.

FIGURE 124 Creating a Single Guest Pass



4. Click **Next**. The **Guest Pass Generated** page appears and presents the guest pass key and options for delivering this key to your guests. Delivery options include **Email** (if you entered an email address for the guest), **SMS** (if you configured a phone number for the guest), and **Print Instructions**.

   FIGURE 125 Guest Pass Generated Page



5. If you want to print the guest access instructions, select the guest pass instructions that you want to print from the menu. If you did not create custom guest pass printouts, select **Default**.
6. Click **Print Instructions**. A new page displays the Guest Pass instructions and the **Print** dialog box is displayed.
7. Select the printer that you want to use, and click **Print** to print the guest pass instructions.

You have completed generating and delivering a guest pass for your guest user.

FIGURE 126 Sending Guest Pass Key through Email Entered on the Guest Information Screen

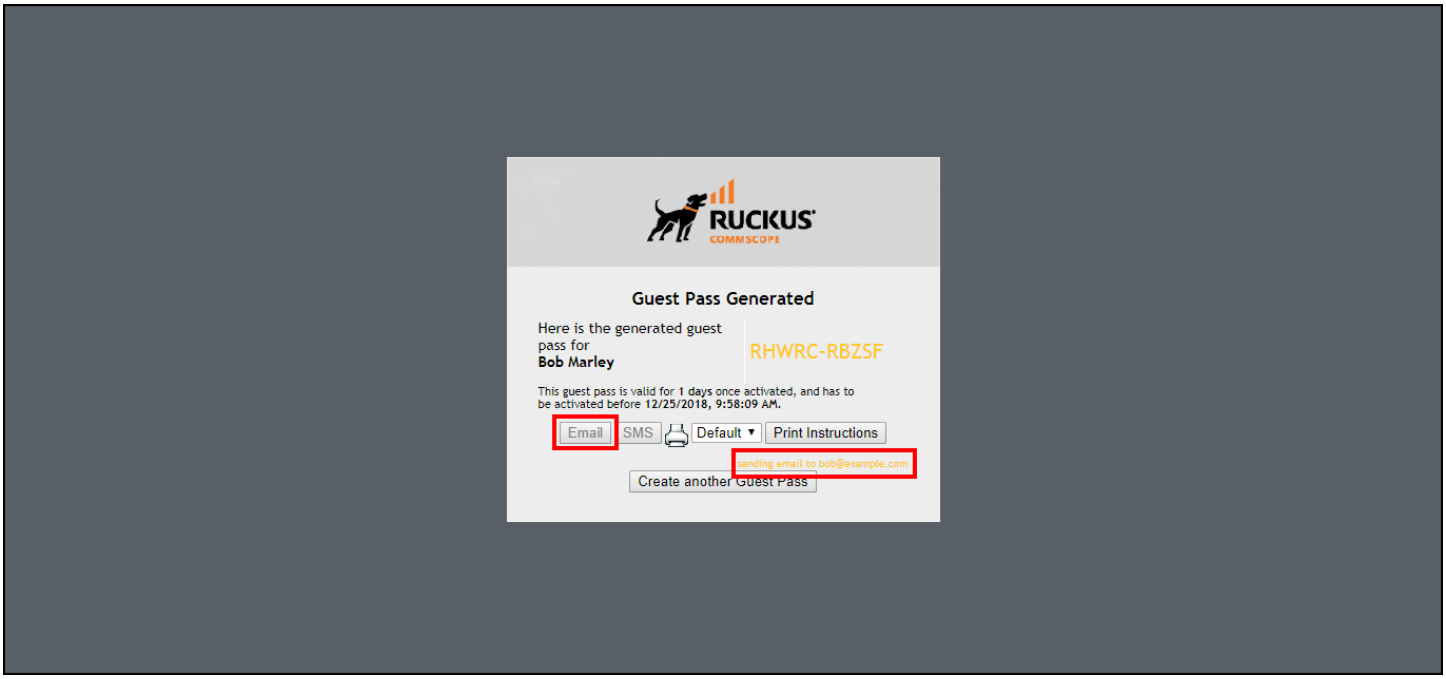
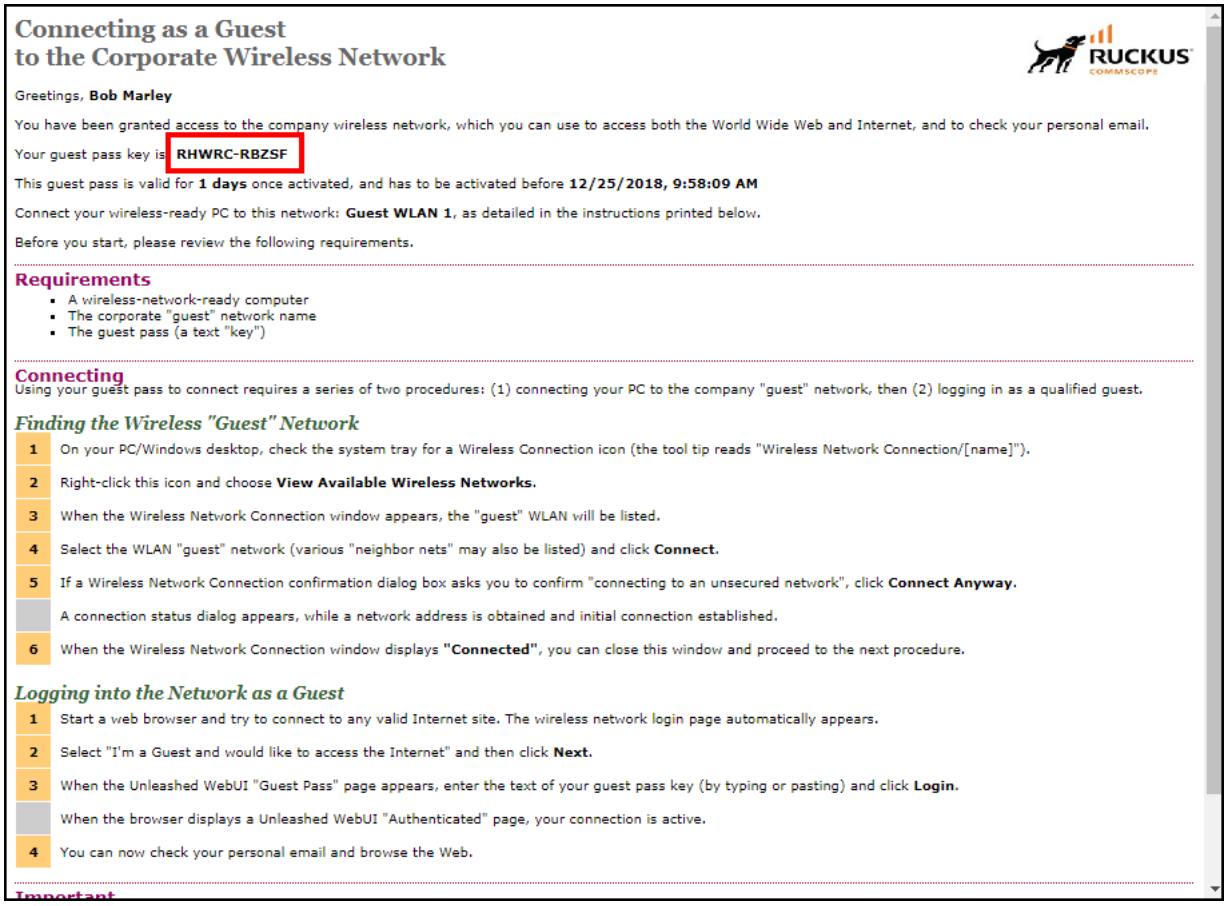


FIGURE 127 Sample Guest Pass Printout



If you want to create additional guest passes one by one, click **Create Another Guest Pass**. Alternatively, you can generate multiple guest passes in batch, as described in Generating and Printing Multiple Guest Passes at Once on page 232.

Generating and Printing Multiple Guest Passes at Once

The following instructions apply to users with guest pass generation privileges.

> **NOTE**
> For instructions on how to generate a single guest pass, refer to Generating and Delivering a Single Guest Pass on page 227.

> **NOTE**
> If printing the guest pass, make sure that your computer is connected to a local or network printer before starting.

Complete the following steps to generate and print multiple guest passes at the same time:

1. Enter the URL of the Guest Pass Generation page in your web browser.

   ```
   https://{unleashed-hostname-or-ipaddress}/guestpass
   ```

2. Enter your username and password, and click **Log In**.

   The **Guest Information** page appears. On this page, you need to provide information about the guest users to enable RUCKUS Unleashed to generate the guest passes.

3. On the **Guest Information** page, fill in the following options:
   - **Creation Type**: Click **Multiple**.
   - **Valid for**: Enter a number in the **Valid for** field and select a time unit (**Hours**, **Days**, or **Weeks**) to specify the time period that the Guest Passes will be valid.
   - **WLAN**: Select one of the existing WLANs with which the guest users will be allowed to associate.
   - **Number**: Select the number of guest passes that you want to generate. RUCKUS Unleashed automatically populates the names of each user (Batch-Guest-1, Batch-Guest-2, and so on) to generate the guest passes.

     NOTE
     Each guest pass key must be unique and is distributed on all guest WLANs. Therefore, you cannot create the same guest pass for use on multiple WLANs.

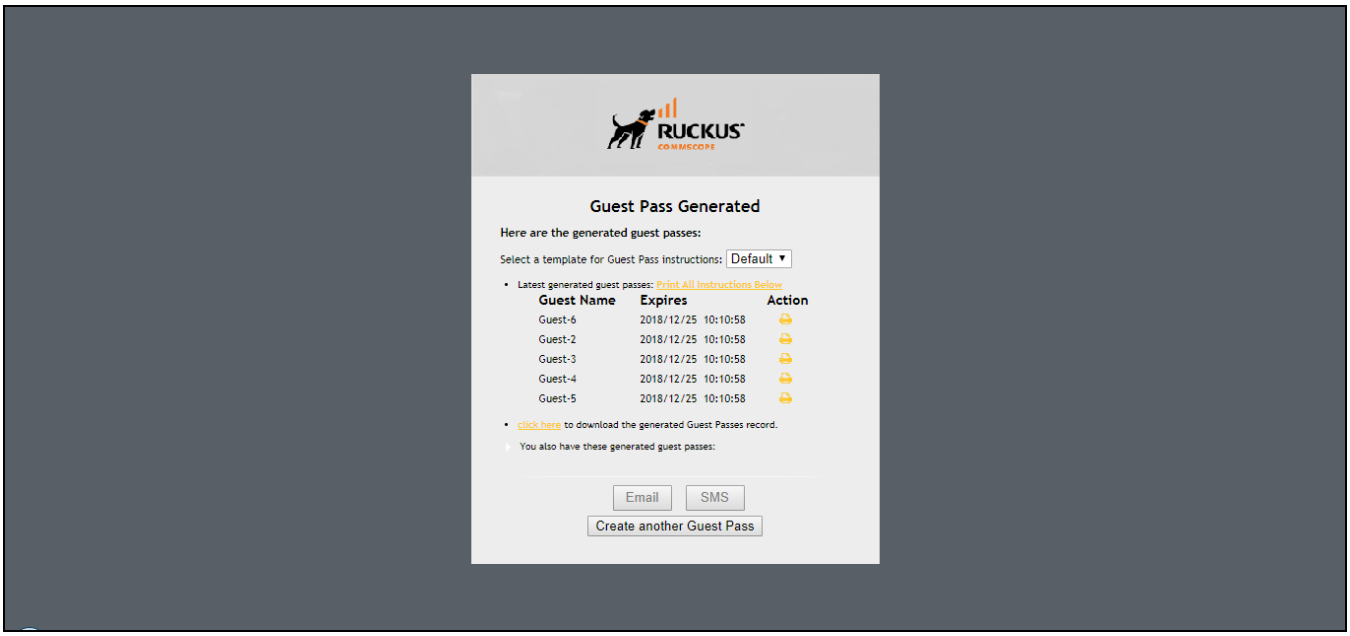
   - **Profile (*.csv)**: If you have created a Guest Pass profile (refer to Creating a Guest Pass Profile), click **Choose File** to import the file.
   - **Sharable**: Configure this option if you want to allow multiple users to share a single guest pass (default: 1; not shared).
   - **Session**: Select the check box and enter an increment of time after which guests must log in again. If the **Session** check box in not selected, connected users will not be required to log in again until the Guest Pass expires.

FIGURE 128 Generating Multiple Guest Passes

NOTE
If you want to be able to identify the guest pass users by their names (for example, for monitoring or auditing purposes in a hotel setting), click **Choose File**, and upload a guest pass profile instead. Refer to Creating a Guest Pass Profile on page 234 for more information.

4. Click **Next**. The **Guest Pass Generated** page appears and displays the guest pass user names and expiration dates.

   FIGURE 129 Multiple Guest Passes Generated



5. For **Select a template for Guest Pass instructions**, select the guest pass instructions that you want to print from the menu. If you did not create custom guest pass printouts, select **Default**.
6. Print the instructions for a single guest pass or print all of them:
   - To print instructions for all guest passes, click **Print All Instructions** below.
   - To print instructions for a single guest pass, click the printer icon in the **Action** column in the same row as the guest pass for which you want to print instructions.

   A new browser page appears and displays the guest pass instructions and the **Print** dialog box is displayed.
7. Select the printer that you want to use and click **Print** to print the guest pass instructions.

You have completed generating and printing multiple guest passes for your guest users. If you want to save a record of the guest passes that you have generated, click the **Click here** link in **Click here to download the generated Guest Passes record**. Download and save the CSV file to your computer.

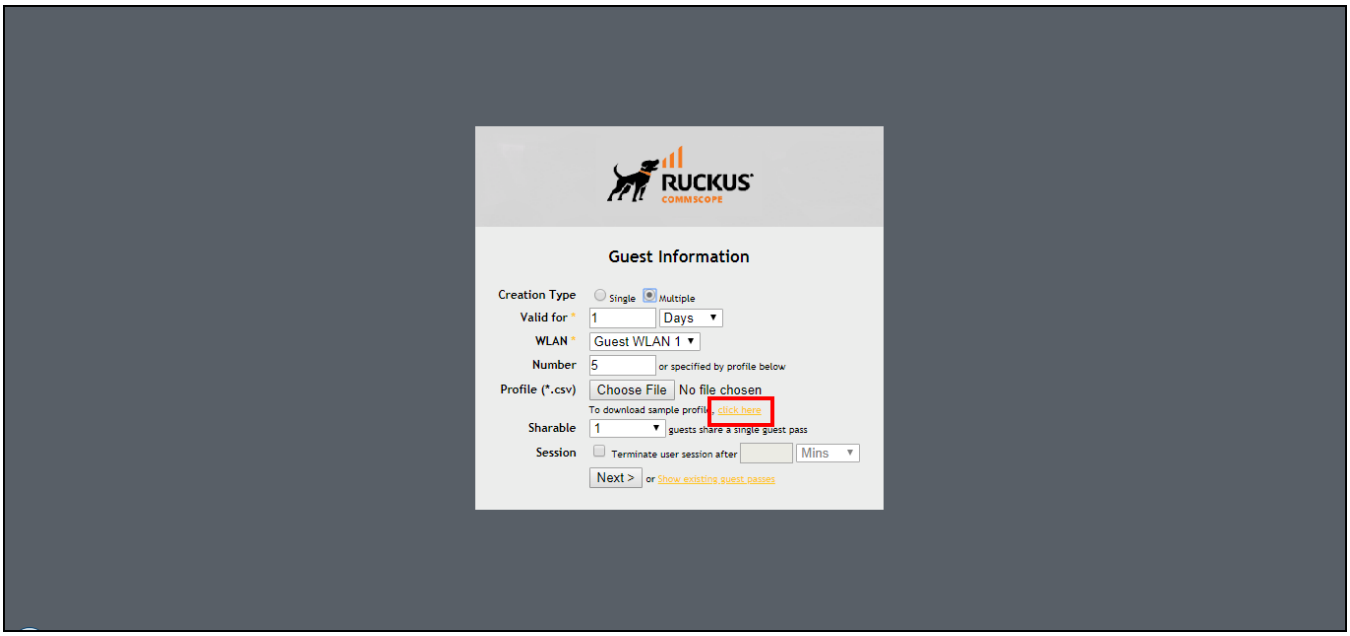
Creating a Guest Pass Profile

Complete the following steps to create a Guest Pass profile.

1. Log in to the guest pass generation page.
2. For **Creation Type**, click **Multiple**.

3. For **Profile (*.csv)**, click the **click here** link in **To download a profile sample, click here**.

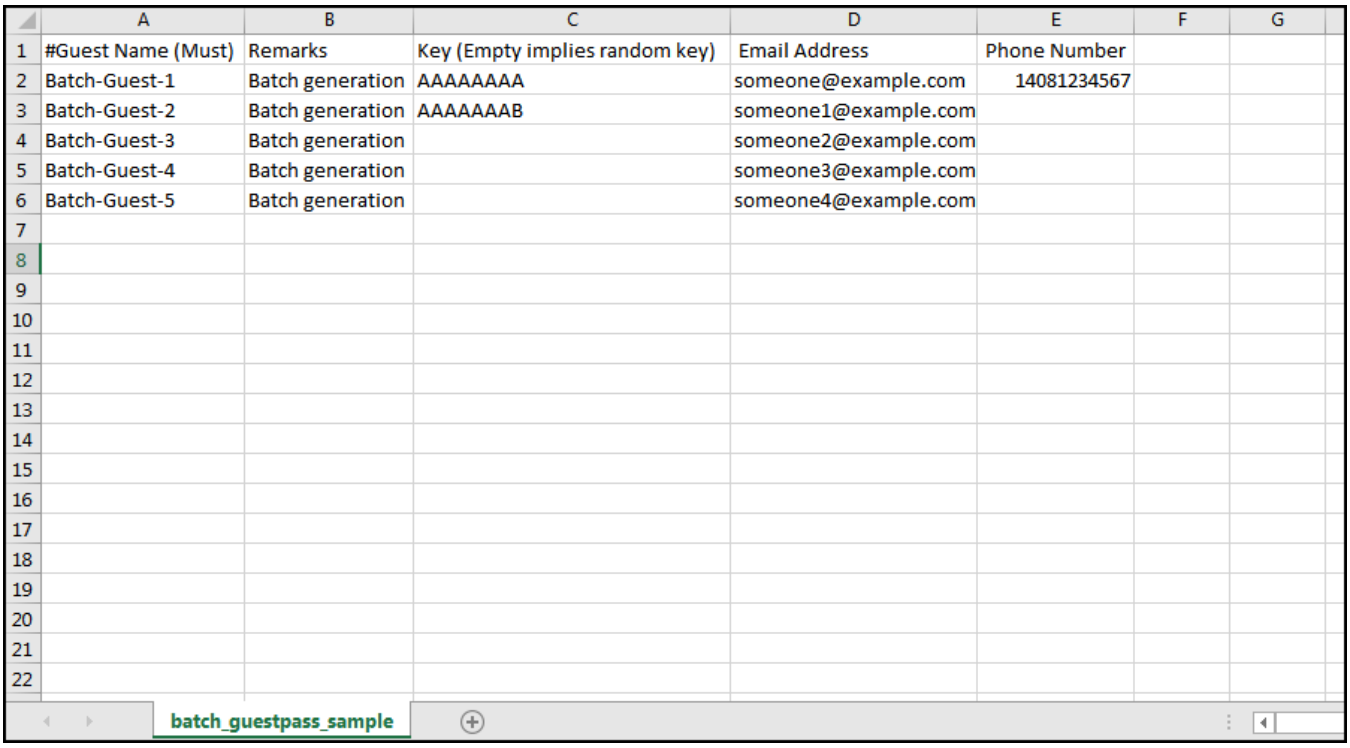
FIGURE 130 Downloading a Sample Profile



4. Save the sample guest pass profile (in CSV format) to your computer.

5. Using a spreadsheet application, open the CSV file and edit the guest pass profile by filling out the following columns:
   - **#Guest Name**: Enter the name of the guest user (one name per row).
   - **Remarks**: (Optional) Enter any note or remarks about the guest pass.
   - **Key**: Enter a guest pass key consisting from 1 through 16 alphanumeric characters. If you want RUCKUS Unleashed to generate the guest pass key automatically, leave this column blank.

FIGURE 131 Editing the CSV File in a Spreadsheet Application

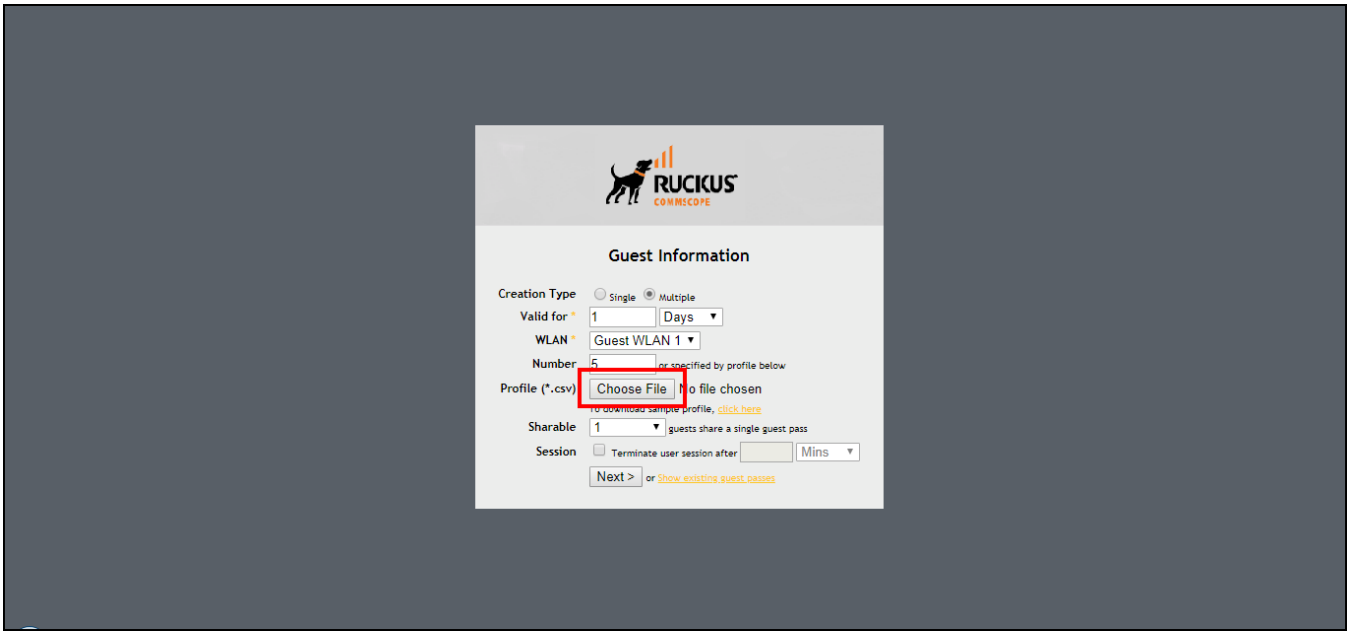


	A	B	C	D	E	F	G
1	#Guest Name (Must)	Remarks	Key (Empty implies random key)	Email Address	Phone Number		
2	Batch-Guest-1	Batch generation	AAAAAAAA	someone@example.com	14081234567		
3	Batch-Guest-2	Batch generation	AAAAAAAB	someone1@example.com			
4	Batch-Guest-3	Batch generation		someone2@example.com			
5	Batch-Guest-4	Batch generation		someone3@example.com			
6	Batch-Guest-5	Batch generation		someone4@example.com			
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							

batch_guestpass_sample

6. Return to the **Guest Information** page, and complete step 3 through step 7 in Generating and Printing Multiple Guest Passes at Once on page 232 to upload the guest pass profile and generate multiple guest passes.

FIGURE 132 Importing Batch Generation CSV File

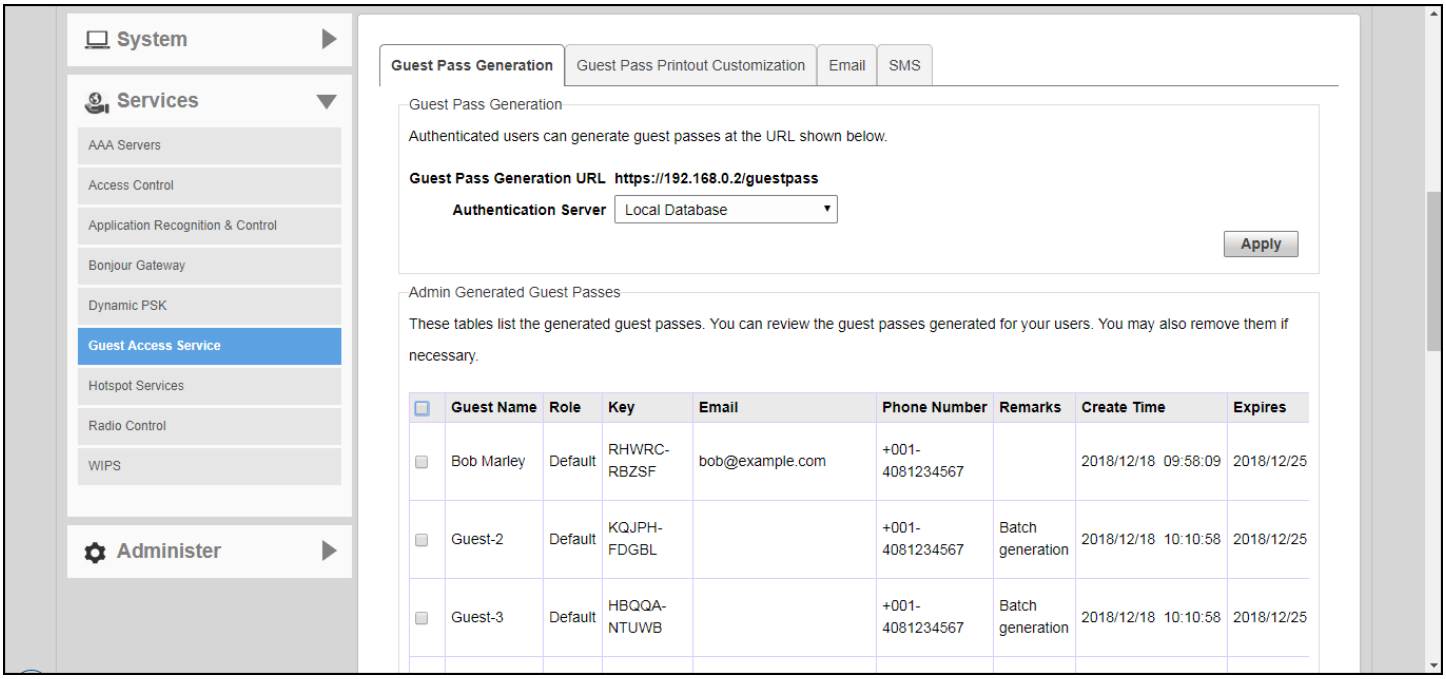


Monitoring Generated Guest Passes

Once you have generated guest passes for your visitors, you can monitor and, if necessary, delete them to revoke the guests' access privileges.

1. Go to **Admin & Services > Services > Guest Access Service > Guest Pass Generation**.
2. Review the generated guest passes in the **Admin Generated Guest Passes** and **Self-Service Generated Guest Passes** tables.
3. To remove a guest pass, select the check box for the guest pass, and click the **Delete** button. Click **Delete All** to delete all generated guest passes at once.

FIGURE 133 Viewing generated Guest Passes



Creating a Custom Guest Pass Printout

The guest pass printout is a printable HTML page that contains instructions for the guest pass user on how to connect to the wireless network.

The authenticated user who is generating the guest pass will need to print out this HTML page and provide it to the guest pass user. A guest pass in English and one in French are included by default.

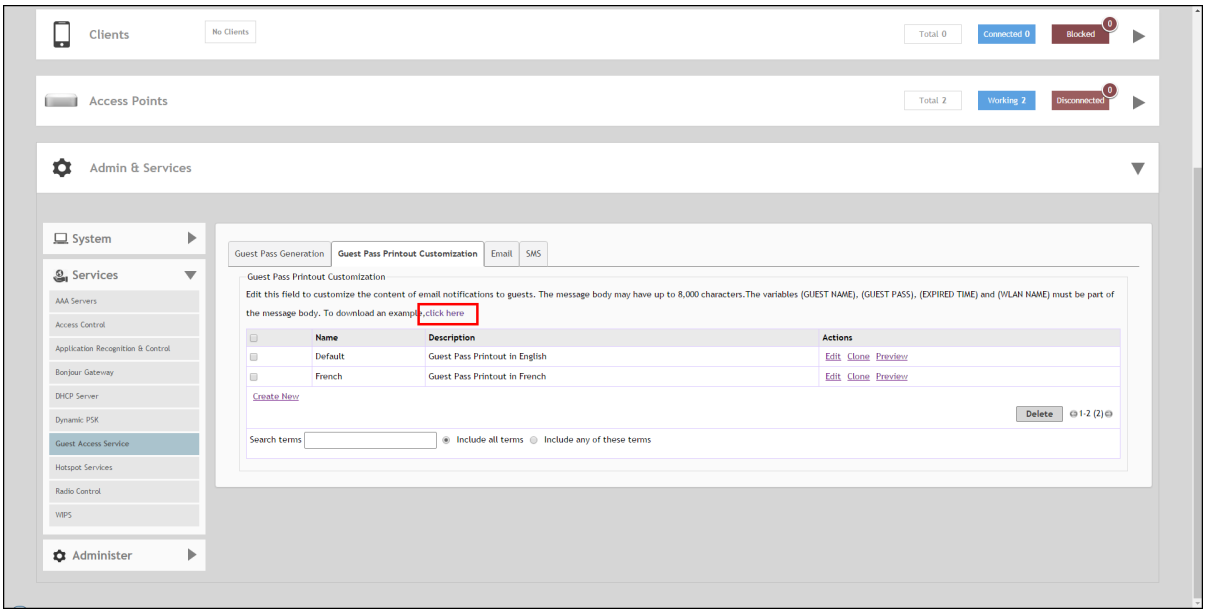
As administrator, you can create custom guest pass printouts. For example, if your organization receives visitors who speak different languages, you can create guest pass printouts in other languages.

To create a custom guest pass printout:

1. Go to **Admin & Services > Services > Guest Access Service > Guest Pass Printout Customization**.

2. Click the **click here** link to download an example of an existing printout.

FIGURE 134 Guest Pass Printout Customization

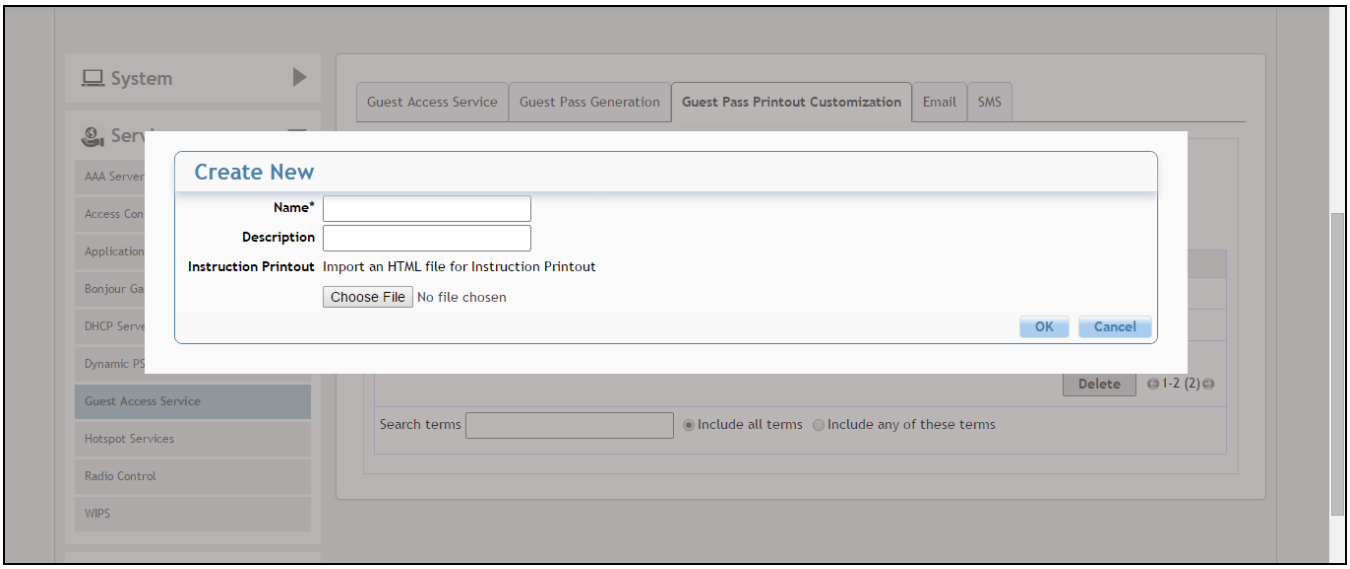


3. Save the HTML file to your computer.
4. Using a text or HTML editor, customize the guest pass printout. Note that only ASCII characters can be used. You can do any or all of the following:
   - Reword the instructions
   - Translate the instructions to another language
   - Customize the HTML formatting

NOTE
The guest pass printout contains several tokens or variables that are substituted with actual data when the guest pass is generated. When you customize the guest pass printout, make sure that these tokens are not deleted. For more information on these tokens, see Guest Pass Printout Tokens on page 240.

5. Go back to the **Guest Pass Printout Customization** screen, and then click **Create New**. The **Create New** form appears.

FIGURE 135 Creating New Guest Pass Printout File



6. In **Name**, type a name for the guest pass printout that you are creating. For example, if this guest pass printout is in Spanish, you can type **Spanish**.
7. In **Description** (optional), add a brief description of the guest pass printout.
8. Click **Choose File**, select the HTML file that you customized earlier, and then click **Open**. Unleashed copies the HTML file to its database.
9. Click **Import** to save the HTML file to the Unleashed AP.

You have completed creating a custom guest pass printout. When users generate a guest pass, the custom printout that you created will appear as one of the options that they can print.

Guest Pass Printout Tokens

The following table lists the tokens that are used in the guest pass printout. Make sure that they are not accidentally deleted when you customize the guest pass printout.

TABLE 30 Tokens that you can use in the guest pass printout

Token	Description
{GP_GUEST_NAME}	Guest pass user name.
{GP_GUEST_KEY}	Guest pass key.
{GP_IF_EFFECTIVE_FROM_CREATION_TIME}	If you set the validity period of guest passes to Effective from the creation time (in the Guest Pass Generation section), this token shows when the guest pass was created and when it will expire.
{GP_ELSEIF_EFFECTIVE_FROM_FIRST_USE}	If you set the validity period of guest passes to Effective from first use (in the Guest Pass Generation section), this token shows the number of days during which the guest pass will be valid after activation. It also shows the date and time when the guest pass will expire if not activated.
{GP_ENDIF_EFFECTIVE}	This token is used in conjunction with either the {GP_ELSEIF_EFFECTIVE_FROM_FIRST_USE} or {GP_ENDIF_EFFECTIVE} token.
{GP_VALID_DAYS}	Number of days for which the guest pass is valid.
{GP_VALID_TIME}	Date and time when the guest pass expires.

TABLE 30 Tokens that you can use in the guest pass printout (continued)

Token	Description
{GP_GUEST_WLAN}	Name of WLAN that the guest user can access.

Customizing the Guest Pass Email Content

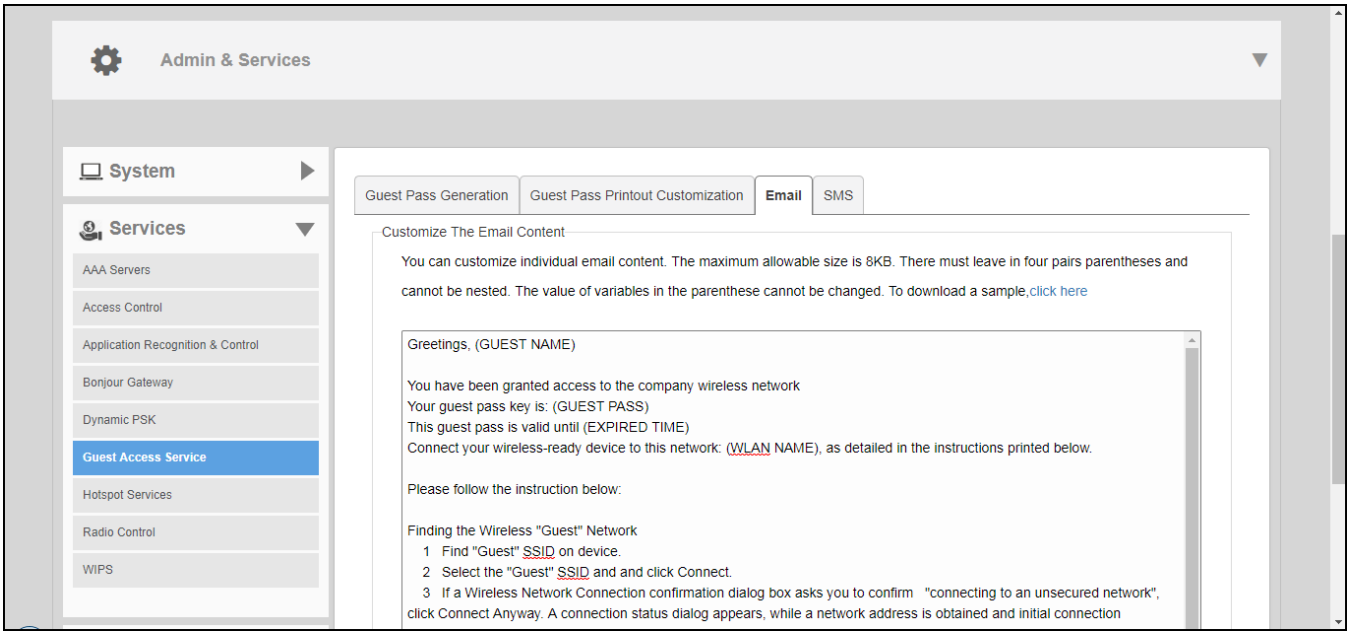
The Unleashed guest pass email content can be customized to suit your preferences.

> **NOTE**
> To allow Unleashed to deliver guest passes via email, you must first configure an email account (and its SMTP settings) from which Unleashed will send the emails. For information on configuring the email server, see Configuring Email Server Settings on page 204.

Use the following procedure to customize the content of the email in which the guest pass keys will be delivered:

1. Go to **Admin & Services > Services > Guest Access Service > Email**.
2. Replace the content in the text box, while ensuring that the following variables remain intact and unchanged:
   - (GUEST NAME)
   - (GUEST PASS)
   - (EXPIRED TIME)
   - (WLAN NAME)
3. To download a sample of the email, click the **click here** link.
4. Click **Apply** to save your changes.

FIGURE 136 Customize guest pass email content



Customizing the Guest Pass SMS Content

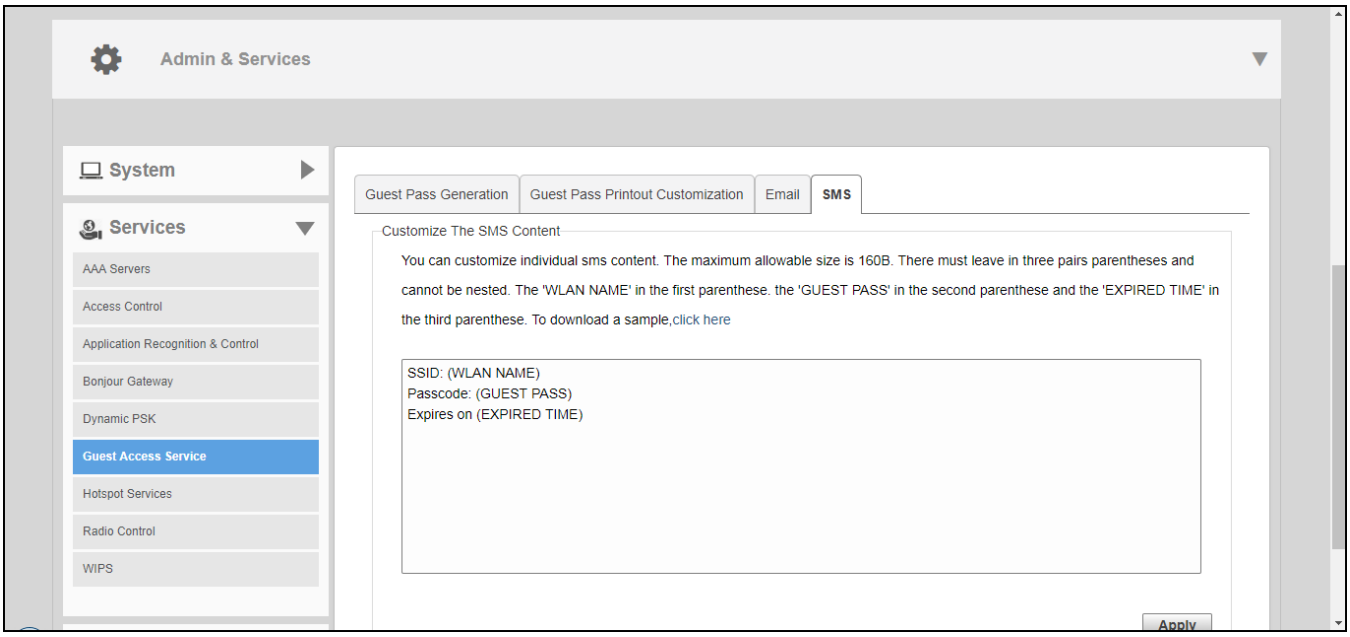
The Unleashed guest pass SMS content can be customized to suit your preferences.

NOTE
To allow Unleashed to deliver guest passes via SMS, you must first configure an SMS delivery account from which Unleashed will send the SMS messages. For information on configuring the SMS server settings, see Configuring Email Server Settings on page 204.

Use the following procedure to customize the content of the SMS messages in which the guest pass keys will be delivered:

1. Go to **Admin & Services > Services > Guest Access Service > SMS**.
2. Replace the content in the text box, while ensuring that the following variables remain intact and unchanged:
   - (WLAN NAME)
   - (GUEST PASS)
   - (EXPIRED TIME)
3. To download a sample of the SMS message, click the **click here** link.
4. Click **Apply** to save your changes.

FIGURE 137 Customize guest pass SMS content



Social Media WLANs

Social Media WLANs allow guest users to access the Internet using a social media account instead of using a WPA password or Guest Pass to login.

The following social media login methods are currently supported:

- Facebook Wi-Fi on page 244
- Google/Google+ on page 244
- LinkedIn on page 254
- Microsoft Live on page 258

- WeChat on page 262

For each of these social media WLAN options, you must create an application or activate a service on the respective social media website first, before your users will be able to log in using their social media accounts.

NOTE
Beginning with release 200.6, multiple social media login types can be enabled for the same WLAN.

FIGURE 138 Creating a Social Media WLAN

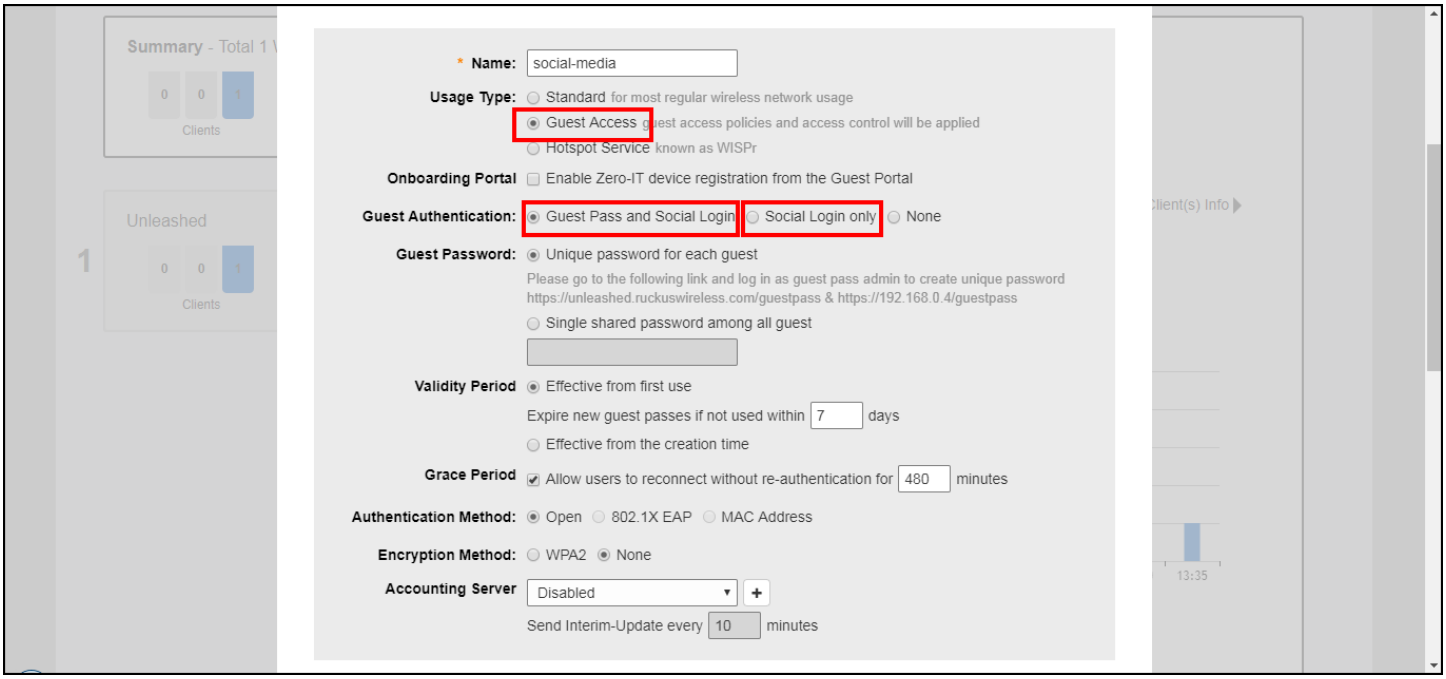
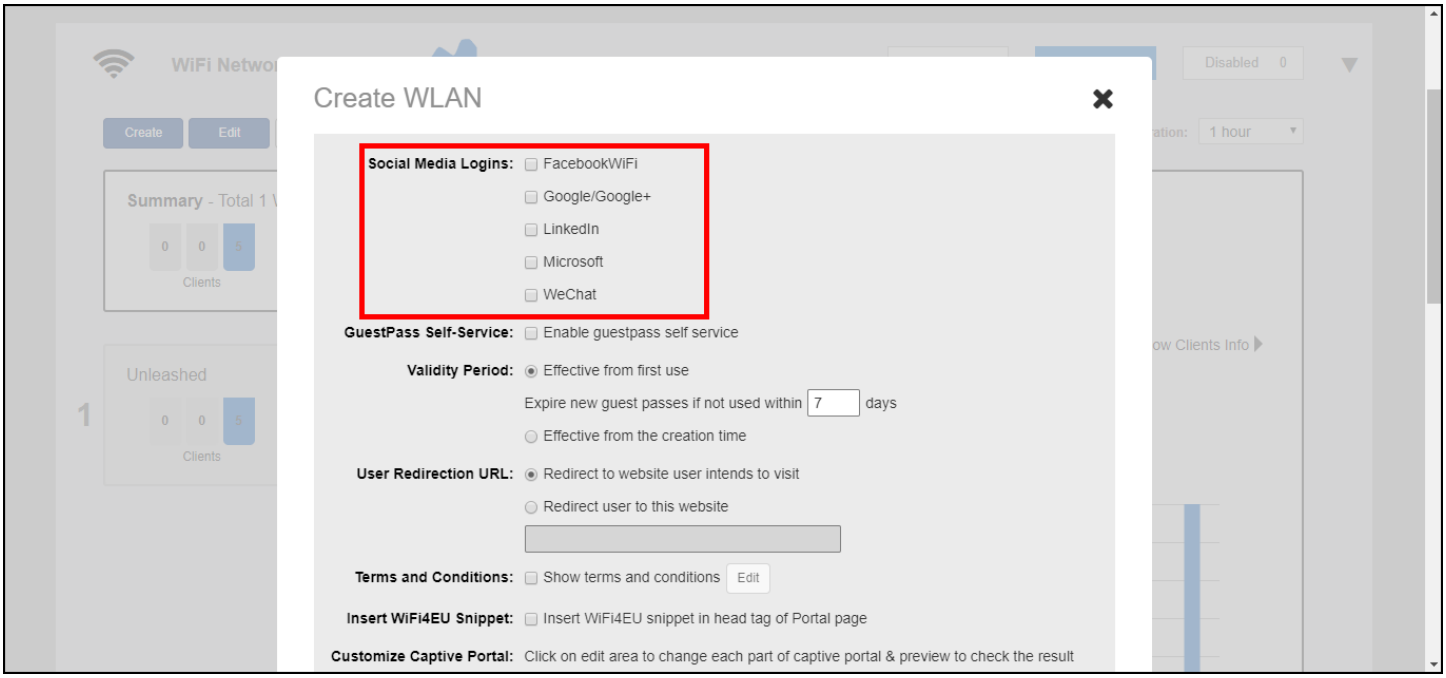


FIGURE 139 Select social media logins



Facebook Wi-Fi

Business owners can use this WLAN type to require users to visit the business owner's Facebook page and "check in" using a Facebook account before being allowed free access to the Internet.

The business owner can also display advertisements and other announcements on this Facebook page, and can control the guest session length and other options using the Facebook Wi-Fi configuration panel. For more information, see the Facebook Wi-Fi Help Center.

The following caveats and limitations should be considered before deploying a Facebook Wi-Fi (or other social media) WLAN:

- You can create a maximum of four Facebook Wi-Fi WLANs.
- Users must launch a browser to trigger the Facebook authentication.
- Invalid users are determined by Facebook. Unleashed queries facebook.com once every five minutes to verify the authentication status of all currently connected users. If an invalid response is received, the end user will be deleted within five minutes. If Unleashed fails to receive a response, it will re-send the request four times. If there is no response after five requests, Unleashed will delete the related stations.

Google/Google+

The Google/Google+ social media login complies with the OAuth 2.0 specification. To create a Google/Google+ social media WLAN, you need an OAuth 2.0 client ID, which is used when requesting an OAuth 2.0 access token.

RUCKUS Unleashed provides a default internal Google client ID. After selecting **Google/Google+**, clear the **Use my own client ID** check box if you do not have or do not want to create your own client ID.

If you do want to use your own client ID and password, enable **Use my own client ID**, and enter your **Google client ID** and **Password** in the fields that appear.

Select **Enable HTTPS** or **Enable HTTP**.

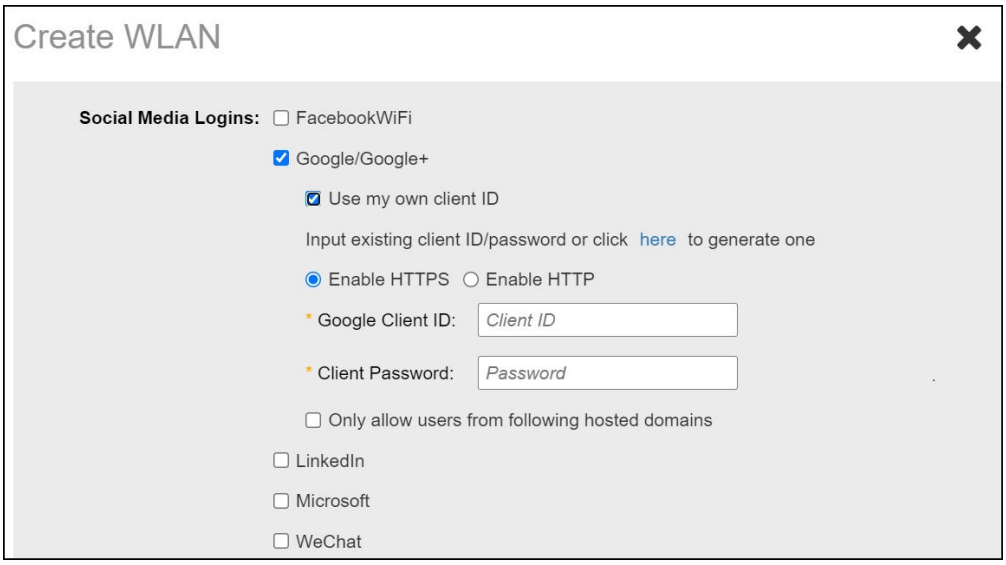
To limit Google/Google+ login to a specific domain or several domains, enable the **Only allow users from the following hosted domains** option and enter the domain names, separated by commas, in the text box.

For example, if a company that uses Gmail accounts wants to limit access to the WLAN to Google accounts that match the company's domain name, enable **Only allow users from the following hosted domains** and enter the company's Google domain (*company_name*.gmail.com). This prevents any other gmail.com accounts from being used to access this WLAN.

Refer to the Google documentation for instructions on configuring your Google/Google+ account to provide social media login details. For information on Google OAuth 2.0 setup instructions, refer to *https://support.google.com/cloud/answer/6158849*.

For more information on OAuth 2.0, refer to *https://en.wikipedia.org/wiki/OAuth*.

FIGURE 140 Logging in Using Google ID



OAuth Setup Procedure for Google+ Social Media Login

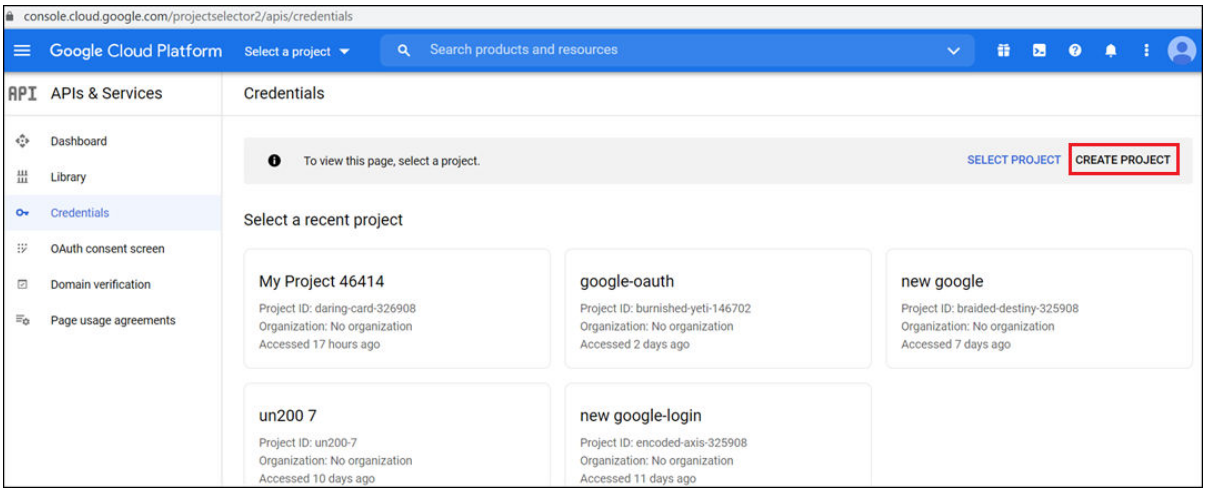
Google+ social media WLANs require a client ID and password, which can be automatically generated or manually entered. You can manually generate an OAuth 2.0 client ID for Google+ social media WLANs using the following procedure.

Complete the following steps to create a project ID in the Google Developers Console.

1. Create a project on the Google OAuth Console. Go to the following URL: https://console.developers.google.com/projectselector2/apis/credentials, and click **CREATE PROJECT**.

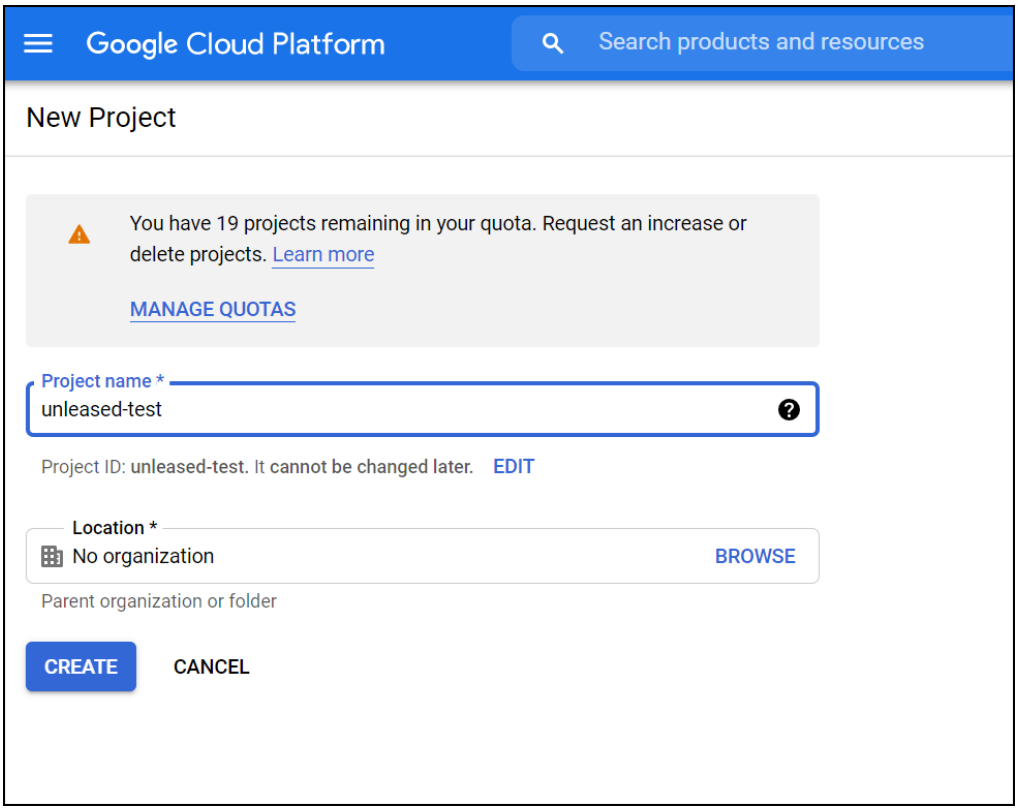
   NOTE
   Alternatively, click the **Click here** link to create a new application or project link from within the RUCKUS Unleashed guest access settings.

FIGURE 141 Creating a New Project on the Google OAuth Console



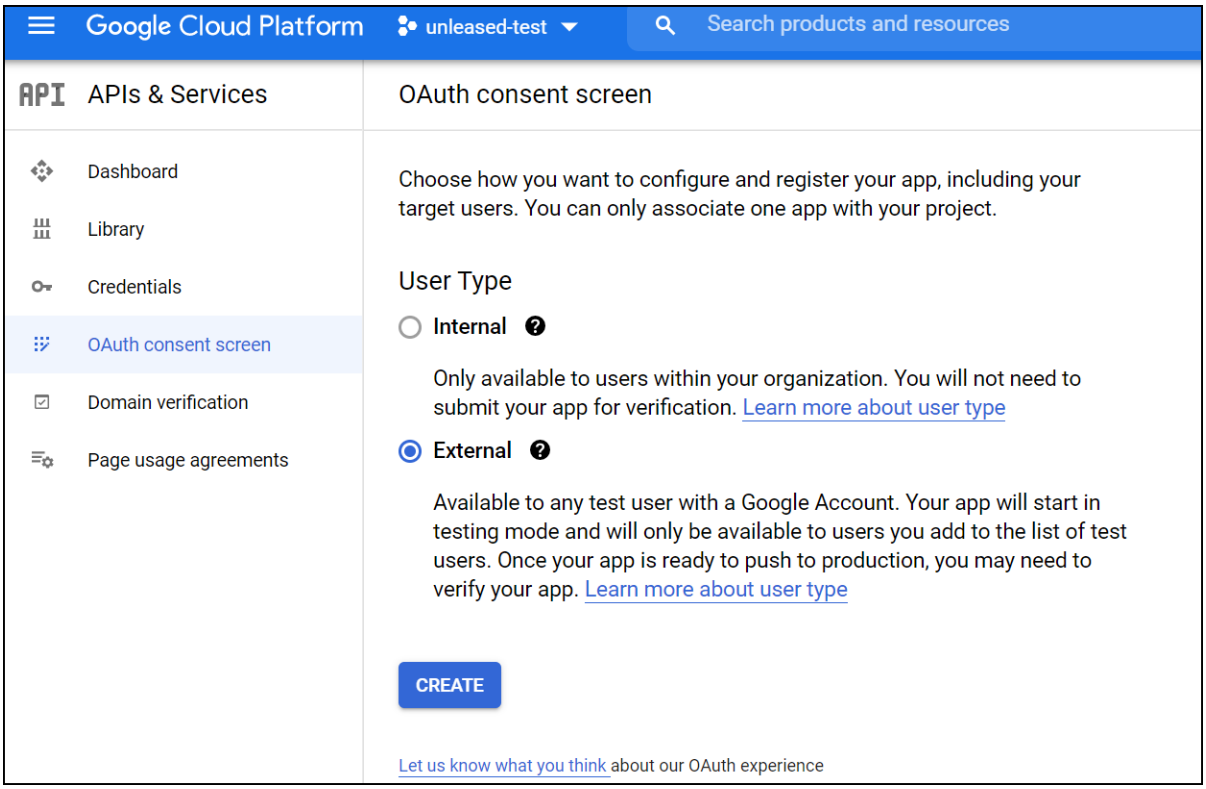
2. Enter **Project Name** and **Location**, and click **Create**.

FIGURE 142 Entering the Project Name



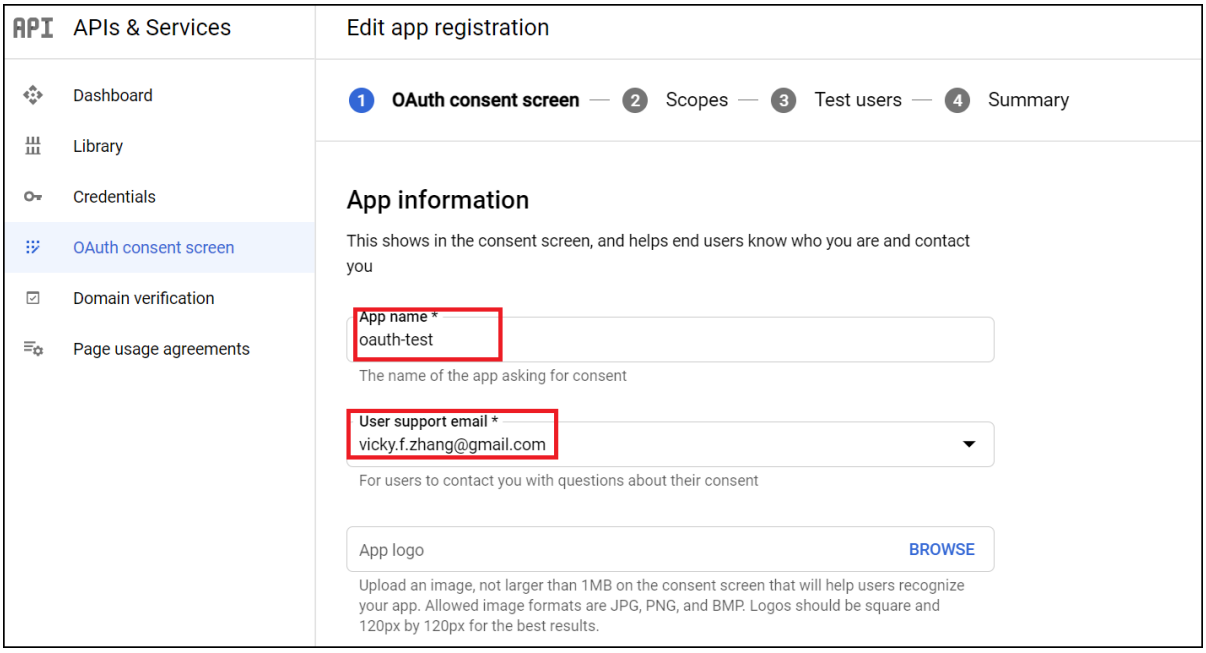
3. Once the project has been created, go to the **OAuth consent screen**, and select **External** and click **Create**.

FIGURE 143 Configuring OAuth Consent Screen



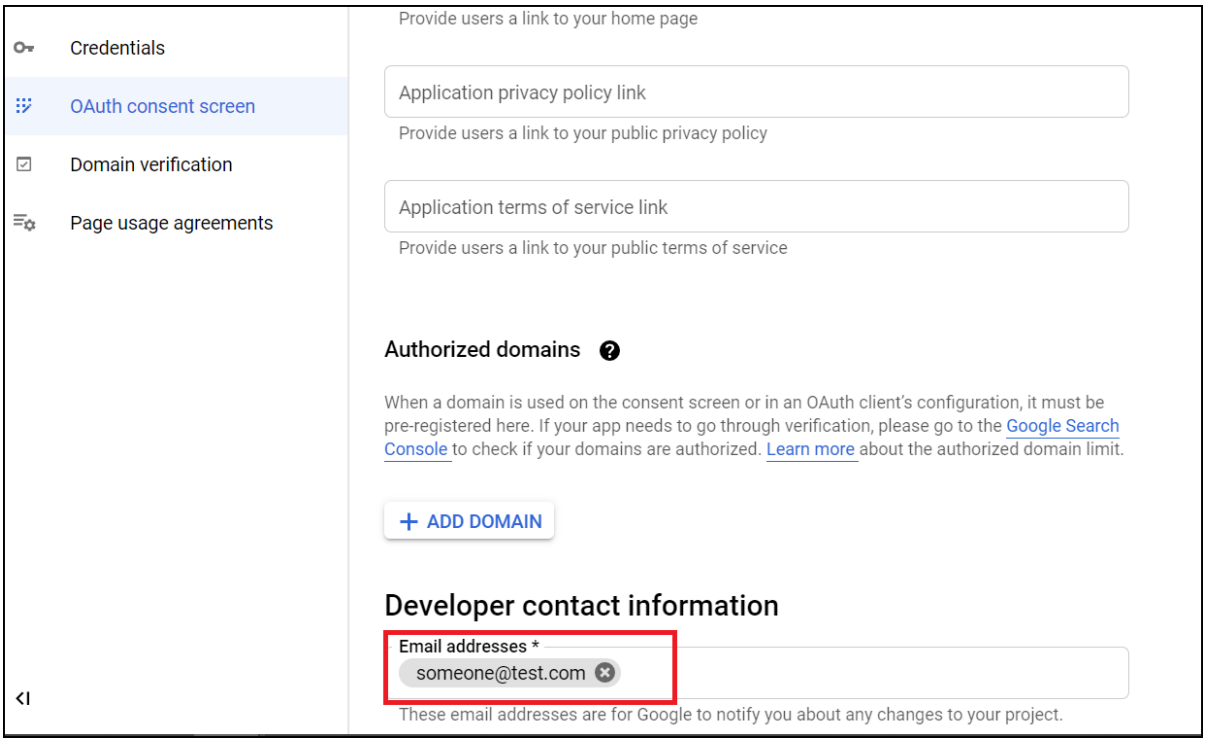
4. Under **App information**, complete the following steps:
   - For **App name**, enter the application name.
   - For **User support email**, select an email address from the list.

FIGURE 144 Entering App Information



5. For **Developer contact information**, enter valid email addresses and click **SAVE AND CONTINUE**.

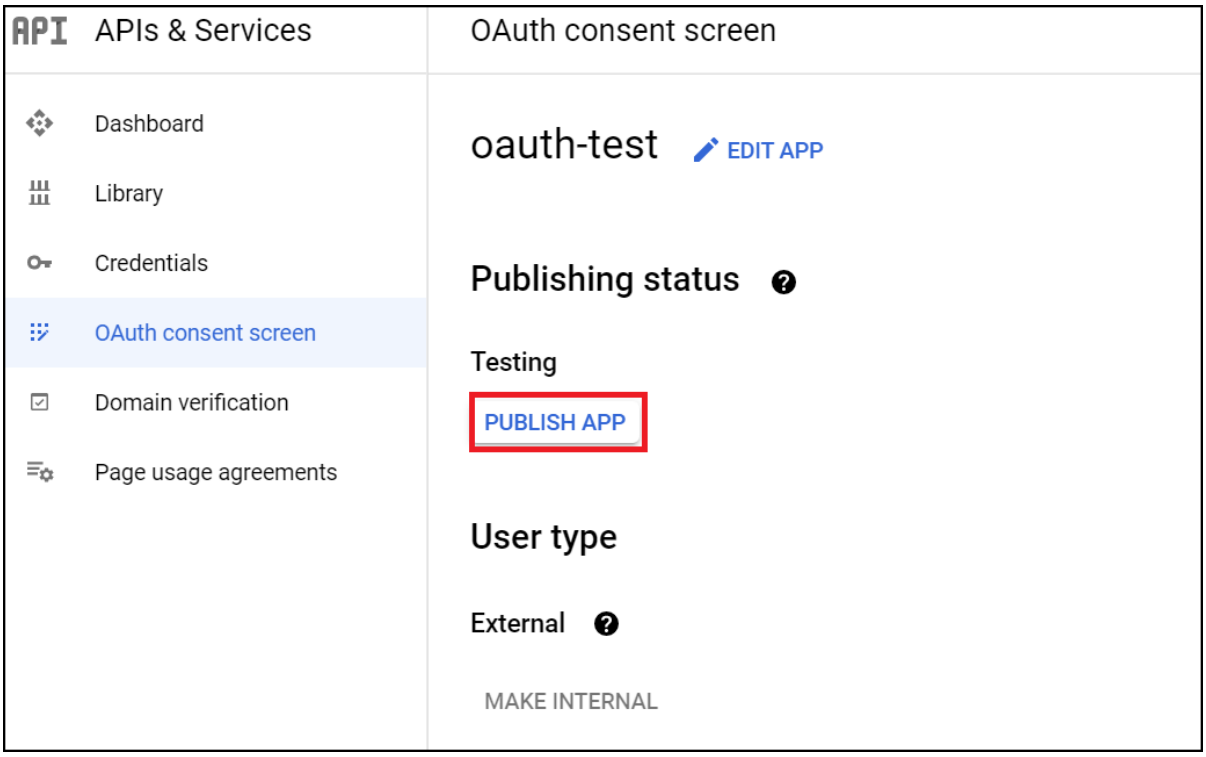
   FIGURE 145 Entering Developer Contact Information



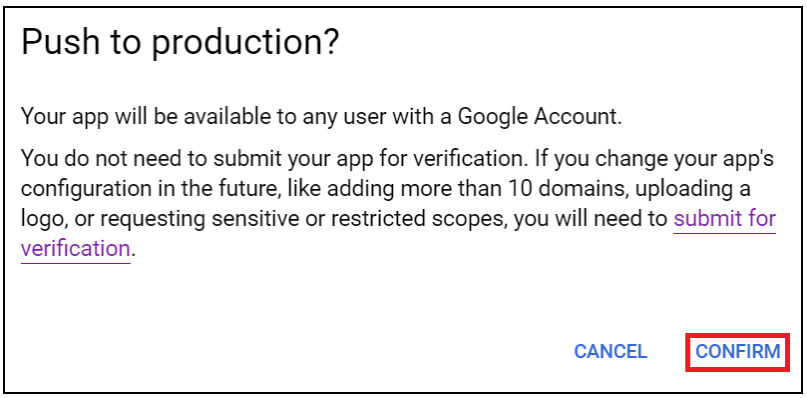
6. In the **Edit app registration** > **Scopes** page, click **SAVE AND CONTINUE**.
7. In the **Edit app registration** > **Test users** page, click **SAVE AND CONTINUE**.

8. On the **OAuth consent screen**, click **PUBLISH APP**.

FIGURE 146 Publishing the App

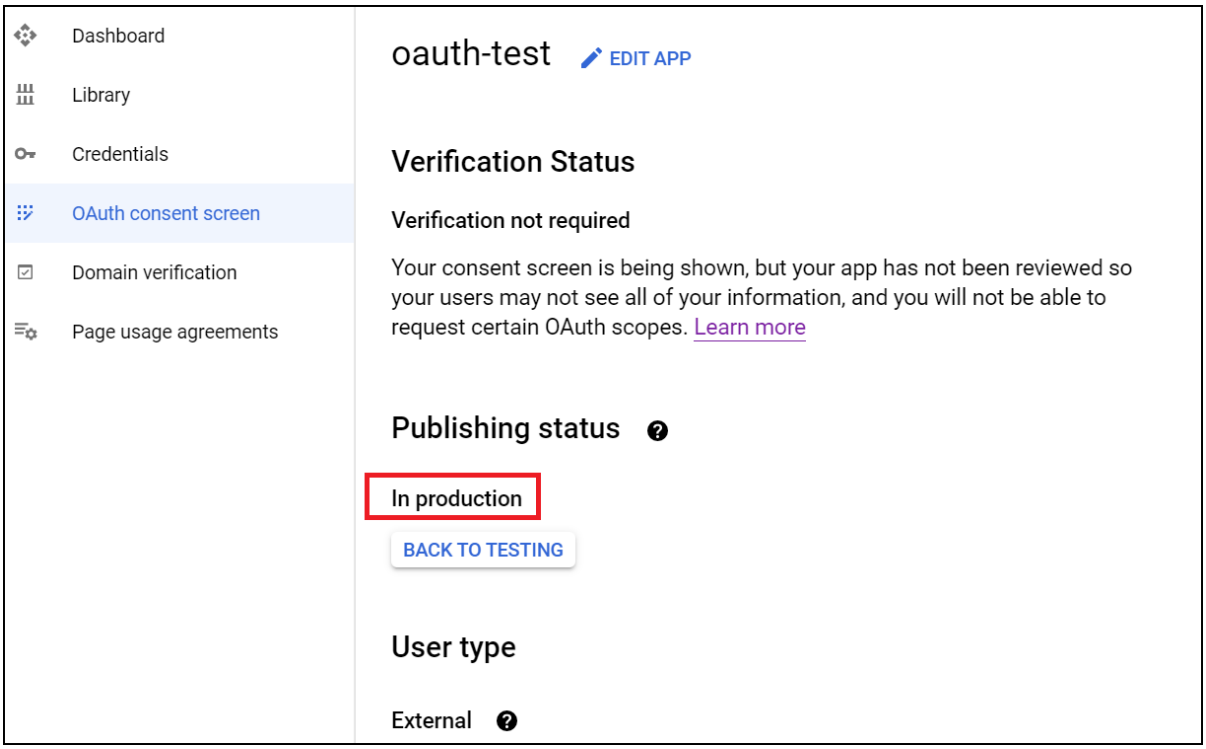


In the **Push to production** dialog box, click **Confirm**.



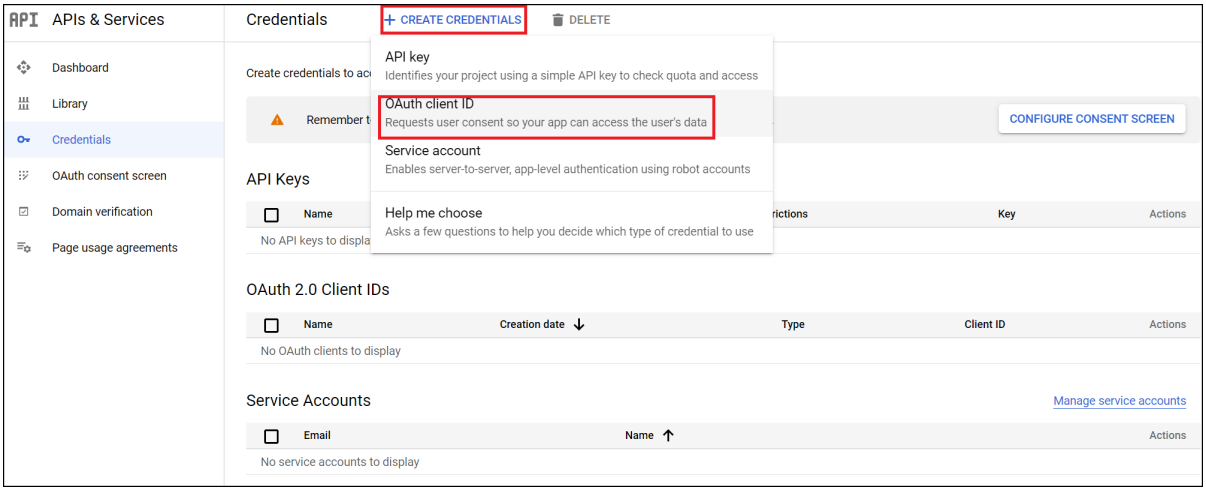
9. Under **Publishing status**, change the status to **In production**.

FIGURE 147 Changing the Publishing Status



10. Go to the **Credentials** page and click **CREATE CREDENTIALS** and select **OAuth client ID**.

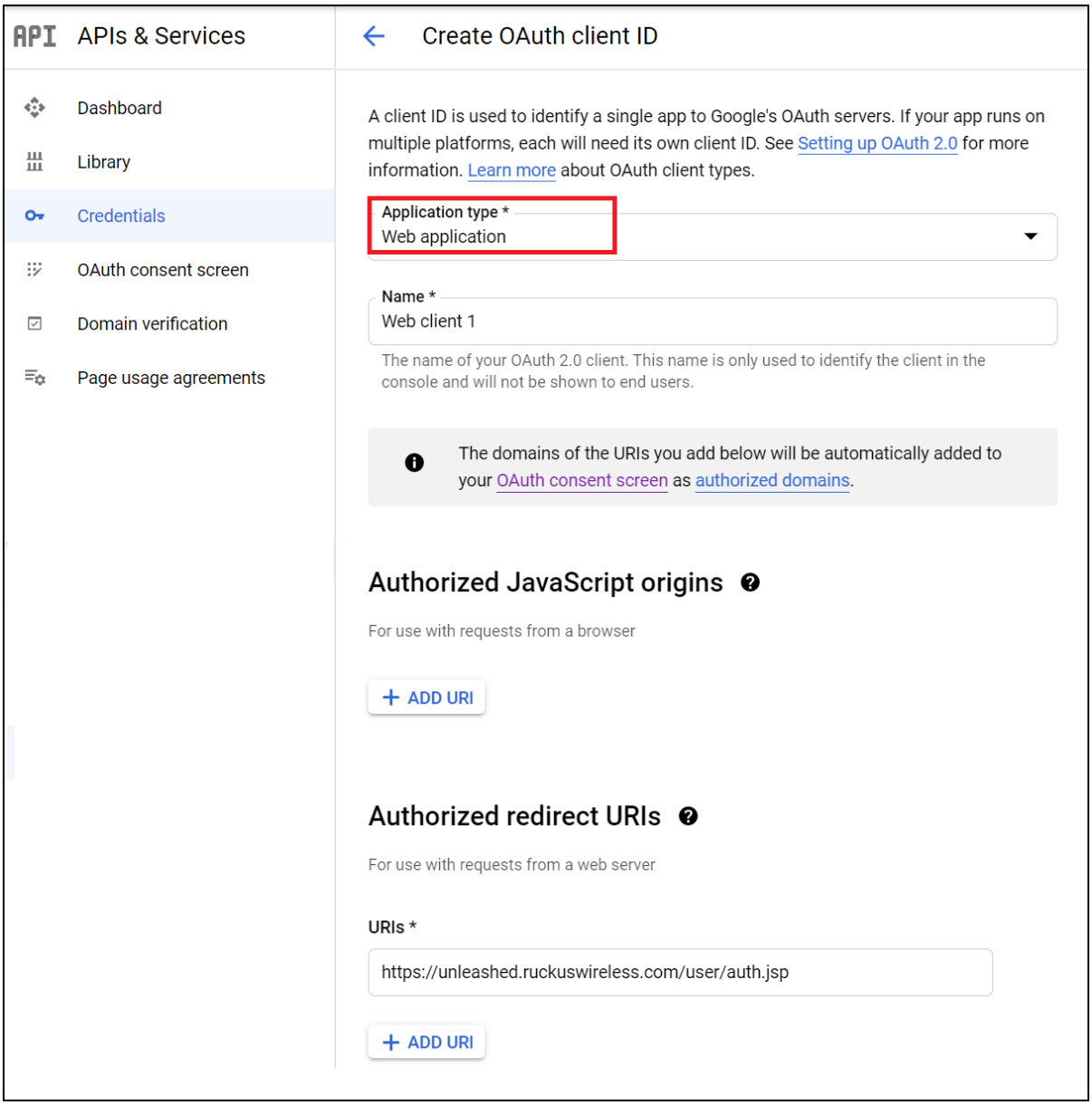
FIGURE 148 Creating Credentials: OAuth Client ID



11. For **Application type**, select **Web application** and for **Authorized redirect URIs**, enter **https://unleashed.ruckuswireless.com/user/auth.jsp**.

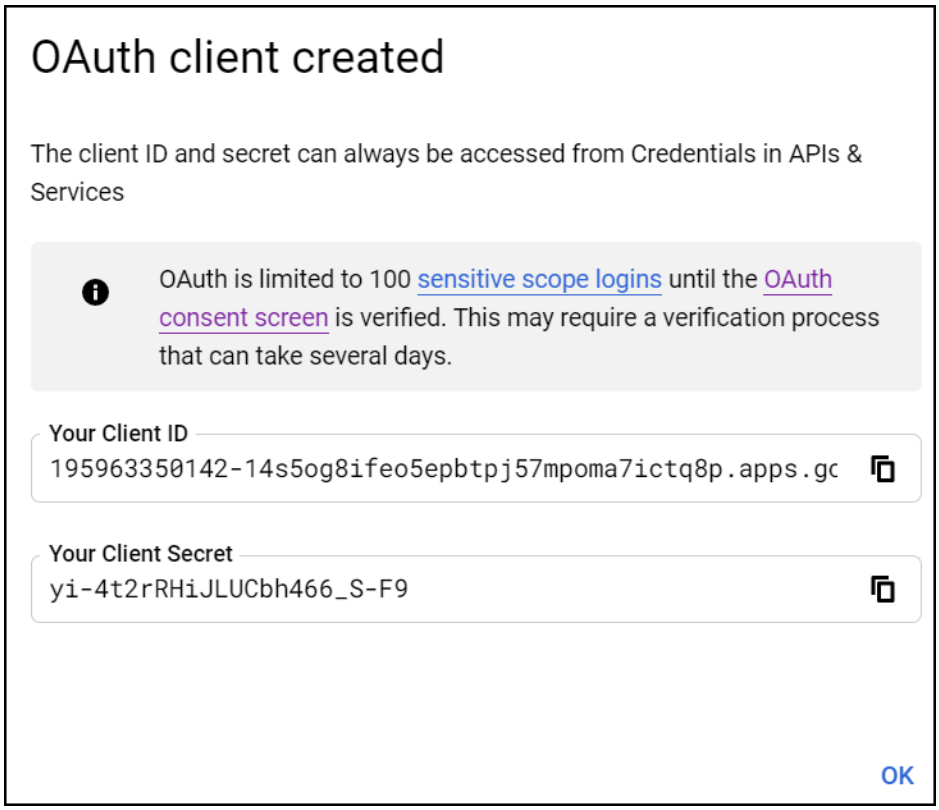
    NOTE
    If you have imported a certificate with a fully qualified domain name (FQDN) to RUCKUS Unleashed, you must use the FQDN instead of "unleashed.ruckuswireless.com". For example, if the FQDN is "mydomain.com", the **Authorized redirect URIs** will be "https://mydomain.com/user/auth.jsp".

FIGURE 149 Selecting Web Application and Entering Authorized Redirect URI



12. Click **Create**. If successful, Google displays the **Client ID** and **Client Secret**, as shown in the following figure.

FIGURE 150 OAuth Client ID and Client Secret



Take note of the Client ID and Client Secret. You will need to enter these values into the RUCKUS Unleashed web interface.

LinkedIn

To configure a LinkedIn social media WLAN, you must first configure an application on the LinkedIn developer apps website.

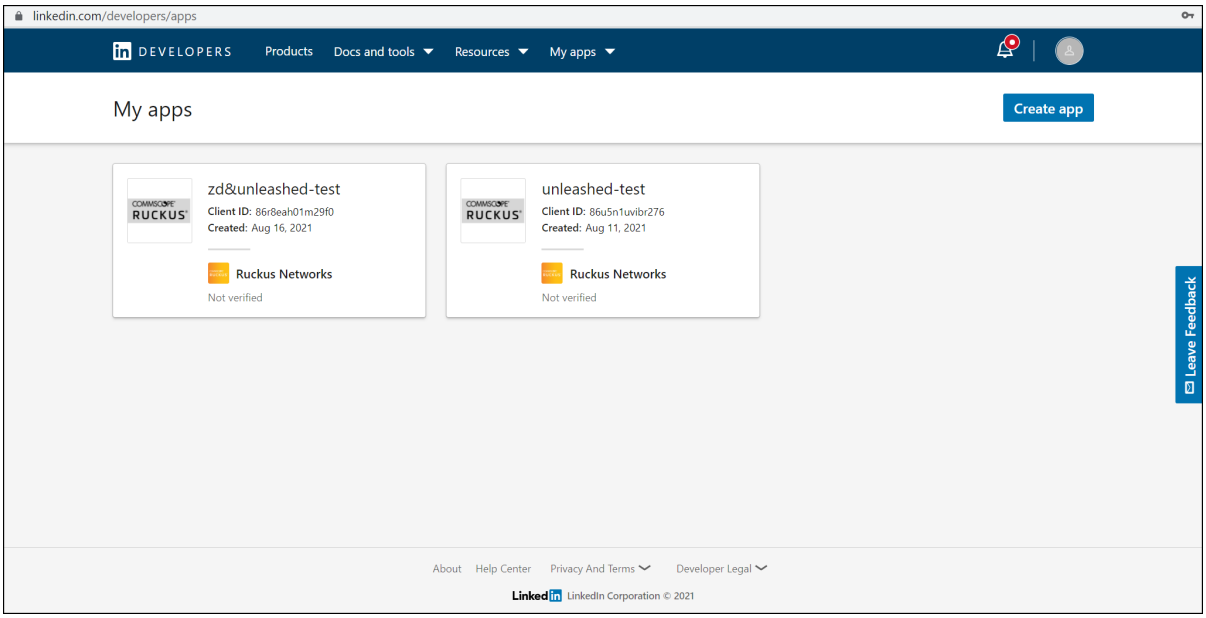
Refer to the following URL for the LinkedIn developer network: https://www.linkedin.com/developer/apps for more information.

OAuth Setup Procedure for LinkedIn Social Media Login

Complete the following steps to configure an application on the LinkedIn developers apps website.

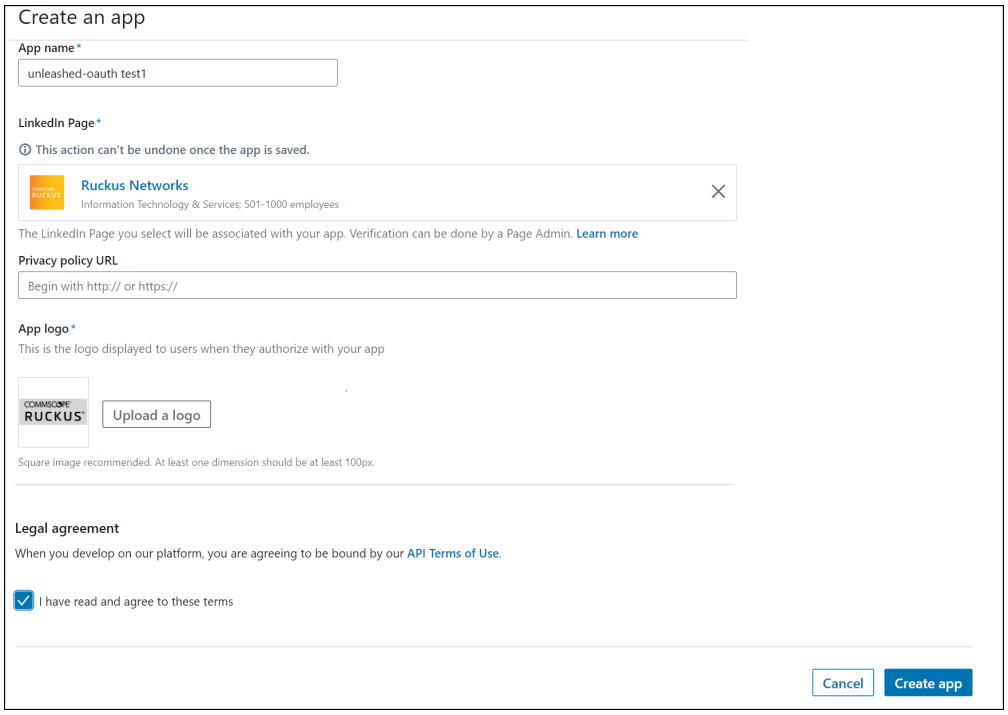
1. Go to the LinkedIn My Applications page (https://www.linkedin.com/developer/apps) and click **Create App**.

FIGURE 151 LinkedIn My Applications



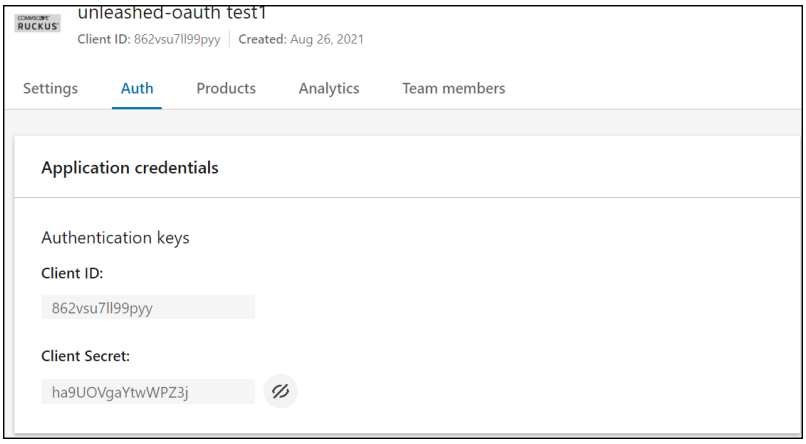
2. Enter the required information and click **Create app**.

FIGURE 152 Creating a New LinkedIn Application



3. Under the **Auth** tab, Linkedin displays the **Client ID** and **Client Secret**.

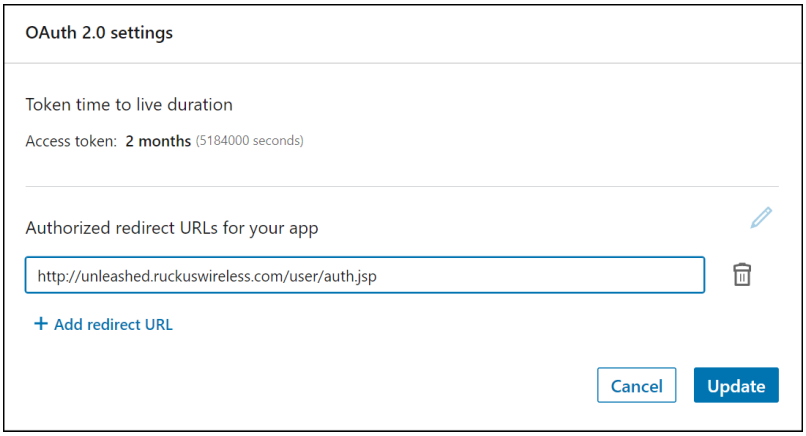
FIGURE 153 LinkedIn Authentication Keys



4. Under **OAuth 2.0 settings**, in **Authorized Redirect URLs**, enter a valid redirect callback URL: **http://unleashed.ruckuswireless.com/user/auth.jsp** and click **Update**.

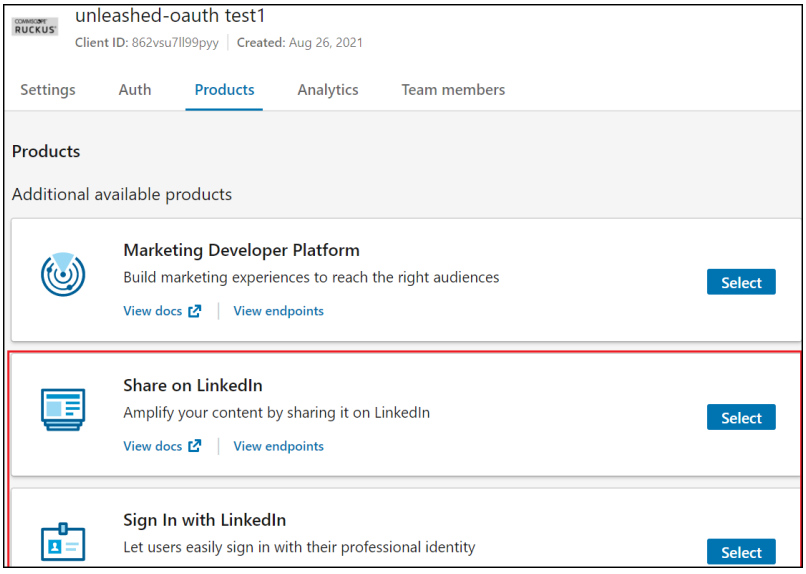
   NOTE
   If you have imported a certificate with a FQDN to RUCKUS Unleashed, you must use the real FQDN instead of "unleashed.ruckuswireless.com". For example, if the FQDN is "mydomain.com", the **Authorized redirect URLs** will be "http://mydomain.com/user/auth.jsp".

   FIGURE 154 Entering the Authorized Redirect URI



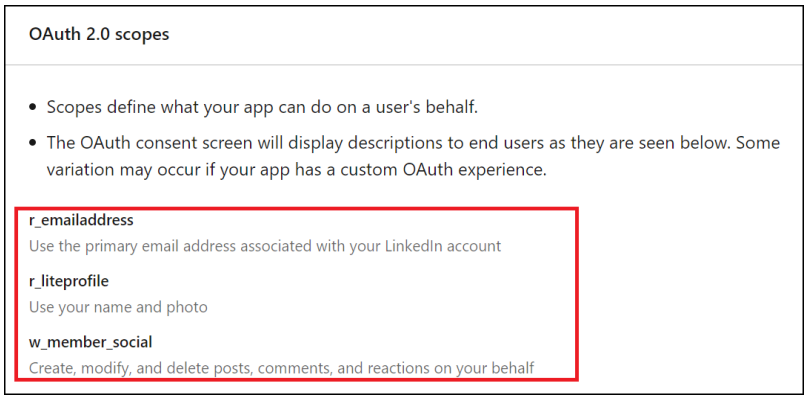
5. Under **Product** tab, select the options **Share on LinkedIn** and **Sign In with LinkedIn**.

   FIGURE 155 Sharing and Signing with LinkedIn



6. Under **Auth** tab, check if the following permissions are added successfully to use the app for LinkedIn login.

   FIGURE 156 Checking the Permissions Added for Linkedin Login



Microsoft Live

To create a Microsoft Live social media WLAN, you must first create an application on the Microsoft Live developer application page.

Go to the following URL to launch Microsoft Live development dashboard and create an application: *https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade*.

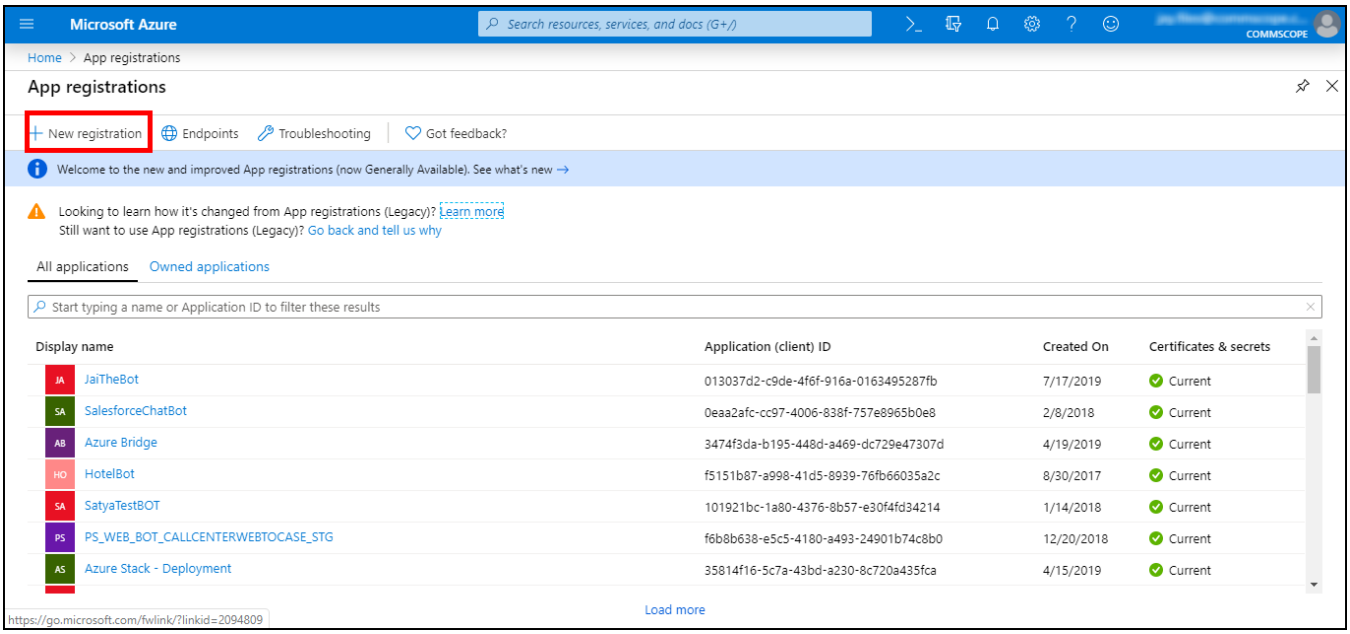
OAuth Setup Procedure for Microsoft Live Social Media Login

To generate an OAuth 2.0 ID for Microsoft Live social media WLAN login, use the following procedure:

1. Go to the following URL to launch Microsoft Live development dashboard and create an application: *https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade*.

2. Click **New Registration**.

FIGURE 157 Create a new app registration

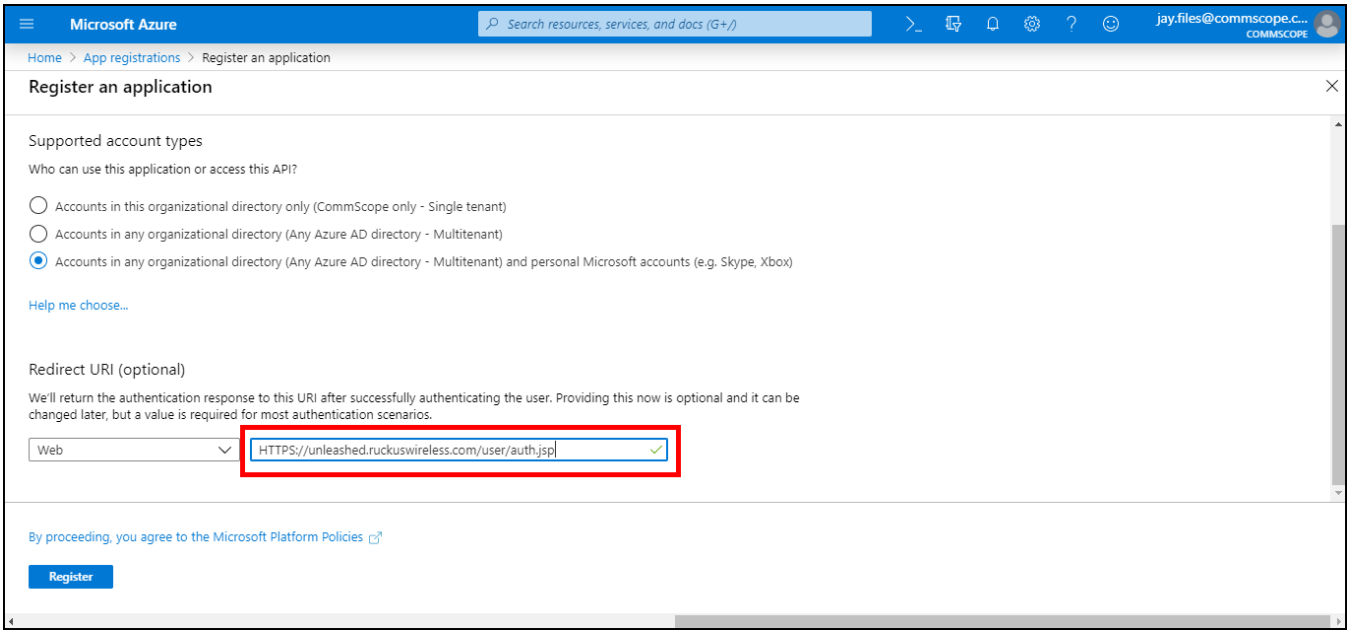


3. Enter a **Name** for the application.
4. For Support Account Types, select the **Accounts in any organizational directory and personal Microsoft accounts** button (see Figure 158).

5. In **Redirect URI:**, provide a valid redirect callback URL, for example:
   - HTTPS://unleashed.ruckuswireless.com/user/auth.jsp (see Figure 158).

     NOTE
     If you have imported an SSL certificate with a FQDN to Unleashed, you should use the real FQDN instead of "ruckuswireless.com". For example, if the FQDN is "mydomain.com", the authorized redirect URI should be "mydomain.com".

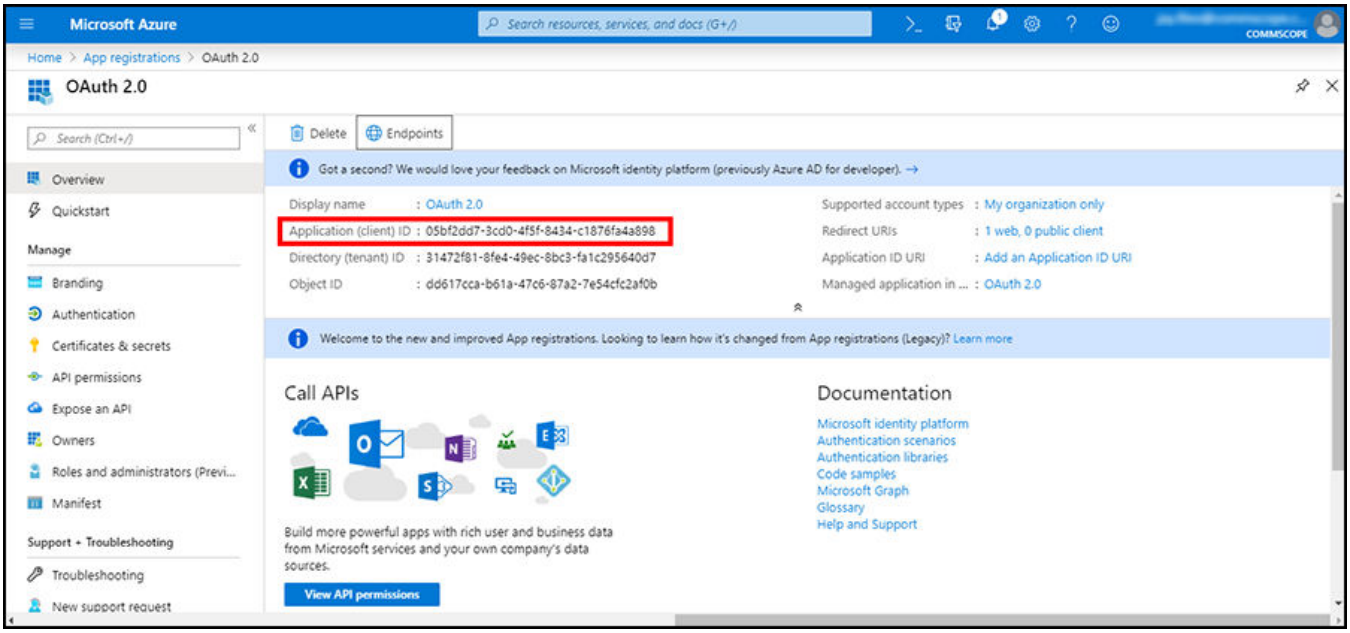
FIGURE 158 Register an Application configuration settings



6. Click **Register**.

7. Microsoft will provide you with the **Application (client) ID**. Take note of this value, as you will need to enter it into the Unleashed web interface later.

   FIGURE 159 Take note of Application (Client) ID

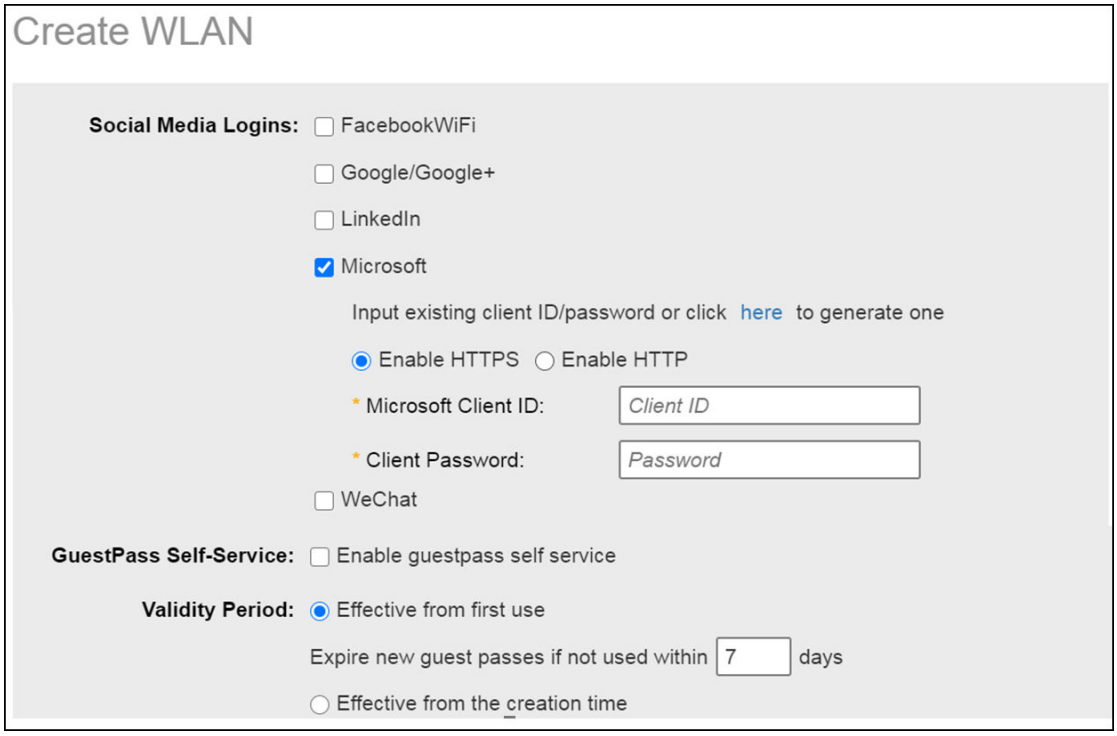


8. You also need to create a client secret by following these steps:
   a) Under **Manage**, select **Certificates & secrets**.
   b) Select the **New client secret** button.
   c) Enter a value in **Description**, select any option for **Expires**, then click **Add**.
   d) Copy and save the client secret before leaving the page, as you will need to enter this value when you log in to the Unleashed web interface.

   FIGURE 160 Take note of Client Secret

9. In the Unleashed UI, use the following settings on the Create WLAN configuration screen (see below):
   - Social Media Logins: Select **Microsoft**.
   - Microsoft Client ID: This is the Application (Client) ID shown in Figure 159.
   - Client Password: The client secret described in Figure 160.

   FIGURE 161 Create WLAN configuration screen - Microsoft Social Media Login



WeChat

"WeChat Connects Wi-Fi" is a solution that allows clients to authenticate to a wireless LAN easily using a WeChat login instead of a username/password.

The solution also allows business owners to easily serve advertisements to visitors, enabling convenient monetization of their Wi-Fi service.

The RUCKUS WeChat WLAN implementation supports the WeChat mobile app only; the desktop version is not supported, nor are smart phones without the WeChat app (web browser login is not supported).

Connecting to a WeChat WLAN

When a user connects to a WeChat WLAN, the WeChat app launches automatically and attempts to authenticate the user to the WLAN using the user's WeChat login credentials.

To connect to a WeChat WLAN:

1. The user connects to the WeChat WLAN, and launches a web browser. (Depending on OS, the browser may launch automatically.)
2. On the WeChat welcome screen, click "Connect to Wi-Fi via WeChat."

   The WeChat app is launched, and attempts to connect to the WeChat server automatically.

3. Once the user is authenticated, the app then displays a connection successful message along with the customer's information as configured on the customer's official WeChat account. (This can include advertisements, for example.)
4. The user clicks a button to accept the terms and conditions, and can then be redirected to the customer's website.

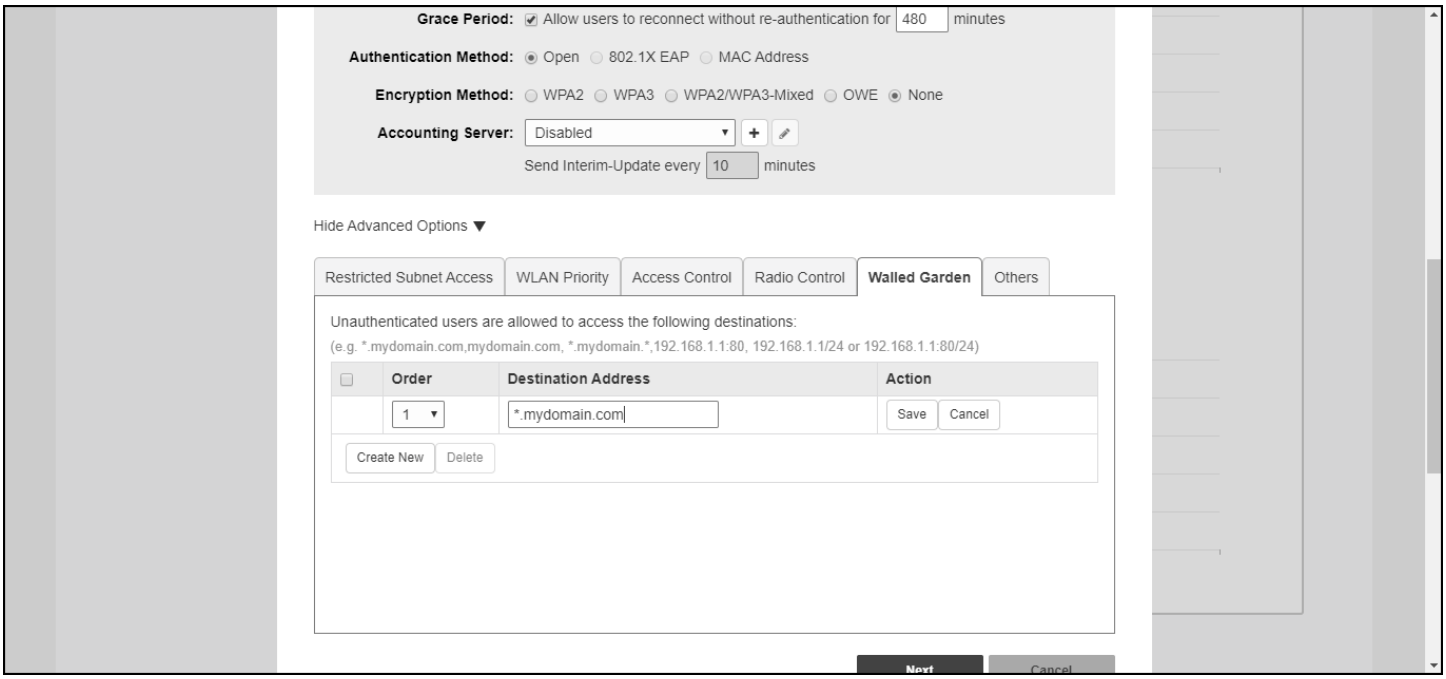
Guest Access Walled Garden

A walled garden is a list of network destinations (URLs or IP addresses) that users can access without going through authentication.

A common use case for this feature is to allow unauthenticated guests to access a company's website or other specific locations prior to entering guest pass or social media login information.

To create a guest access walled garden entry, go to **WiFi Networks > Create/Edit (WLAN) > Advanced Options > Walled Garden**. Click **Create New** to create a new rule, and enter the destination IP address or domain name in the field.

FIGURE 162 Enter domain name or IP addresses to allow access to unauthenticated users



Hotspot WLANs

A hotspot is a venue or area that provides Internet access to devices with wireless networking capability. Hotspots are commonly available in public venues such as hotels, airports, coffee shops and shopping malls.

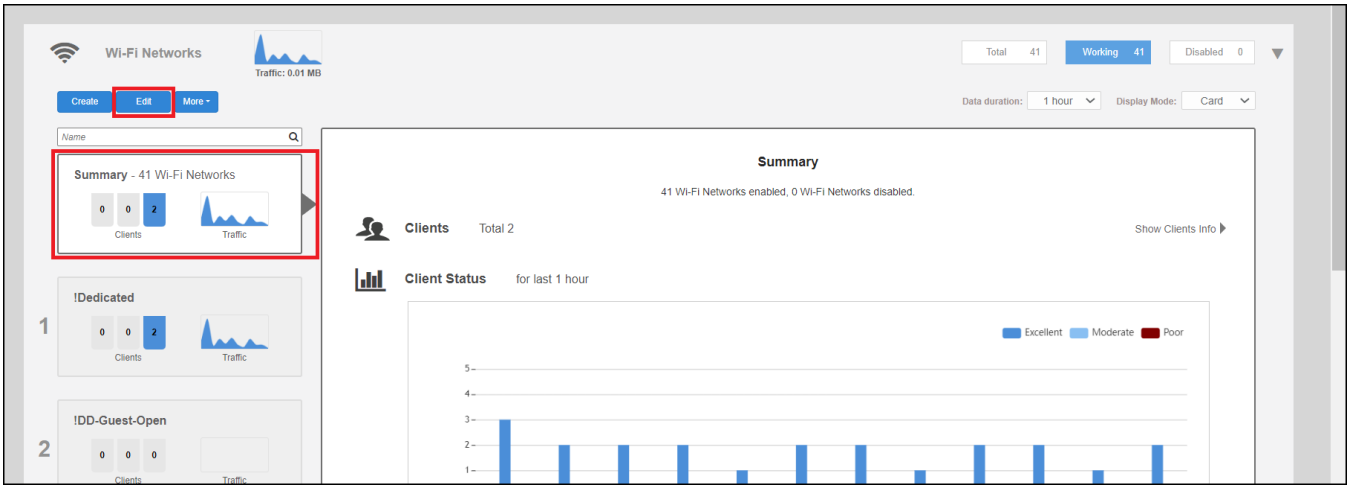
Unleashed supports Hotspot WLANs that conform to the WISPr (Wireless Internet Service Provider roaming) standard. For more information on Hotspot services, see Hotspot Services on page 436.

Configuring Global WLAN Settings

Complete the following steps to configure global settings for all WLANS.

1. In the **Wi-Fi Networks** section, select the **Summary** WLAN box, and click **Edit**.

   FIGURE 163 Configuring Global Settings for All WLANs



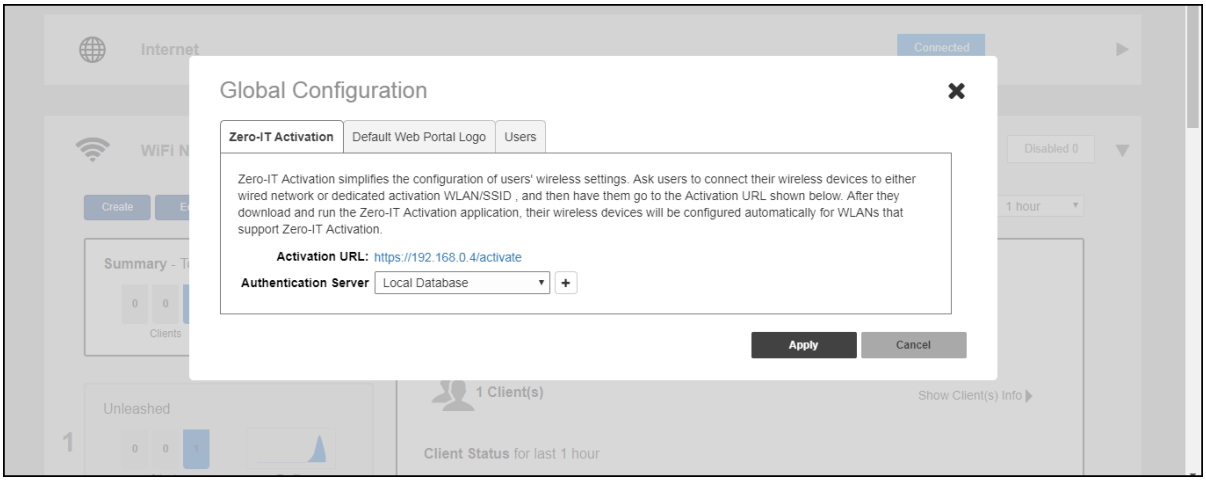
2. From the **Global Configuration** dialog box, select one of the following tabs to configure settings for all WLANs:
   - **Zero-IT Activation**: Select an Authentication Server from the list, or click **Create Service** to create a new one.
   - **Default Web Portal Logo**: Replace the RUCKUS logo with your own logo to be displayed on the login page when clients connect to a Web Auth WLAN.

     NOTE
     The recommended image size is 138 x 40 pixels. The maximum file size is 20 KB.

   - **Users**: Create new users on the internal database.

3. Click **Apply** to save your changes.

FIGURE 164 Global Configuration Settings for All WLANs



Editing an Existing WLAN

To edit an existing WLAN, expand the **Wi-Fi Networks** section, click on the **WLAN** that you want to configure, and click **Edit**.

FIGURE 165 Click Edit to edit an existing WLAN

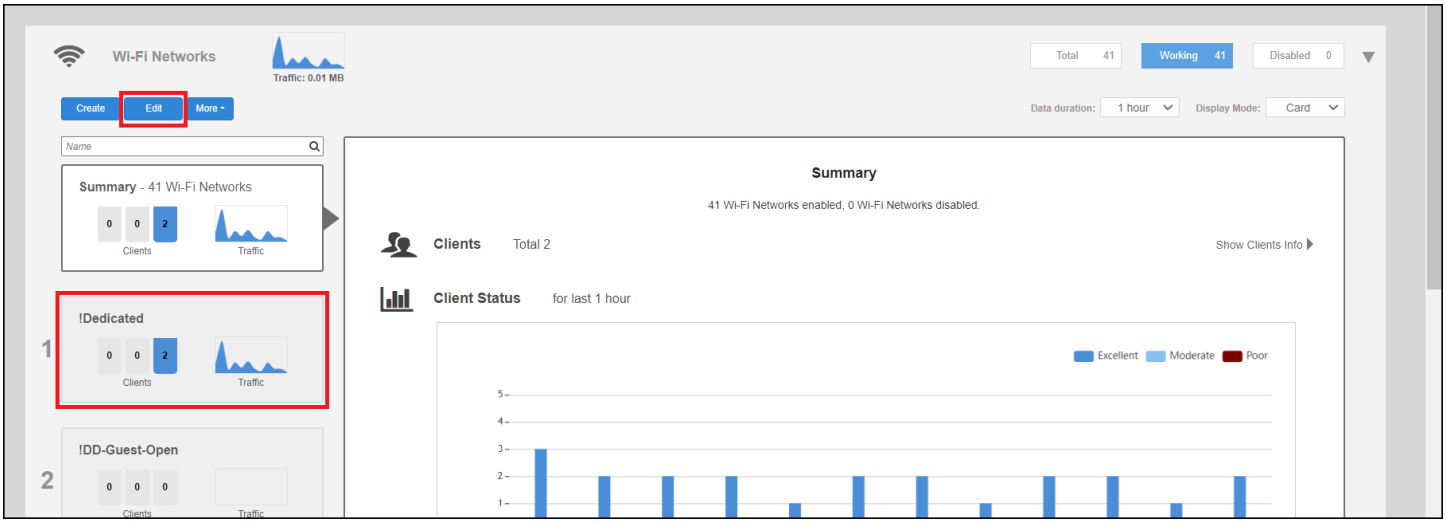
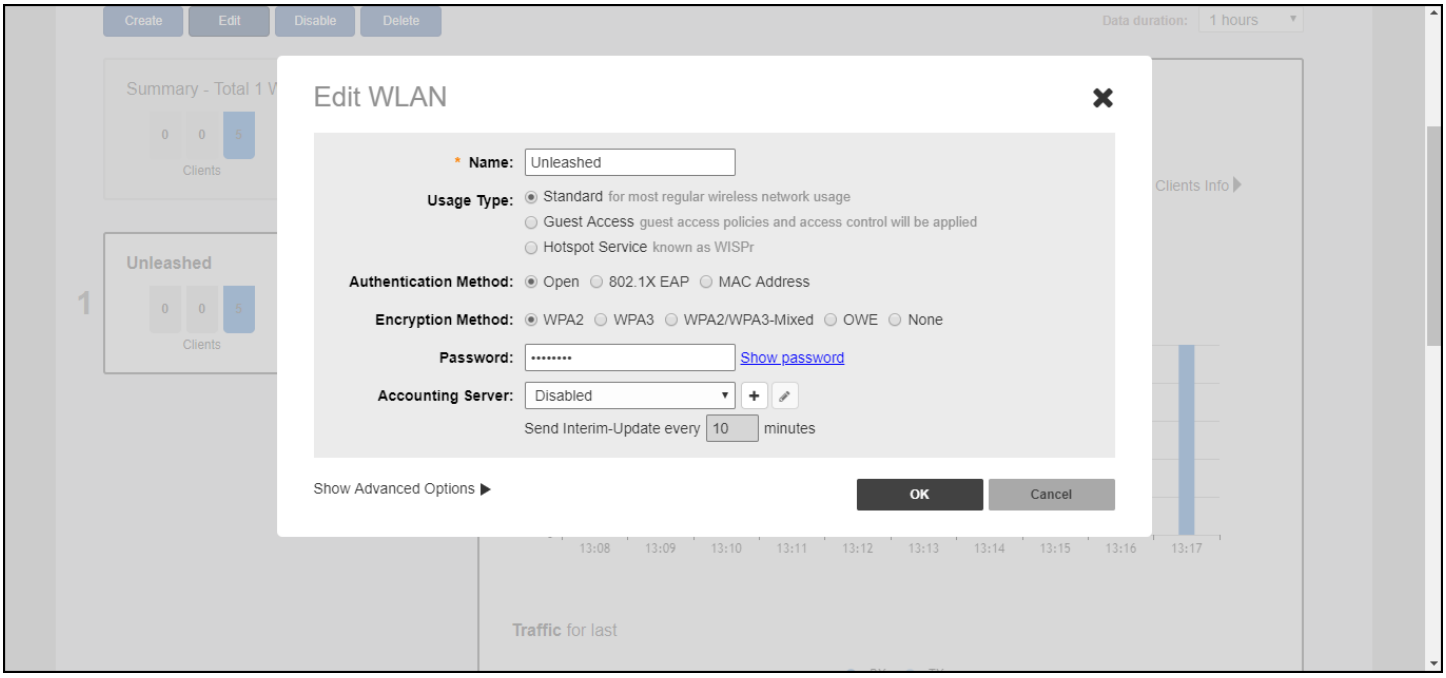


FIGURE 166 Modify WLAN settings



If you made any changes, click **OK** to confirm your changes.

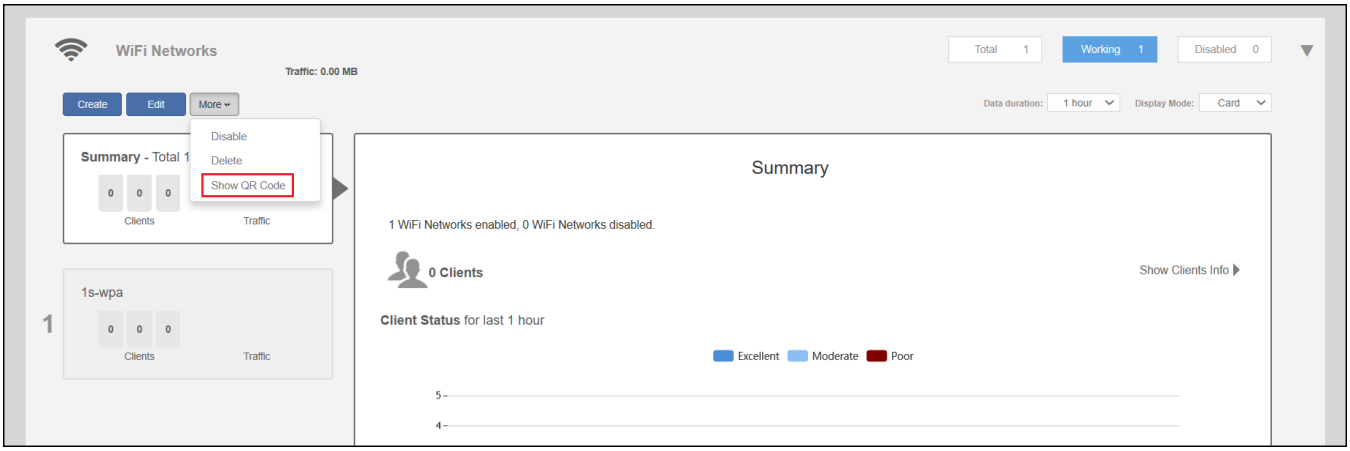
Using a QR Code to Join a Wi-Fi Network

Instead of entering a Wi-Fi password manually, you can join a Wi-Fi network using a QR code.

Complete the following steps to join a Wi-Fi network using a QR code.

1. From the **Unleashed Dashboard**, expand the **Wi-Fi Networks** and select **More** > **Show QR Code**.

   FIGURE 167 Joining a WLAN Using a QR Code



2. In the **QR Code** page, click **Print** to print the QR code or scan the QR code using a smartphone camera.

FIGURE 168 QR Code Page

The **Show QR Code** option is not supported across all WLAN types. Refer to the following table for more information.

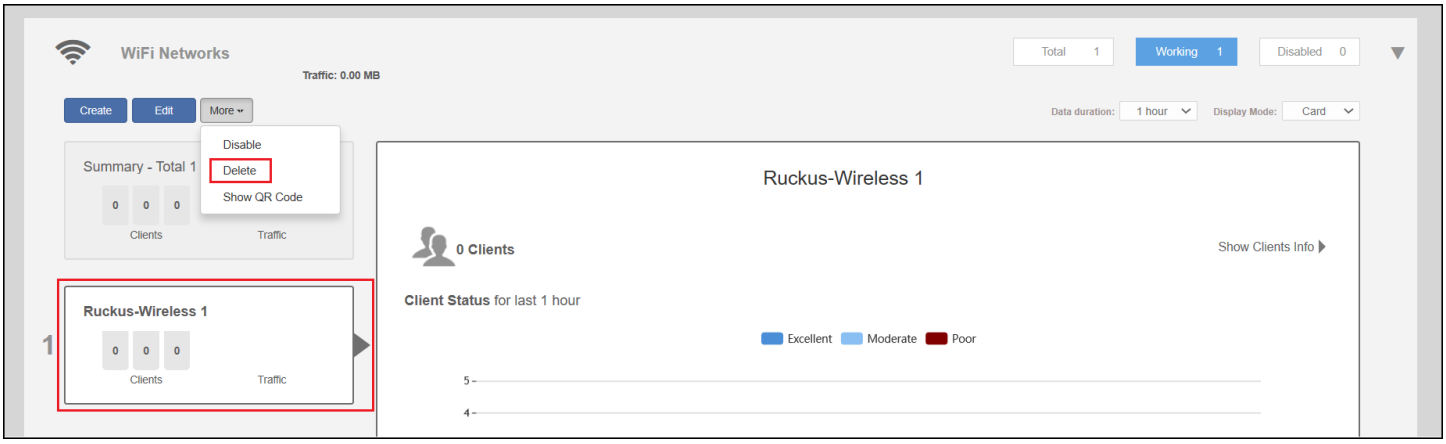
TABLE 31 QR Code Support for WLAN Types

WLAN Type	QR Code Support
Open/None	Yes
Open WPA2	Yes
Open WPA3	No
Open WPA2/WPA3-Mix	No
Open OWE	No
802.1x + WPA2	No
802.1x + WPA3	No
802.1x + WPA2/WPA3-Mix	No
MAC + WPA2	Yes
MAC + WPA3	No
MAC + WPA2/WPA3-Mix	No
MAC + None	Yes

Deleting a WLAN

To delete a WLAN, in the **Wi-Fi Networks** section, select the **WLAN box** from the list on the left side that you want to delete, and click **More** > **Delete**.

FIGURE 169 Deleting a WLAN



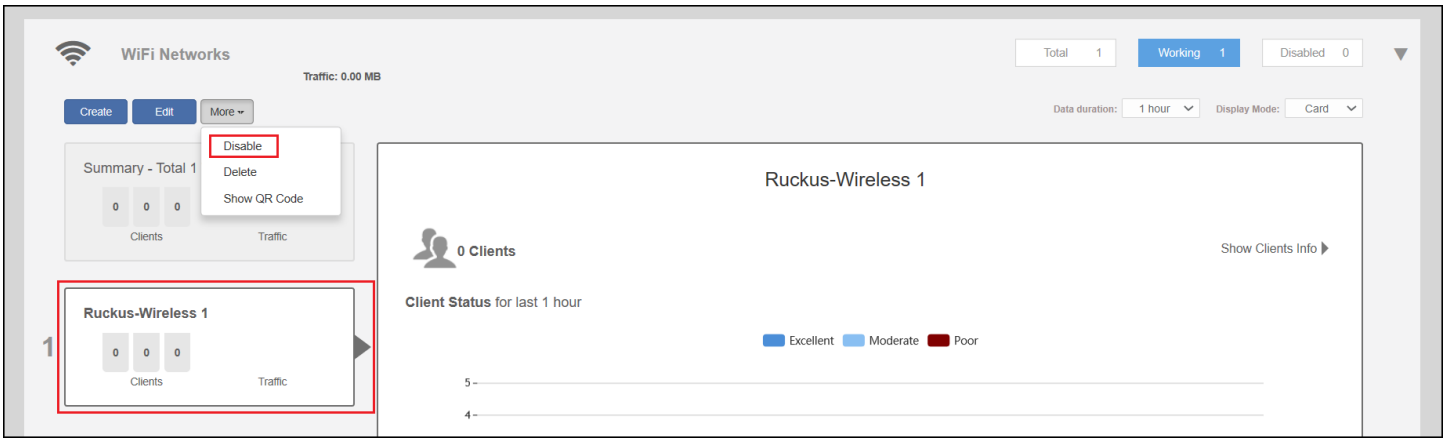
Click **OK** when prompted to delete the selected WLAN.

Disabling a WLAN Temporarily

Complete the following steps to temporarily disable a WLAN:

1. In the **Wi-Fi Networks** section, select the WLAN that you want to disable, and click **More** > **Disable**.
2. Click **OK** when prompted to disable the selected WLAN.
3. Click **Enable** to re-enable the WLAN.

FIGURE 170 Disabling a WLAN Temporarily



Advanced WLAN Configuration

- Advanced WLAN Configuration Overview....269
- Configuring Advanced WLAN Options....269
- Zero-IT and DPSK Settings....271
- WLAN Priority Settings....278
- Access Control Settings....279
- Application Policies....281
- Radio Control Settings....284
- Other Advanced WLAN Settings....286

Advanced WLAN Configuration Overview

The WLAN Advanced options include settings such as Zero-IT and Dynamic PSK options, WLAN priority, VLAN, access controls, rate limiting, application policies, URL filtering controls, radio controls and other advanced settings.

The advanced WLAN options available vary depending on the authentication and encryption methods chosen as well as the WLAN usage type.

Configuring Advanced WLAN Options

To edit the advanced options for a WLAN:

1. Select the WLAN you want to configure from the **Wi-Fi Networks** component and click **Edit**, or click **Create** to create a new custom WLAN.

2. Click the arrow next to **Show advanced options** to expand the advanced options section.

FIGURE 171 Click Show Advanced Options

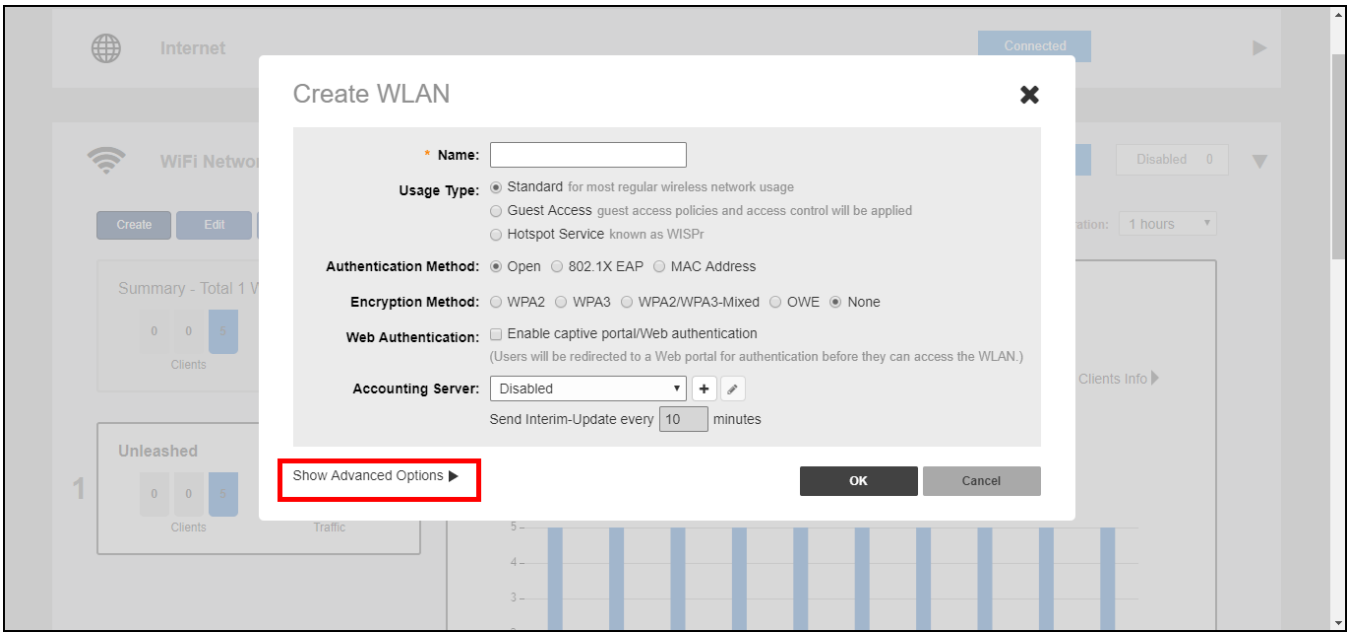
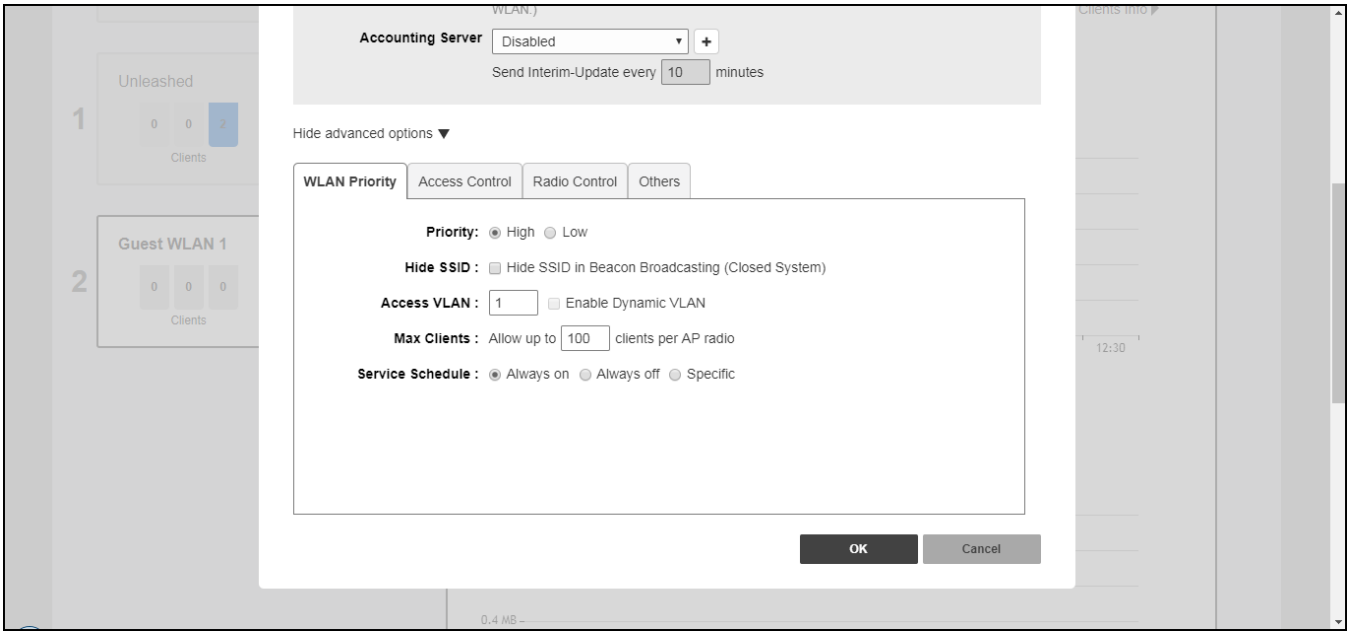


FIGURE 172 WLAN advanced options



3. Configure the following advanced options according to your preferences:
   - **Zero-IT & DPSK**: Enable and configure Zero-IT and Dynamic PSK settings for the WLAN. See Zero-IT and DPSK Settings on page 271.
   - **WLAN Priority**: Contains options for setting the WLAN's priority level, WLAN visibility, VLAN, max clients and service schedule. See WLAN Priority Settings on page 278.
   - **Access Control**: Contains options for configuring Call Admission Control, rate limiting, access controls, application visibility policies and URL filtering. See Access Control Settings on page 279.
   - **Radio Control**: Contains options for configuring radio settings including 802.11k radio resource management, Background Scanning, load balancing and band balancing. See Radio Control Settings on page 284.
   - **Others**: Contains options for configuring force DHCP, inactivity timeout, wireless client isolation, and enabling the Apple CNA bypass feature. See Other Advanced WLAN Settings on page 286.
4. Click **OK** to save your changes.

Zero-IT and DPSK Settings

Zero-IT and Dynamic Pre-Shared Key (DPSK) are two unique RUCKUS technologies that provide enhanced security, improved user credentials maintenance, and reduced IT support requirements for client wireless configuration.

Zero-IT

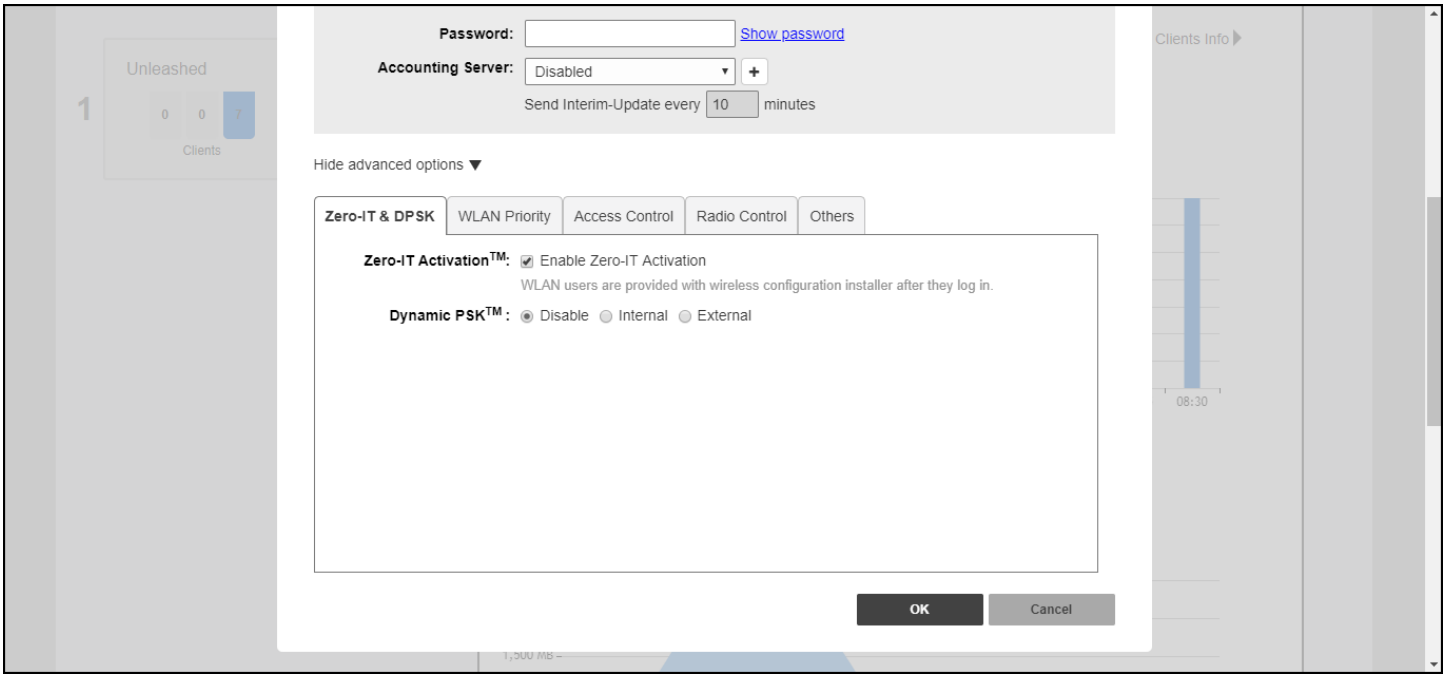
Zero-IT Activation allows network users to self-activate their devices for secure access to your wireless networks with no manual configuration required by the network administrator.

Once your Unleashed network is set up, you need only direct users to the **Activation URL**, and they will be able to automatically activate their devices to securely access your wireless LAN.

At the activation URL, users must first enter a valid user name and password to be granted this access. Users can be authenticated against either an internal database (manually configured for each user), or against an external authentication server, such as Active Directory or RADIUS. For smaller deployments, you can manually create user accounts on the internal user database from the *Admin & Services > Users* screen. If an external server is used, you must configure Unleashed with the IP address and login for the external auth server.

Once authentication is successful, a Zero-IT Activation file is downloaded and run on the client device, automatically configuring the device's wireless connection settings.

FIGURE 173 Enabling Zero-IT for a WLAN



Dynamic PSK

Dynamic PSK (DPSK) is a unique RUCKUS feature that enhances the security of normal Pre-Shared Key (PSK) wireless networks. Unlike typical PSK networks, which share a single key amongst all devices, a DPSK network assigns a unique key to every authenticated user. Therefore, when a person leaves the organization, network administrators do not need to change the key on every device.

RUCKUS DPSK offers the following benefits over standard WPA2-PSK security:

- Every device on the WLAN has its own unique DPSK that is valid for that device only (by default).
- Each DPSK is bound to the MAC address of an authorized device; even if that PSK is shared with another user, it will not work for any other machine.
- Since each device has its own DPSK, you can associate a user (or device) name with each key for easy reference.
- Each DPSK may also have an expiration date; after that date, the key is no longer valid and will not work.
- DPSKs can be created and removed without impacting any other device on the WLAN.
- If a hacker manages to crack the DPSK for one client, it does not expose other devices that are encrypting their traffic with their own unique DPSKs.

DPSKs can be created in bulk and manually distributed to users and devices, or they can be sent as part of the Zero-IT automatic provisioning file that is sent when a client connects to the network for the first time using Zero-IT Activation.

NOTE
Zero-IT and DPSK features are only available on WLANs with WPA2 encryption.

Enabling Zero-IT for a WLAN

To enable Zero-IT for a WLAN:

1. Expand the **Wi-Fi Networks** section, and click **Create** (or **Edit** an existing WLAN).
2. Select **Standard** for **Usage Type**, and either **Open** or **802.1X EAP** for **Authentication Method**, and **WPA2** for **Encryption Method**.
3. Click **Show advanced options**, then select the **Zero-IT & DPSK** tab.
4. Enable the **Zero-IT Activation** check box.
5. Optionally, enable **Dynamic PSK** to allow Zero-IT auto-configuration with Dynamic Pre-Shared Keys for each client. (See Enabling DPSK for a WLAN on page 273 for more information).
6. Click **OK** to save.

This WLAN is now ready to allow users to self-configure their client devices using a Zero-IT auto-configuration file that will be provided once a user successfully logs in to the WLAN.

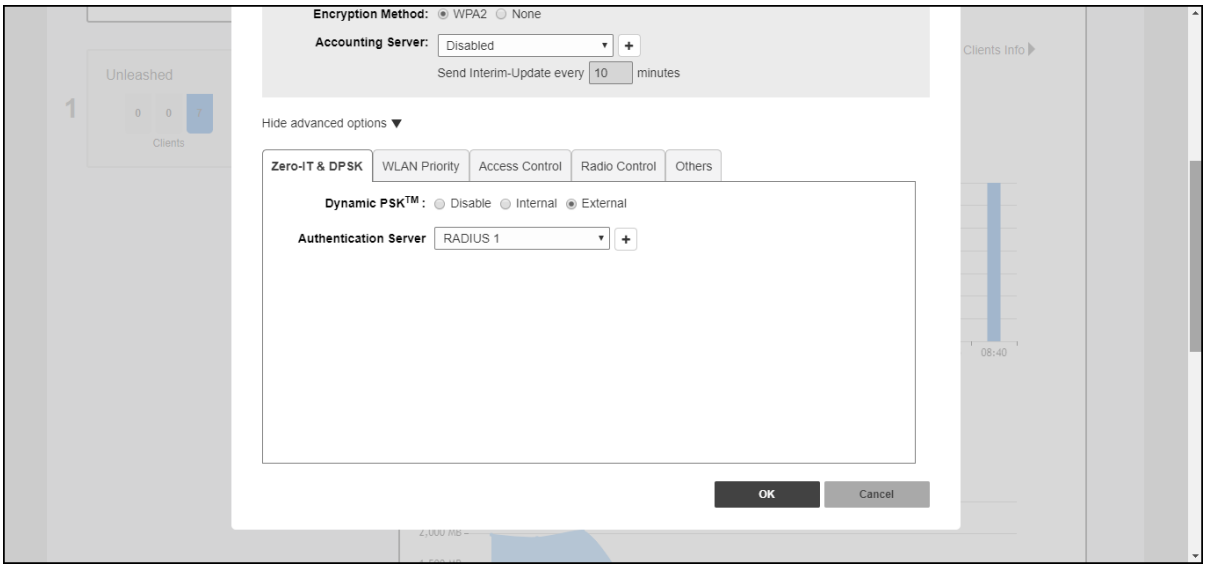
Enabling DPSK for a WLAN

Complete the following steps to enable DPSK for a WLAN.

1. Expand the **Wi-Fi Networks** section, and click **Create** to configure a new WLAN (or **Edit** for an existing WLAN).
2. For **Usage Type**, select **Standard**.
3. For **Authentication Method**, select **Open**.
4. For **Encryption Method**, select **WPA2**.
5. Click **Show advanced options** and select the **Zero-IT & DPSK** tab.
6. For **Dynamic PSK**, choose one of the following options:
   - **Internal**: Use the internal database for client authentication.
   - **External**: Use an external AAA (RADIUS) server for client authentication.

7. If using an external RADIUS server for authentication, select the authentication server from the list and click **OK** to save.

   FIGURE 174 Using an External RADIUS Server for DPSK Authentication



   If using an internal database, continue with the following steps.

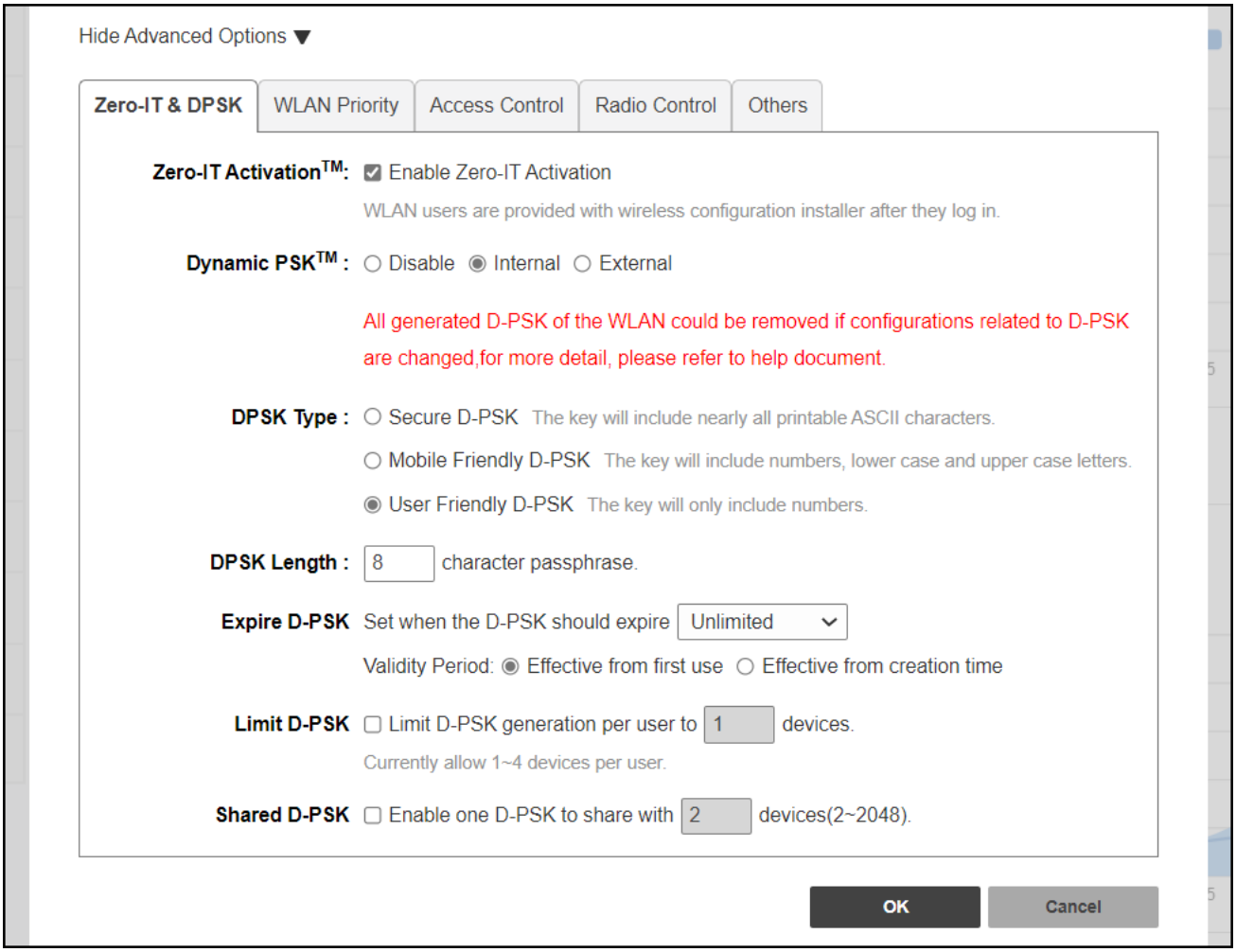
8. For **DPSK Type**, select one of the following options:
   - **Secure D-PSK**: Includes almost all printable ASCII characters, including periods, hyphens, dashes, and so on. This option is more secure; however it may be difficult to use for mobile clients whose keyboards may not contain the entire set of printable ASCII characters.
   - **Mobile Friendly D-PSK**: Select this option if this WLAN is used for mobile clients. This range of characters is limited to lowercase letters, uppercase letters, and numbers that makes it easier for users to input the DPSK when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the DPSK length to 8 characters for the convenience of your mobile client users.)
   - **User Friendly D-PSK**: This option includes numbers only. By default, the DPSK length is set to 8 characters automatically and the maximum DPSK length is 62 characters.

     NOTE
     All generated DPSK keys (only numbers) must also be unique within the same WLAN and MAC address (bound or unbound).

9. For **DPSK Length**, enter a PSK passphrase length (from 8 through 62 characters).
10. **Expire D-PSK**: Set the time interval from when the DPSK must expire. For **Validity Period**, select whether the DPSK expiration period will start from first use or the creation time.
11. **Limit D-PSK**: By default, each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs that each user can generate across multiple devices (1 through 4).
12. **Shared D-PSK**: Enable this option to allow a single user to share a single DPSK across multiple devices. By default, each DPSK is unique and mapped to a single MAC address; the **Shared D-PSK** option allows the administrator to override this rule and allow a user to share a single DPSK across multiple devices.
13. Click **OK** to save your changes.

This WLAN is now ready to authenticate users using DPSKs once their credentials are verified against either the internal database or an external AAA server.

FIGURE 175 Using the Internal Database for DPSK Authentication



NOTE
For information on DPSK management and batch generation, refer to Dynamic PSK on page 428.

DPSK Functionality for Legacy and Non-Legacy Devices

The following use cases apply to DPSK functionality for legacy and non-legacy devices:

- If you change the name of the **WLAN SSID**, Unleashed deletes all the DPSKs of legacy and non-legacy devices.
- If **Dynamic PSK** is changed from **Internal** to **External** or **Disable**, Unleashed deletes all the DPSKs of legacy and non-legacy devices.
- If **DPSK Validity Period** or **Shared DPSK** options are changed, Unleashed deletes all the DPSKs of non-legacy devices only.
- If **Allow Legacy Devices to connect to WLAN by previous password** is disabled, Unleashed deletes DPSKs of legacy devices only.
- If the legacy device is unmarked, Unleashed deletes the DPSK of this legacy device.
- If the legacy device is deleted from the UI, Unleashed does not delete the DPSKs of this legacy device.

Using External DPSK with RADIUS Authentication

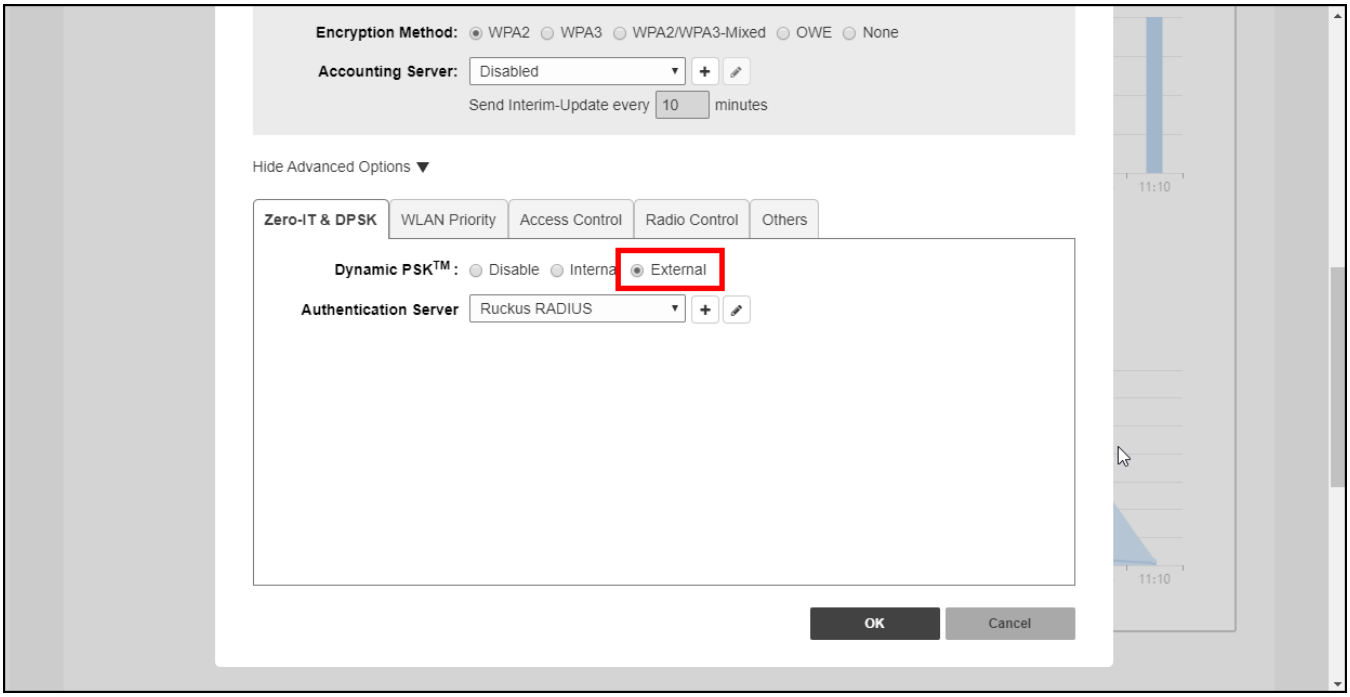
Using an external AAA server for managing Dynamic Pre-Shared Keys provides several advantages to internal DPSKs stored on the AP or controller.

The external DPSK feature allows customers to exceed the maximum number of DPSKs that can be stored on the controller, and provides the option to store and manage DPSKs on the AAA server for distribution to multiple controllers.

To enable external DPSK using an external authentication server:

1. Go to **WiFi Networks > Create/Edit WLAN > Advanced Options > Zero-IT & DPSK**.
2. In **Dynamic PSK**, select **External**.
3. In **Authentication Server**, select or create an AAA server entry.
4. Click **OK**.

FIGURE 176 External DPSK



5. The controller will send `Access-Request` messages to the RADIUS server with following attributes: `Ruckus-SSID, Ruckus-BSSID, User-Name, Ruckus-Dpsk-Params`.
6. The AAA server sends back a RADIUS `Access-Accept` or `Access-Reject` message with the following attributes: `Access-Accept: Calling-station-id, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-Id, MS-MPPE-Recv-Key,Session-Timeout, Ruckus-User-Groups, User-Name`. The `MS-MPPE-Recv-Key` is mandatory.

NOTE
If the `User-Name` attribute is empty in the `Access-Accept` packet of external Radius server, the column **User** in the web UI uses the `User-name` attribute from the `Access-Request` packet of Unleashed.

7. The AAA server generates a DPSK key (PMK) for each wireless station. This key is encrypted and entered in the attribute `MS-MPPE-Recv-Key: PMK = PBKDF2_SHA1(PassPhrase, Wlan-SSID, Wlan-SSID-Len, 4096, 32)`. See RFC2548 Chapter 2.4.3.

   NOTE
   The `WLAN-SSID` attribute will exist in the authentication request. The AAA server can use this value to generate the PSK or the AAA server can be pre-configured with WLAN-SSID value.

8. The AAA server calculates the wireless station's Pairwise Transient Key (PTK) from the `Ruckus-Dpsk-Params` attribute (`AKM Suite, Cipher, Anonce, EAPOL-Key-Frame`) in the `Access-Request` message and generates the PMK key, and finally verifies the Key MIC of the station. If it matches, the RADIUS server will send back an `Access-Accept` message with the `MS-MPPE-Recv-Key` attribute.
9. With the DPSK keys generated managed by the AAA server, the controller's internal max DPSK limits are avoided and an unlimited number of DPSKs can be generated.

External DPSK RADIUS Attribute Value Pairs

The RADIUS Attribute Value Pairs (AVP) and Vendor Specific Attributes (VSA) used in external DPSK generation are listed in the following table.

The following parameters are used in access-request messages.

TABLE 32 Access-Request message parameters

	Parameter	AVP / VSA name	Comment
1	SSID	Ruckus-SSID	Since DPSK passphrases are bound to SSIDs, it's expected that AAA server will have the PMK lists indexed by SSID value.
2	UE's MAC address	User-Name	This AVP chosen for backward compatibility with MAC Authentication use case. The AAA server can override this value with a real (human or account) user-name when User-Name AVP is included in an Access-Accept or Access-Reject message.
3	AP's BSSID	Ruckus-BSSID	Note: the AAA Interface Document needs to be updated. Currently it states, "BSSID for each WLAN in each radio"; however, only a single BSSID (the one the client has associated with) is included in the VSA.
4	Anonce	Ruckus-DPSK-params	This is a new RUCKUS VSA, defined below.
5	Snonce	Ruckus-DPSK-params	The Snonce is parsed from the EAPOL Key Frame field of Ruckus-dpsk-params.
6	MIC	Ruckus-DPSK-params	The MIC is parsed from the EAPOL Key Frame field of Ruckus-dpsk-params.
7	4WHS-M2 EAPOL Key frame	Ruckus-DPSK-params	The EAPOL-Key-Frame is used for the MIC calculation.
8	Cipher	Ruckus-DPSK-params	If the UE has negotiated TKIP-based encryption (this would be a really old device), then the key integrity algorithm is different than AES (Advance Encryption Standard, the encryption algorithm currently in use). In this case, AAA server also has to use the same algorithm as the UE in order to properly identify the PMK. TKIP is indicated according to the Cipher octet (see below). Note that two different integrity algorithms are used: HMAC-SHA1 ands HMAC-MD5.
9	AKM Suite	Ruckus-DPSK-params	The use of the AES key integrity and key hierarchy is indicated by the AKM Suite value. If the UE has negotiated FT encryption (FT - fast transition, aka 802.11r), generating the PTK from the PMK uses a different algorithm than AES. In this case, AAA server also has to use the same algorithm as the UE in order to properly identify the PMK. The AKM Suite value indicates whether FT is used.

The following parameters are used in access-accept/access-reject messages.

TABLE 33 Access-accept/Access-reject message parameters

	Parameter	RADIUS AVP or VSA name	Mandatory / Optional	Comment
1	MS-MPPE-Recv-Key	MS-MPPE-Recv-Key	Mandatory	Included whenever the AAA server has found a matching PMK (for either bound or unbound case).
2	PMK-time	Session-Timeout	Mandatory	Included whenever the AAA server has found a matching PMK, this is PMK expired time for the controller. Its range could be 0-14400 minutes.
3	User-name	User-name	Optional	Included if admin desires the username to be included in syslog events generated by the controller.
4	VLAN assignment	The following triplet of AVPs: 1. Tunnel-Type 2. Tunnel-Medium-Type 3. Tunnel-Private-Group-Id	Optional	Included if admin requires dynamic VLAN assignment. Note: the Tag field in all three AVPs is set to the same value (see RFC-2868). 1. Tunnel-Type is set to the value "VLAN". Note: the AVP encodes this enumeration as an integer set to the value of 13 (see RFC-3580). 2. Tunnel-Medium-Type is set to the string value of "802" 3. Tunnel-Private-Group-Id is set to the value "<VLAN ID>". VLAN ID has a value between 1 and 4094 and is encoded as a string (see RFC-3580).
5	Ruckus-User-Groups	Ruckus-User-Groups	Optional	Ruckus-User-Groups is used as Role of UE, It is the same as "Group Attributes " in ZD WebUI Configuration "Roles and Policies ".
6	Authorization reason	Reply-message	Optional	Included if AAA server sends an Access-Accept in the workflow for DPSK passphrase renewal. When included, the ZD shall copy the contents of this AVP to the relevant syslog message (event ID 206 clientAuthorization).

WLAN Priority Settings

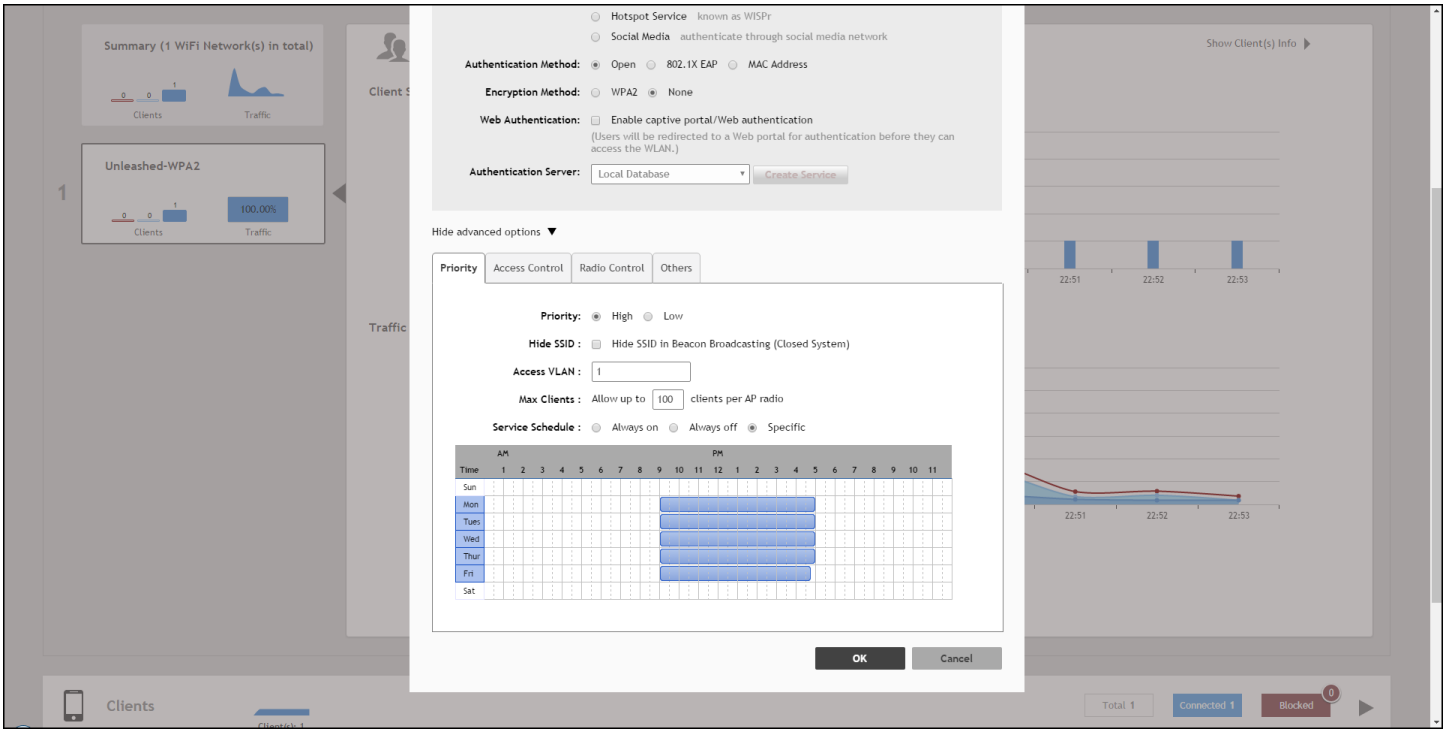
The **WLAN > Advanced Options > Priority** tab provides the following options:

- **Priority**: Set the priority of this WLAN to *Low* if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to "Low." By default, all WLANs are set to High priority.
- **Hide SSID**: Activate this option if you do not want the ID of this WLAN advertised at any time. This will not affect performance or force the WLAN user to perform any unnecessary tasks.
- **Access VLAN**: By default, all wireless clients are placed into a single VLAN (with VLAN ID 1). If you want to tag this WLAN traffic with a different VLAN ID, enter a valid VLAN ID (2- 4094) in the box.
- **Enable Dynamic VLAN**: Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes. The Dynamic VLAN option is only available for 802.1X EAP WLANs with a RADIUS server configured.
- **Max Clients**: Limit the number of clients that can associate with this WLAN per AP radio (default is 100, max is 256).
- **Service Schedule**: Use the Service Schedule tool to control which hours of the day, or days of the week to enable/disable WLAN service. For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Click on a day of

the week to enable/disable this WLAN for the entire day. Colored cells indicate WLAN *enabled*. Click and drag to select specific times of day. You can also disable a WLAN temporarily for testing purposes, for example.

NOTE
This feature will not work properly if the Unleashed network does not have the correct time. To ensure the correct time is always maintained, configure an NTP server and point the Unleashed Master AP to the NTP server's IP address, as described in Configuring the System Time on page 388.

FIGURE 177 Configuring a specific Service Schedule for a WLAN



Access Control Settings

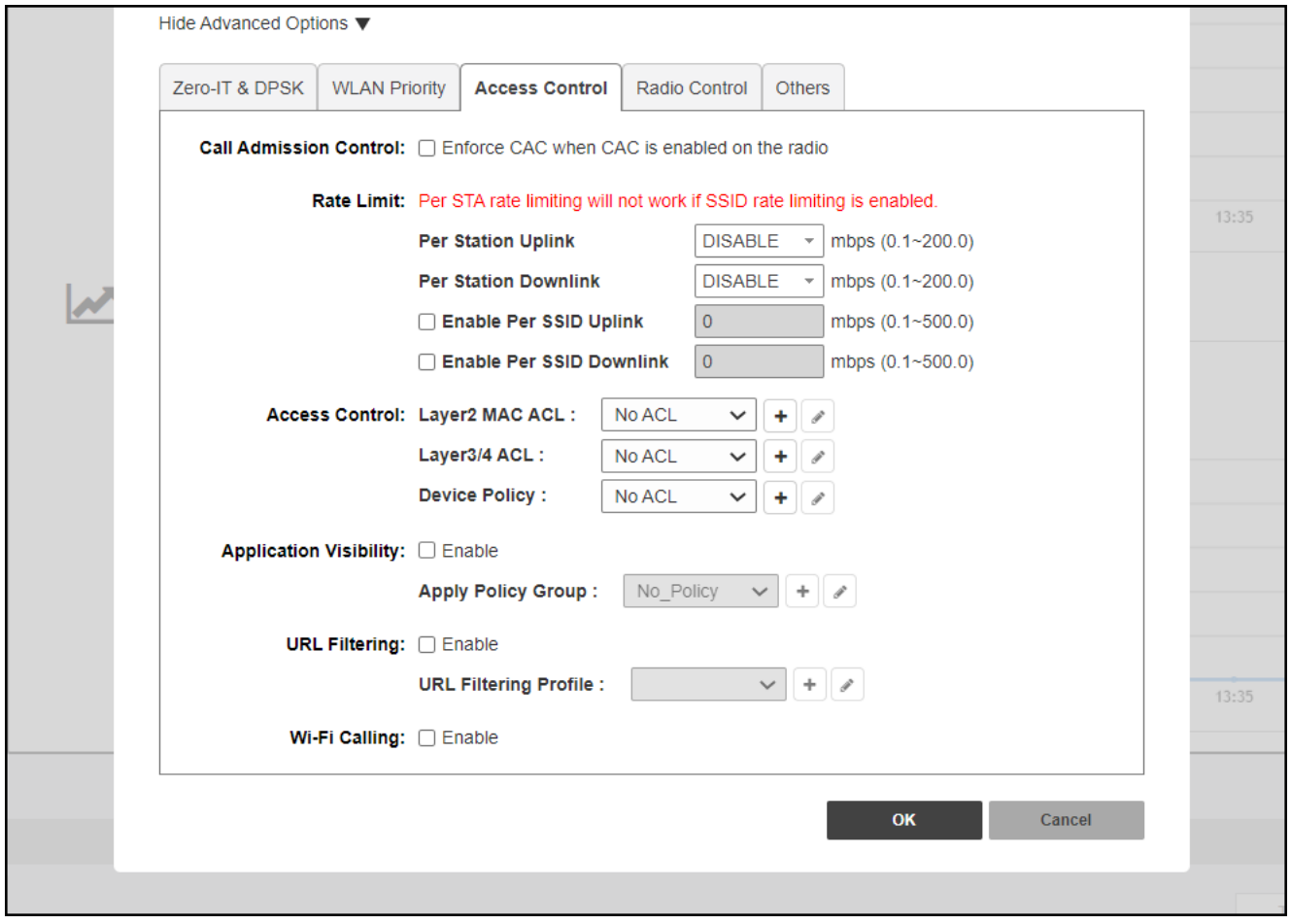
The **Access Control** tab provides the following options:

- **Call Admission Control**: (Disabled by default.) Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink Voice Interoperability for Enterprise Wireless (VIEW) certification. When enabled, the AP announces in beacons if admission control is mandatory for various access categories and admits only the traffic streams it can support based on available network resources. When network resources are not sufficient to provide this level of performance, the new traffic stream is not admitted. Call Admission Control is effective only when both the AP and the client support WMM-AC. RUCKUS APs are capable of handling hundreds of simultaneous clients, but when it comes to VoIP traffic, the number of VoIP calls must be policed to ensure adequate voice and video quality. RUCKUS recommends limiting bandwidth allocation to six calls (four active calls and two reserved for roaming) on the 2.4 GHz radio and ten calls on the 5 GHz radio (seven active calls and three reserved for roaming). Enable this feature if you want this WLAN to serve as a VoIP WLAN to support Spectralink phones.
- **Rate Limit**: Rate limiting controls fair access to the network. When enabled, the network traffic throughput of each network device (that is, a client) is limited to the rate specified in the traffic policy, and that policy can be applied on either the uplink or downlink. Use the

Uplink and/or Downlink drop-down lists to limit the rate at which WLAN clients upload/download data. The "Disabled" state means rate limiting is disabled; thus, traffic flows without prescribed limits.

- **Access Control**: Use this drop-down list to select Access Control Lists (L2 or L3/L4) and Device Policy to apply to this WLAN. An access control entry or a device policy must be created before being available here. For more information, refer to Access Control on page 415.
- **Application Visibility**: Enable Application Visibility to allow APs to collect client application data, which can then be consolidated for use by the application recognition and control pie charts (refer to Application Recognition and Control on page 419), and can be used to deny access or rate limit application traffic based on administrator-configured application policies.
  - **Apply Policy Group**: This option allows the administrator to deny application access or rate limit application traffic based on predefined or user-defined applications. Using application policies, administrators can block specific applications if they are seen to be consuming excessive network resources, or enforce network usage policies such as blocking social media sites. For more information, refer to Application Policies on page 281.
- **URL Filtering**: Enable URL Filtering and select a URL Filtering Profile from the list (or create a new one). For more information, see URL Filtering on page 452.
- **WiFi Calling**: Wi-Fi Calling is a service for Android and iOS smartphones that allows clients to make and receive voice phone calls over a Wi-Fi connection. For more information, see Wi-Fi Calling on page 458.

FIGURE 178 Advanced WLAN Settings - Access Control Configuration



Application Policies

For instructions on configuring Application Control Policies, see Creating an Application Control Policy on page 281.

This option allows the administrator to deny application access by blocking any HTTP host name (FQDN - Fully Qualified Domain Name) or L4 port. Using application denial policies, administrators can block specific applications if they are seen to be consuming excessive network resources, or enforce network usage policies such as blocking social media sites.

The following usage guidelines need to be taken into consideration when defining application control policies:

- "www.corporate.com" – This will block access to the host web server at the organization "corporate.com" i.e., the FQDN. It will not block access to any other hosts such as ftp, ntp, smtp, etc. at the organization "corporate.com".
- "corporate.com" – This will block access to all hosts at the domain "corporate.com," i.e., it will block access to www.corporate.com, ftp.corporate.com, smtp.corporate.com, etc.
- "corporate" – This will block access to any FQDN containing the text "corporate" in any part of the FQDN. Care should be taken to use as long as possible string for matching to prevent inadvertently blocking sites that may contain a shorter string match i.e., if the rule is "net" then this will block access to any sites that have the text "net" in any part of the FQDN or ".net" as the FQDN suffix.
- *.corporate.com – This is an invalid rule. Wildcard "*" and other regular expressions cannot be used in any part of the FQDN.
- "www.corporate.com/games" - This is an invalid rule. The filter cannot parse and block access on text after the FQDN, i.e., in this example it cannot filter the microsite "/games".

NOTE
Many global organizations have both a ".com" suffix and country specific suffix such as ".co.uk", ".fr", ".au".etc. To block access to, for example, the host web server in all regional specific web sites for an organization, a rule like "www.corporate" could be used.

NOTE
Many global organizations use distributed content delivery networks such as Akamai. In such cases creating a rule such as "www.corporate.com" may not prevent access to the entire site. Further investigation of the content network behavior may need to be undertaken to fully prevent access.

NOTE
When using port-based rules, there is no distinction between the TCP and UDP protocols, so care should be taken if wishing to block a specific application port, as this will apply to both IP protocols and may inadvertently block another application using the other protocol.

Creating an Application Control Policy

Application control policies can be used to block access to certain applications, to rate limit traffic identified as belonging to certain applications, or to perform QoS traffic shaping on traffic identified as belonging to a certain application.

NOTE
For more information on configuring and enforcing application control policies, see Application Policy on page 421.

To create an Application Control Policy:

1. Go to **WLAN > Advanced Options > Access Control**.
2. Enable **Application Visibility**.
3. In **Apply policy group**, click **Create New** to create a new policy.

NOTE
Alternatively, go to *Admin & Services > Services > Application Recognition & Control > Application Policy* to configure multiple application policies and then apply them to WLANs one by one.

4. Enter a **Name** and optionally a **Description** for the policy.
5. In **Rules**, click **Create New** to create a new rule for this policy.
6. In **Rule Type**, select whether this will be a Denial policy, a Rate Limiting policy or a QoS policy.
7. In **Application Type**, Select **System Defined** or one of the user-defined application types (IP-based, port-based or application name-based).
8. In **Application**, select the user-defined application from the list, or select the application category and application name from the list of system-defined applications.
9. If the Rule Type you selected was Rate Limiting or QoS, enter the uplink and downlink speeds at which to limit this application, or the QoS traffic shaping rules to enforce if it is a QoS rule.

10. Click **Save** to save the rule, and click **OK** to save the policy.

FIGURE 179 Applying an Application Control Policy to a WLAN

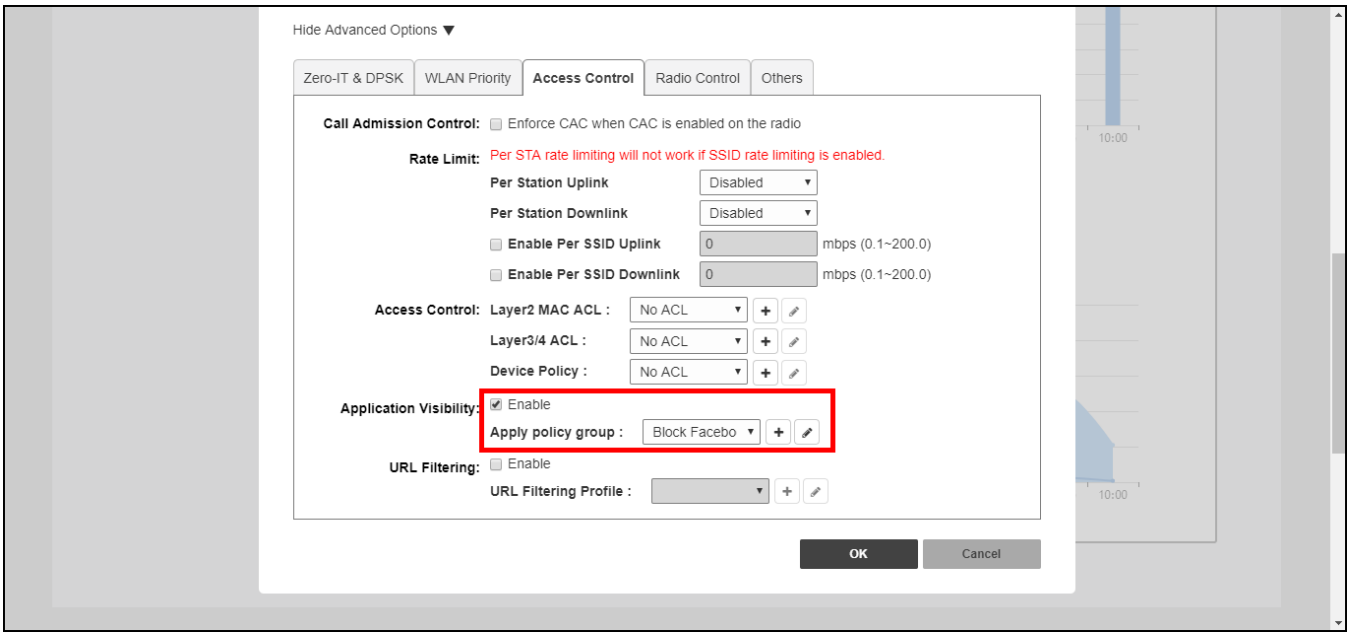
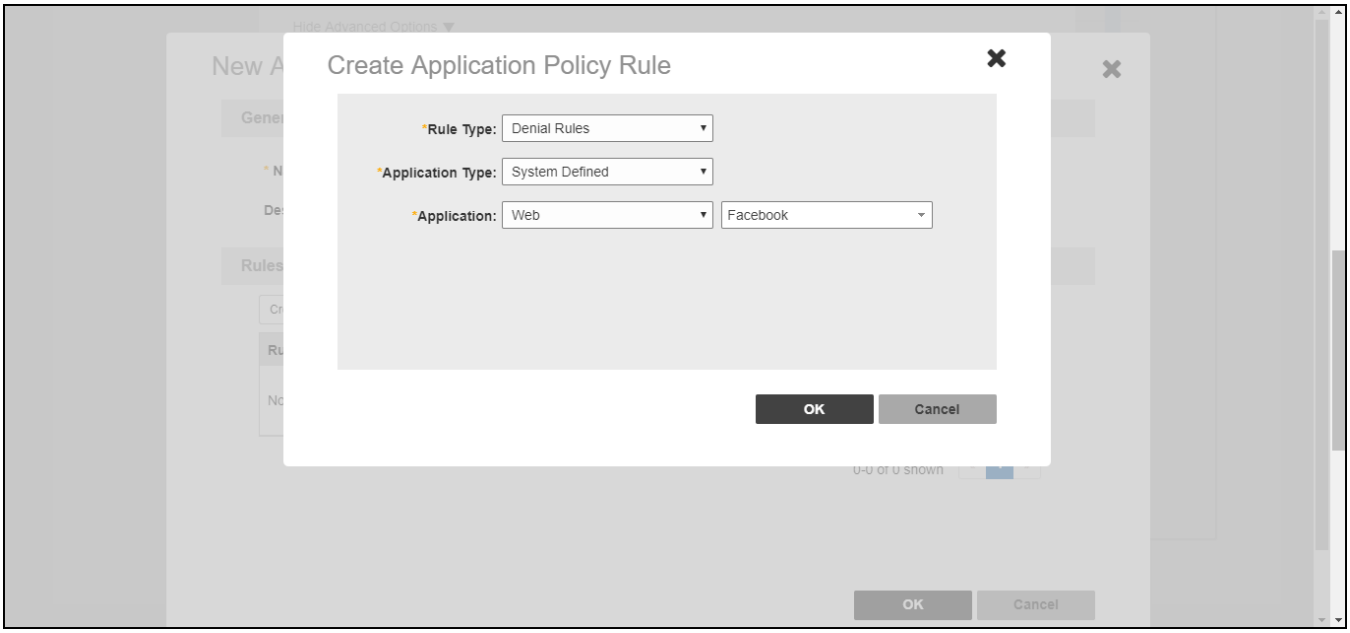


FIGURE 180 Creating an Application Control Policy for a specific website



Radio Control Settings

The **Radio Control** tab provides options for configuring radio settings for the WLAN, such as load balancing, band balancing, fast BSS transition, and radio resource management.

The following options can be configured on a per-WLAN basis:

- **Fast BSS Transition**: (Disabled by default.) The Fast BSS Transition feature uses messages and procedures defined in 802.11r to allow continuous connectivity for wireless devices in motion, with fast and secure handoffs from one AP to another. A fast BSS transition is a BSS transition in the same mobility domain that establishes the state necessary for data connectivity before the re-association rather than after the re-association. In this way, clients that support the 11r standard (including iOS devices) can achieve significantly faster roaming between APs.
- **Radio Resource Management**: (Disabled by default.) Radio Resource Management utilizes 802.11k Neighbor Reports, which are sent by the AP to inform clients of the preferred roaming target AP. The client sends a neighbor report request to an AP, and the AP returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition.
- **Background Scanning**: Background scanning regularly samples the activity in all Access Points to assess RF usage for automatic optimal channel selection, to detect rogue APs, and to determine which APs are near each other for radio resource management and load balancing. These scans sample one channel at a time in each AP so as not to interfere with network use.
- **Load Balancing**: Enabling load balancing can improve WLAN performance by helping to spread the client load between nearby access points. The load balancing feature can be controlled from within the web interface to balance the number of clients per radio on adjacent APs. "Adjacent APs" are determined by the Master AP by measuring the RSSI during channel scans. After startup, the Master AP uses subsequent scans to update the list of adjacent radios periodically and when a new AP sends its first scan report. When an AP leaves, the Master AP immediately updates the list of adjacent radios and refreshes the client limits at each affected AP. Once the Master AP is aware of which APs are adjacent to each other, it begins managing the client load by sending desired client limits to the APs. These limits are "soft values" that can be exceeded in several scenarios, including: (1) when a client's signal is so weak that it may not be able to support a link with another AP, and (2) when a client's signal is so strong that it really belongs on this AP. The APs maintain these desired client limits and enforce them once they reach the limits by withholding probe responses and authentication responses on any radio that has reached its limit.
- **Band Balancing**: (Enabled by default.) Band balancing balances the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios. To balance the load on a radio, the AP encourages dual-band clients to connect to the 5 GHz band when the configured percentage threshold is reached.
- **802.11d**: (Enabled by default.) The 802.11d standard provides specifications for compliance with additional regulatory domains (countries or regions) that were not defined in the original 802.11 standard. For optimal performance of Apple iOS devices, it is recommended that you enable this option.

  NOTE
  Some legacy embedded devices (such as wireless barcode scanners) may not operate properly if the 802.11d option is enabled.

- **Enable WLAN on**: (Enabled by default on both radios.) Manually enable or disable WLAN service per radio. Select **2.4 GHz only** to disable WLAN service on the 5 GHz radio, or select **5 GHz only** to disable WLAN service on the 2.4 GHz radio.

  This option allows you to create separate WLANs on the two radios. For example, you could create a "2.4G" WLAN with the **Enable WLAN on** feature set to **2.4 GHz only**, and a "5G" WLAN with the feature set to **5 GHz only**.

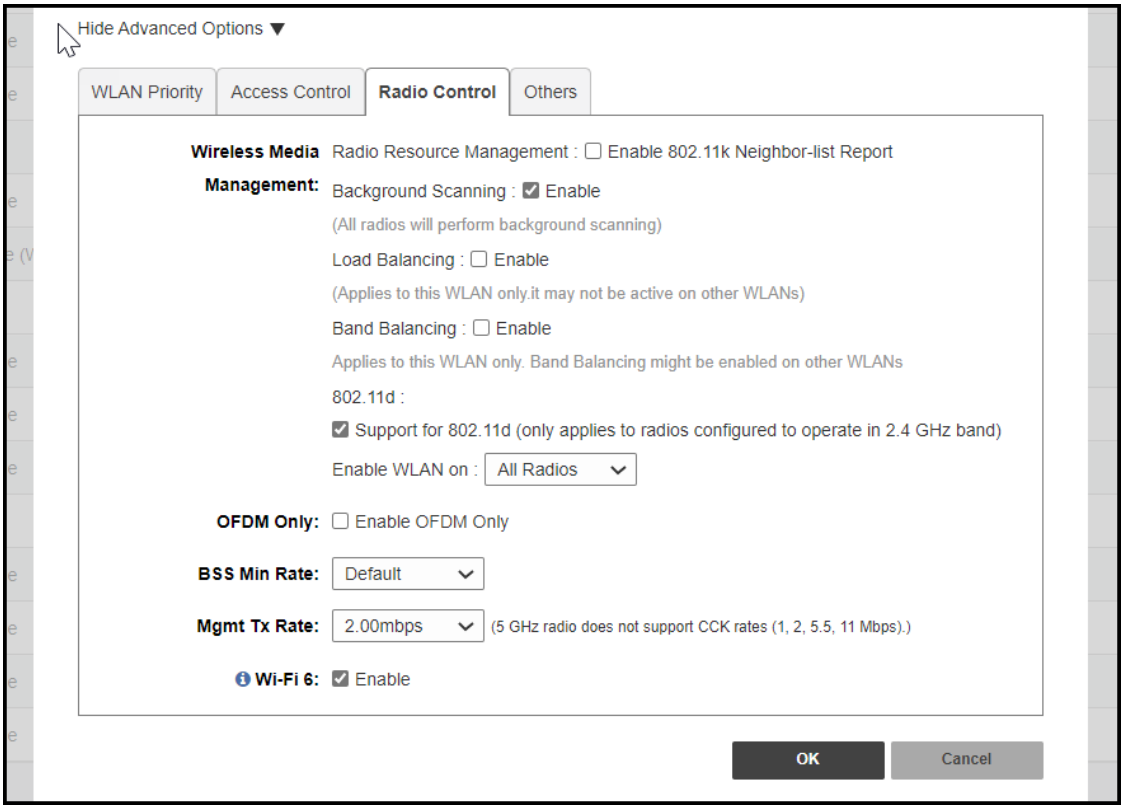
  For more information, refer to Creating Separate WLANs for 2.4 GHz and 5 GHz Radios on page 285.
- **OFDM Only**: Enable this option to disable CCK rates of 1, 2, 5.5, and 11 Mbps; therefore, 802.11b-only clients cannot connect to the WLAN. Beacons and probe responses are transmitted at 6 Mbps, and data 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.

- **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the WLAN. When **OFDM Only** is enabled, **BSS Min Rate** offers three options: **Default**, **12 Mbps**, and **24 Mbps**. If set to **Default**, **Mgmt Tx rate** is fixed at 6 Mbps. This option can also be used to prevent 802.11b clients from connecting, and to allow greater client density with higher data rates.

  NOTE
  When **BSS Min Rate** is set to a non-default value, **Mgmt Tx Rate** cannot be set manually and its value must be consistent with **BSS Min Rate**.

- **Mgmt Tx Rate**: Use this setting to configure the rate at which management frames are sent. The default is 2 Mbps. This option is only available if both **OFDM Only** and **BSS Min Rate** are disabled. (Otherwise, **Mgmt Tx Rate** is defined by those settings.)

FIGURE 181 Radio Control Options



Creating Separate WLANs for 2.4 GHz and 5 GHz Radios

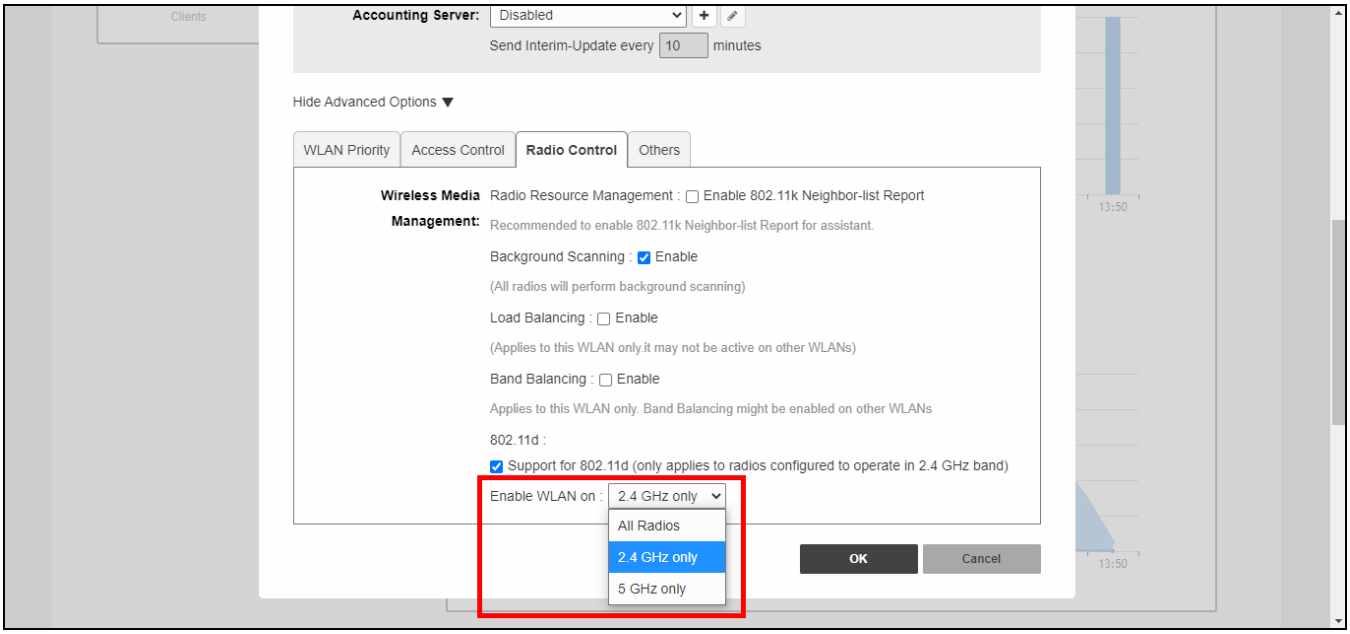
Use the "Enable WLAN on" option to configure 2.4 or 5 GHz radio service on/off for the WLAN. This allows you to create two separate WLANs that each operates on one or the other of the 2.4 or 5 GHz radios.

In some scenarios, it may be preferable to deploy a separate WLAN/SSID for each radio; one 2.4 GHz SSID and one 5 GHz SSID. In this way, you can ensure that all 2.4 GHz-only devices connect to the 2.4 GHz WLAN only, while 5 GHz-capable devices are allowed to connect to the 5 GHz WLAN.

1. Create the 2.4 GHz WLAN.
2. Go to **WiFi Networks > Create > Advanced Options > Radio Control**.
3. In **Enable WLAN on**, select **2.4 GHz only**.
4. Click **OK** to save.

5. Create the 5 GHz WLAN.
6. Go to **WiFi Networks > Create > Advanced Options > Radio Control**.
7. In **Enable WLAN on**, select **5 GHz only**.
8. Click **OK** to save.

FIGURE 182 Use the "Enable WLAN on" option to configure 2.4 or 5 GHz radio service on/off for the WLAN



9. To verify that only 2.4 GHz devices are connected to the 2.4 GHz WLAN and 5 GHz devices are connected to the 5 GHz WLAN, expand the **Clients** section and view the list of connected wireless clients. Check the *WLAN* and *Radio* columns to view connection status.

Other Advanced WLAN Settings

The **Others** tab provides the following options:

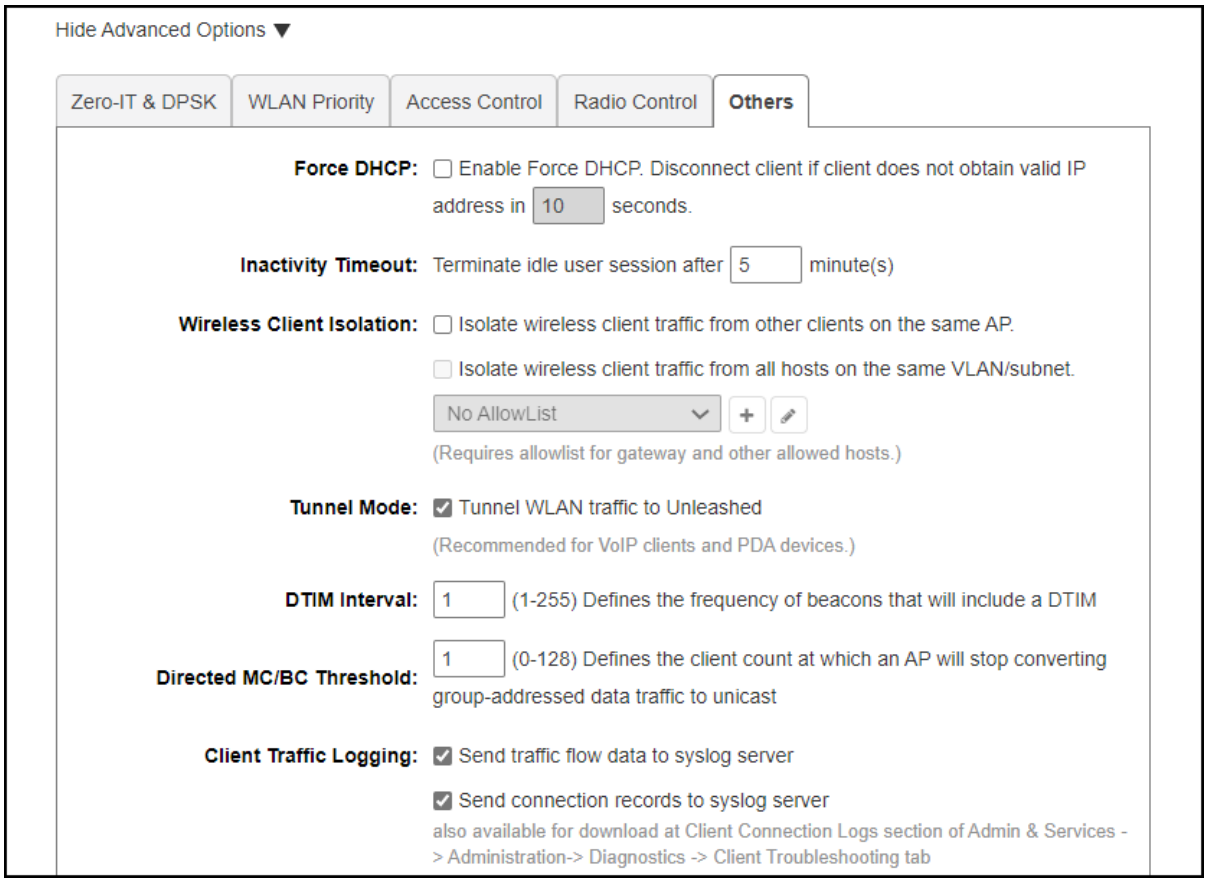
- **Force DHCP**: (Disabled by default) Enable this option to force clients to obtain a valid IP address from DHCP within the specified number of seconds, thereby preventing clients configured with a static IP address from connecting to the WLAN.
- **Inactivity Timeout**: Enter a value in minutes after which idle stations will be disconnected (from 1 through 500 minutes).
- **Wireless Client Isolation**: Select the level of client isolation you want to enforce:
  - **Isolate wireless client traffic from other clients on the same AP**: Enables client isolation on the same access point (clients on the same subnet but connected to other APs will still be able to communicate).
  - **Isolate wireless client traffic from all hosts on the same VLAN/subnet**: Prevents clients from communicating with any host on the same subnet or VLAN other than those listed on the client isolation allowlist. If this option is chosen, you must select an allowlist from the list. (Refer to Configuring Client Isolation Allowlists on page 288.)
- **Bypass Apple CNA Feature**: With Bypass Apple CNA enabled, captive portal (web-based authentication) login must be performed by opening a browser to any unauthenticated page (HTTP) to be redirected to the login page. This option is available when you select **Usage Type** as **Guest Access** or **Hotspot Service**. (Refer to Bypass Apple CNA on page 289.)

- **Tunnel Mode**: Select this check box if you want to tunnel the WLAN traffic back to the Dedicated Master. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP devices), RUCKUS recommends enabling tunnel mode.

  NOTE
  When tunnel mode is enabled on a WLAN, multicast video packets are blocked on that WLAN; however, multicast voice packets are allowed.

- **DTIM Interval**: Configure the Delivery Traffic Indication Message (DTIM) interval to control how often DTIM messages are transmitted. This setting affects the frequency of data transmissions per broadcast beacon. Setting the DTIM interval to a lower value results in more frequent DTIM messages, which can prevent mobile devices from going into power save mode and thereby increasing battery consumption.
- **Directed MC/BC Threshold**: Enter a value to set the client count at which an AP will stop converting group-addressed data traffic to unicast traffic. This setting allows RUCKUS APs to convert incoming broadcast and multicast traffic to unicast, reducing airtime utilization and improving data throughput performance.
- **Client Traffic Logging**: Configure options for log generation and delivery to the syslog server (refer to Client Connection Troubleshooting on page 361):
  - **Send traffic flow data to syslog server**: RUCKUS Unleashed sends client flow data only to the syslog server.
  - **Send connection records to syslog server**: RUCKUS Unleashed sends client connection event logs only to the syslog server.
- **Wifi6**: (Optional) (Disabled by default) Enables Wi-Fi 6.

FIGURE 183 Configuring Other Advanced WLAN Settings



Configuring Client Isolation Allowlists

When Wireless Client Isolation is enabled on a WLAN, all communication between clients and other local devices is blocked at the access point.

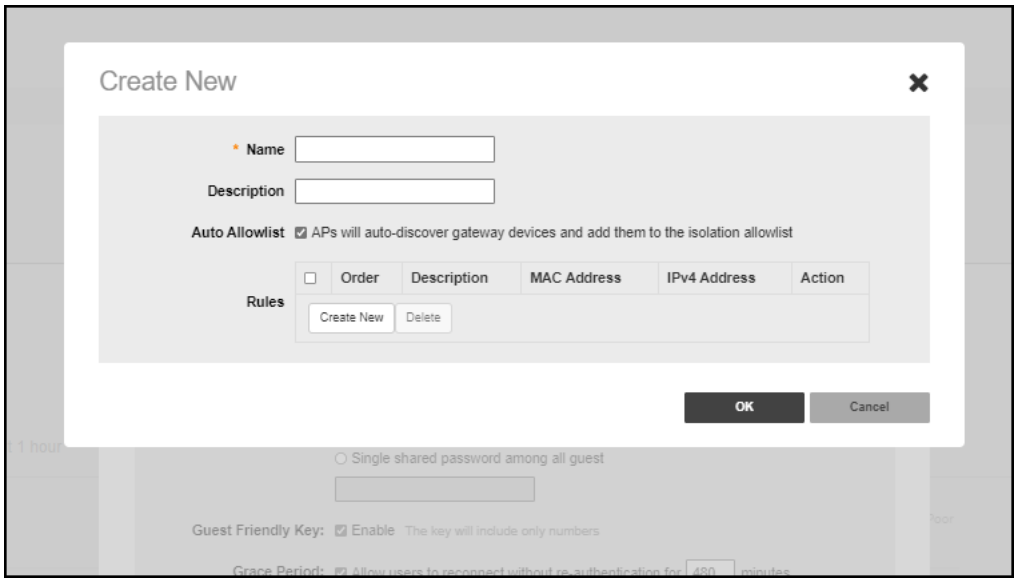
To prevent clients from communicating with other nodes, the access point drops all ARP packets from stations on the WLAN where client isolation is enabled and which are destined to IP addresses that are not part of a per-WLAN allowlist.

You can create exceptions to client isolation (for example, allowing access to a local printer) by creating client isolation allowlists.

Complete the following steps to configure a client isolation allowlist:

1. Go to **Wi-Fi Networks > Advanced Options > Others**.
2. Under **Wireless Client Isolation**, select both the options:
   - **Isolate wireless client traffic from other clients on the same AP**
   - **Isolate wireless client traffic from all hosts on the same VLAN/subnet**
3. Click **Create Allowlist**.
4. Enter a name and a description (optional) for the allowlist.
5. **Auto Allowlist** is enabled by Default, which allows the APs to auto-discover gateway devices and add them to the isolation allowlist.
6. Under **Rules**, click **Create New** to create multiple device-specific rules for each device to be allowlisted. For each rule, enter the following:
   - **Description**: Description of the device.
   - **MAC Address**: Enter the MAC address of the device.
   - **IPv4 Address**: Enter the IP address of the device.
7. Click **Save** to save the rule you created.
8. To change the order in which rules are implemented, select the order from the drop-down menu in the **Order** column. You can also edit or clone rules from the **Action** column. To delete a rule, select the check box next to the rule and click **Delete**.
9. Click **OK** to save the allowlist.

FIGURE 184 Creating a Client Isolation Allowlist



Bypass Apple CNA

Some Apple iOS and OS X clients include a feature called Captive Network Assistant (Apple CNA), which allows clients to connect to an open captive portal WLAN without displaying the login page.

When a client connects to a wireless network, the CNA feature launches a pre-browser login utility and it sends a request to a success page on the Apple website. If the success page is returned, the device assumes it has network connectivity and no action is taken. However, this login utility is not a fully functional browser, and does not support HTML, HTML5, PHP or other embedded video. In some situations, the ability to skip the login page for open WLANs is a benefit. However, for other guest or public access designs, the lack of ability to control the entire web authentication process is not desirable.

ZoneDirector provides an option to work around the Apple CNA feature if it is not desirable for your specific deployment. With CNA bypass enabled, captive portal (web-based authentication) login must be performed by opening a browser to any unauthenticated page (http) to get redirected to the login page.

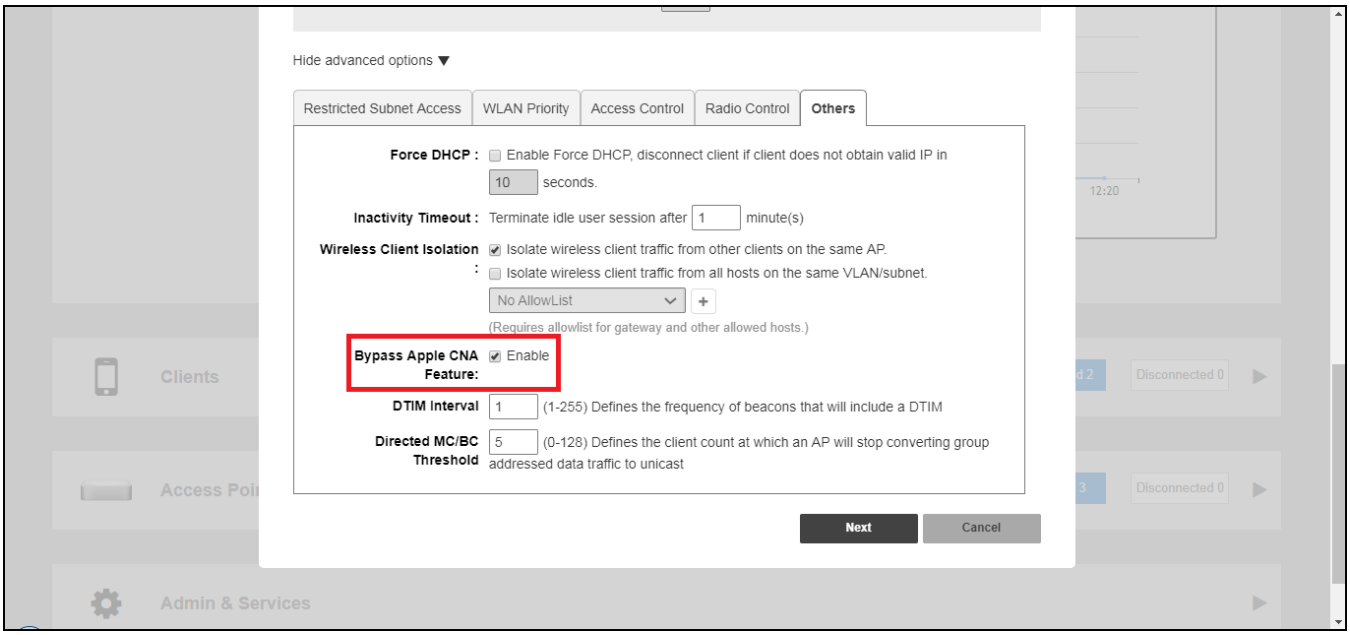
To enable Apple CNA bypass, use the following procedure:

1. Expand the **WiFi Networks** component and select the WLAN you want to configure, then click **Edit**.

   Select one of the following WLAN usage types:

   - Standard Usage with Web Auth enabled
   - Guest Access (including Social Media)
   - Hotspot (WISPr)
2. Click **Show Advanced Options**.
3. Click the **Others** tab.
4. Select the **Enable** check box next to **Bypass Apple CNA Feature**.
5. Click **OK** to save your changes.

FIGURE 185 Enable Bypass Apple CNA feature



Access Point Configuration

- Access Points Configuration Overview 291
- Show Mesh Topology 293
- Show Client Info 294
- Show Events and Alarms 296
- Configuring Global AP Settings 297
- Monitoring an Individual AP 303
- Configuring an Individual AP 310
- Working with AP Groups 314
- Restarting an AP 330
- Removing an AP 331

Access Points Configuration Overview

The **Access Points** component provides tools for monitoring and configuring all APs at once, configuring each AP individually, or configuring multiple groups of APs with a set of common custom settings.

The **Access Points** component on the dashboard presents an overview of the connected and disconnected APs that are recognized by this RUCKUS Unleashed network.

The **Access Points** component offers two display modes:

- Card display mode
- Table display mode

The **Access Points** component offers the following options:

- **Summary** AP box: Click this box to view a summary of all AP clients, signal quality, and traffic statistics.
- Individual AP boxes: Click any of these boxes to view details specific to the indicated AP.
- View mode: Switch between AP and AP Group views. AP mode lets you view and configure APs individually, while AP Group mode lets you create and manage AP groups. For more information, refer to Working with AP Groups.
- **Data Duration**: Select the duration of time interval (10 minute, 1 hour, and 12 hours) to view the client status and traffic information of the indicated WLAN.
- **Display Mode**: Switch between card and table display modes. If there are more than 20 APs or AP groups, they are displayed in table mode automatically. The display mode returns to the default (card mode) when the web interface is refreshed.

  NOTE
  You can configure 32 AP groups in Dedicated mode and 10 AP groups in local bridge mode from the web interface, CLI, and mobile app.

- **Search** field: Search AP or AP groups in card or table display mode.
- **Sort**: Sort items with **Device Name**, **Clients**, **Mac Address**, **Model**, **SN**, **Version** in AP page and **Group Name**, **APs**, **Clients**, **WLANs** in AP group name.
- **Show Mesh Topology**: Click this link to view the Mesh topology.
- **Show Clients Info**: Click this link to view a table of currently connected clients.
- **Show Events & Alarms**: Click this link to view a table of events and alarms.

- **Client Status** bar chart: This chart displays the number of connected clients and the client signal quality across all connected APs at one-minute intervals (over the last 10 minutes).
- **Traffic** graph: This graph displays the Received (Rx), Transmitted (Tx), and Total traffic values as per the time interval selected for **Data Duration**.

FIGURE 186 Access Points Component: Card Display Mode

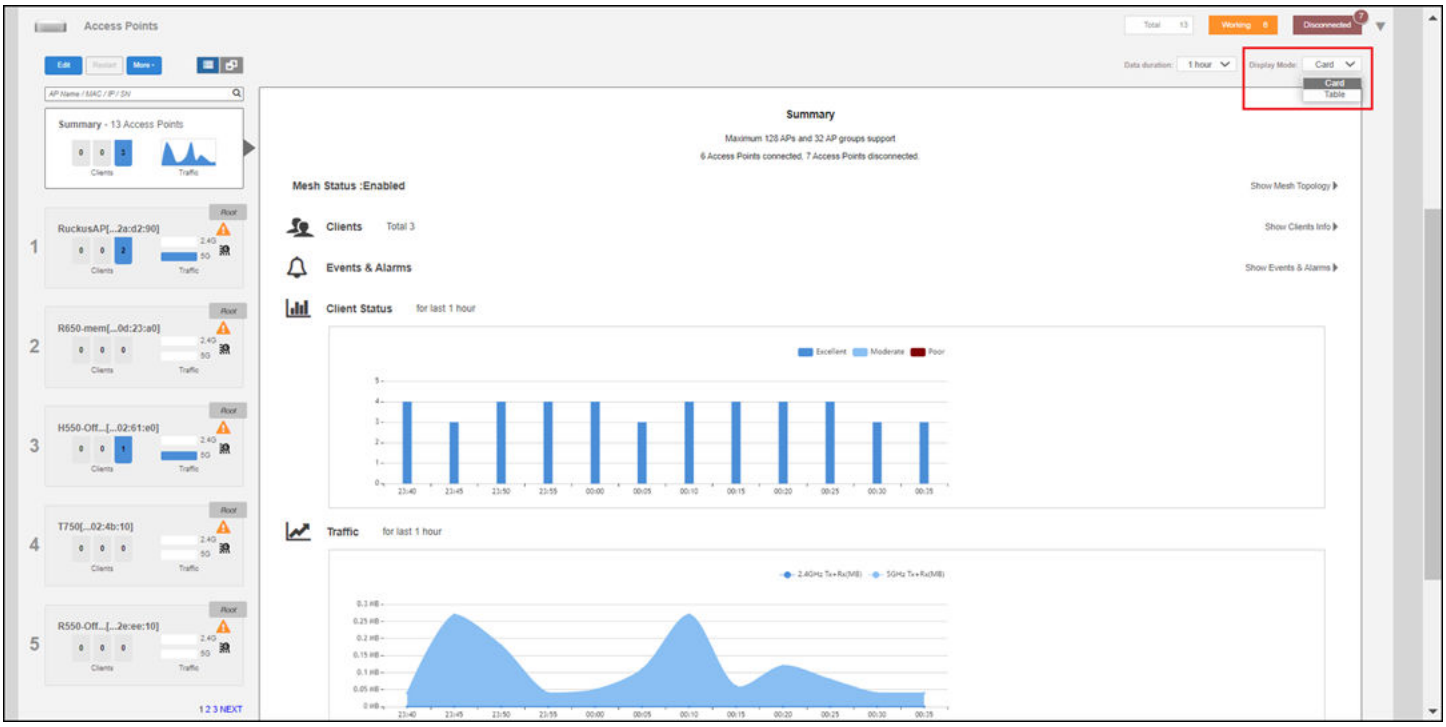
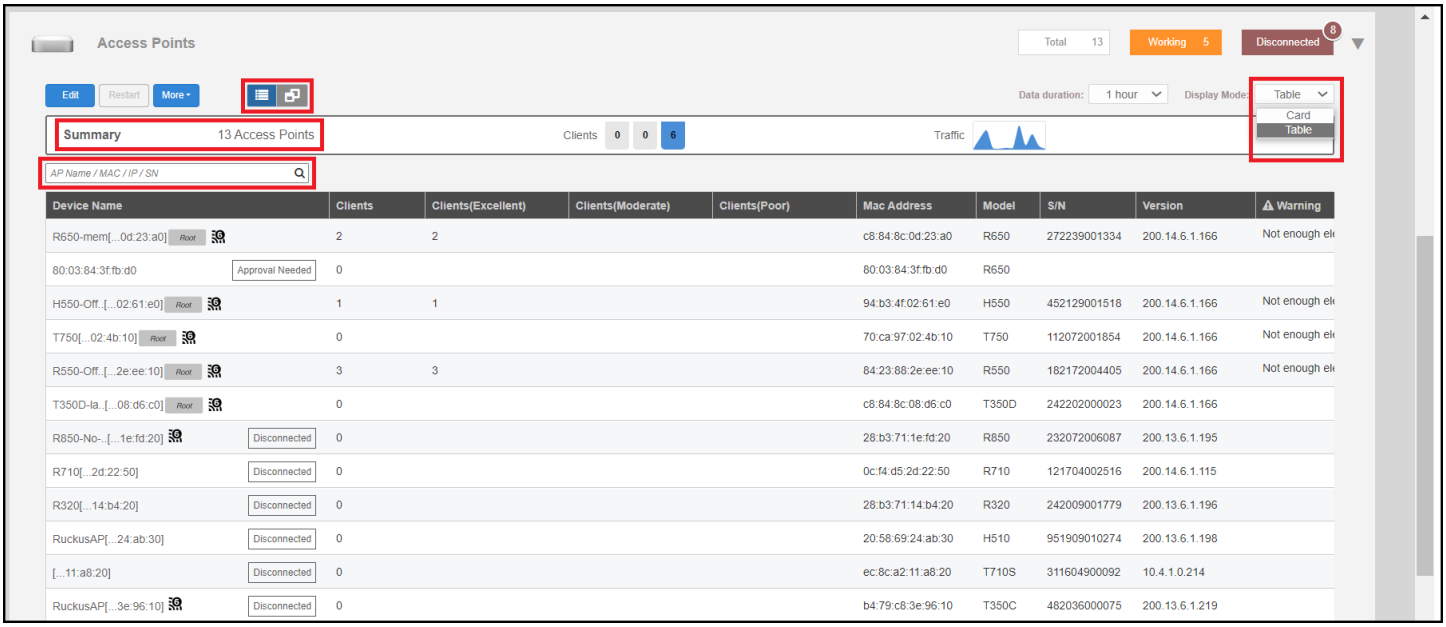


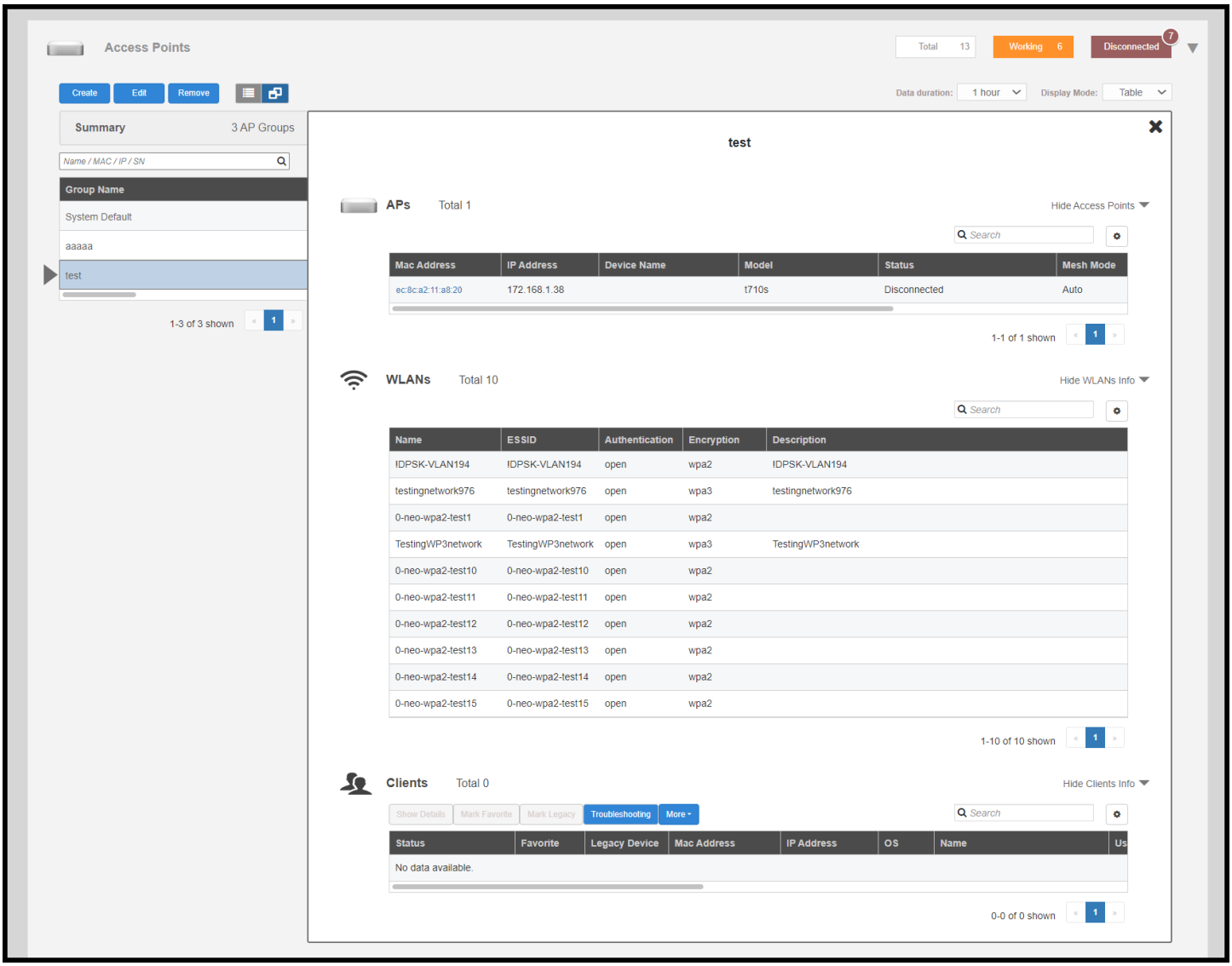
FIGURE 187 Access Points Component: Table Display Mode



You can sort the items in the table by clicking the **Device Name**, **Clients**, **Mac Address**, **Model**, **SN**, and **Version** column headings for APs, and the **Group Name**, **APs**, **Clients**, and **WLANs** column headings for AP groups.

In the table display mode and group view mode, you can click individual rows to view information about the APs, WLANs, and clients associated with the selected AP group.

FIGURE 188 Viewing Individual AP Information in Table Display Mode



Show Mesh Topology

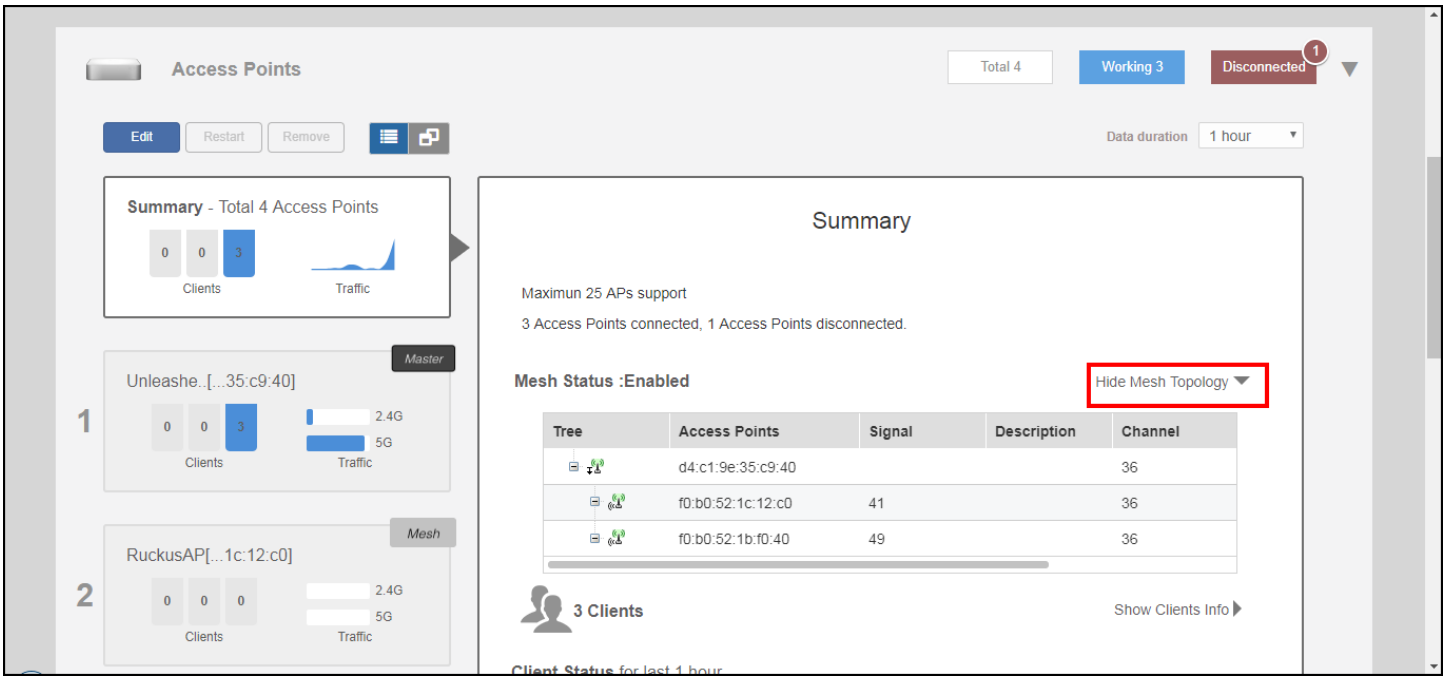
Click this link to display the Mesh topology.

The **Mesh Topology** table displays the relationships between Root APs and Mesh APs in the Mesh. The table includes the following information:

- **Access Points**: Lists the APs in the Mesh by MAC address.

- **Signal**: Displays the signal quality of the Mesh link to/from the uplink AP.
- **Description**: The AP description, if configured.
- **Channel**: Displays the channel used by the Mesh link, as well as the channel width (20/40/80).
- **IP Address**: The IP address of the Root or Mesh AP.
- **Clients**: Number of clients connected to the AP.

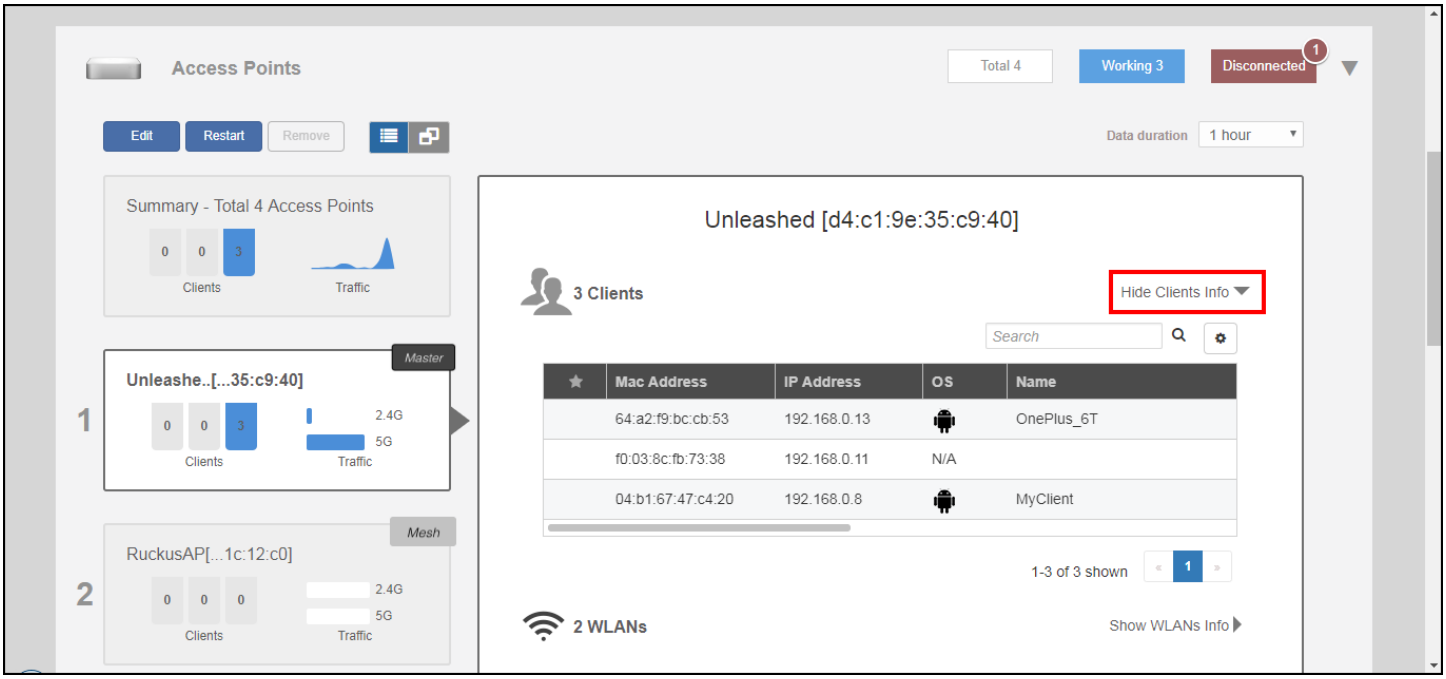
FIGURE 189 Mesh Topology



Show Client Info

Click this link to display the currently connected clients list.

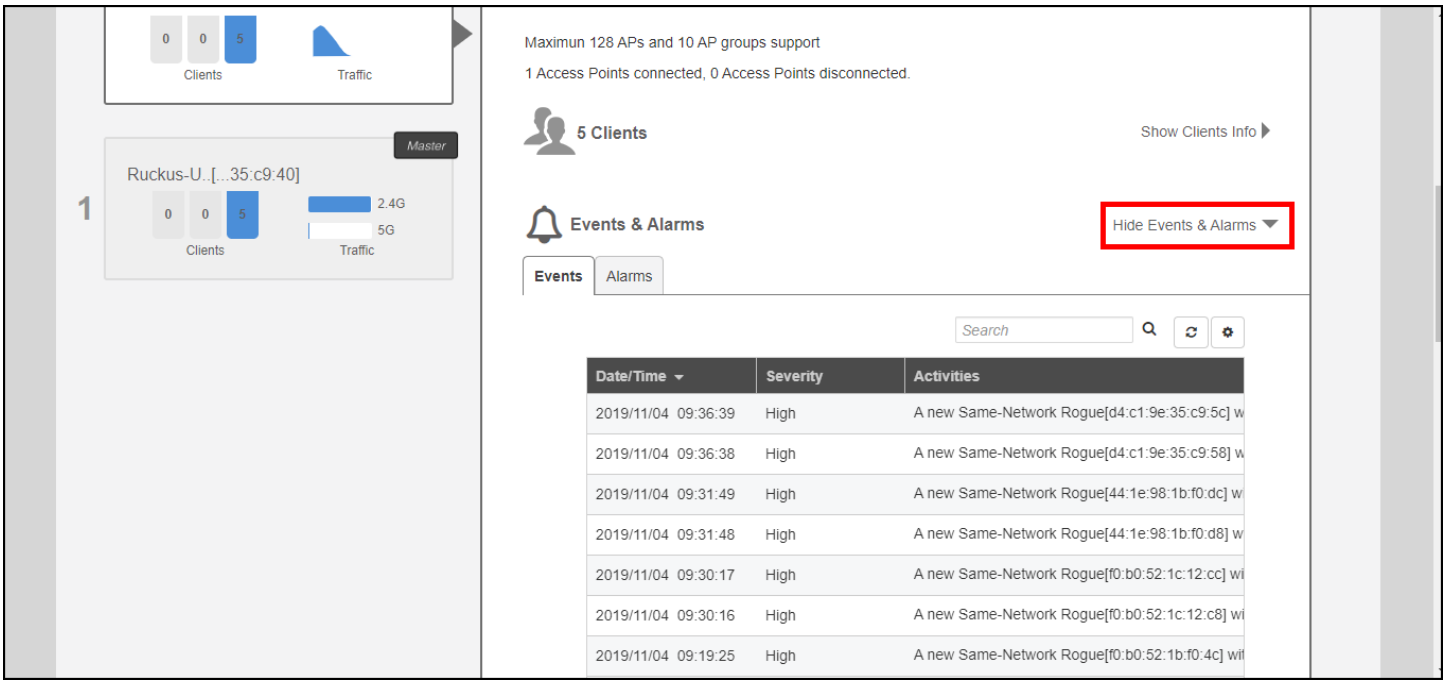
FIGURE 190 Client Info summary



Show Events and Alarms

Click this link to display a list of events and alarms for all APs or for the selected AP.

FIGURE 191 Show/hide Events & Alarms



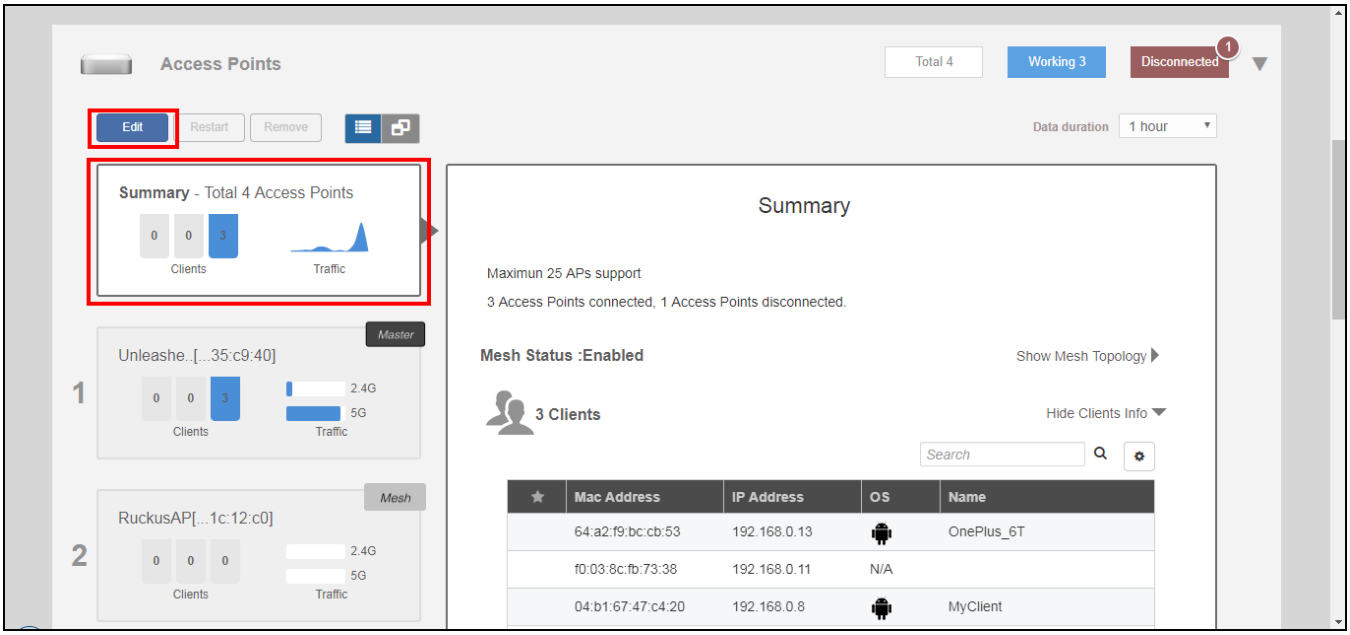
Configuring Global AP Settings

Global AP settings are applied to all members of the Unleashed network, unless overridden by AP group or individual AP settings.

To configure settings for all APs connected to the Unleashed network in the "System Default" AP group:

1. Select the **Summary** AP box, and click the **Edit** button in the **Access Points** component.

   FIGURE 192 Click Edit to configure AP global settings



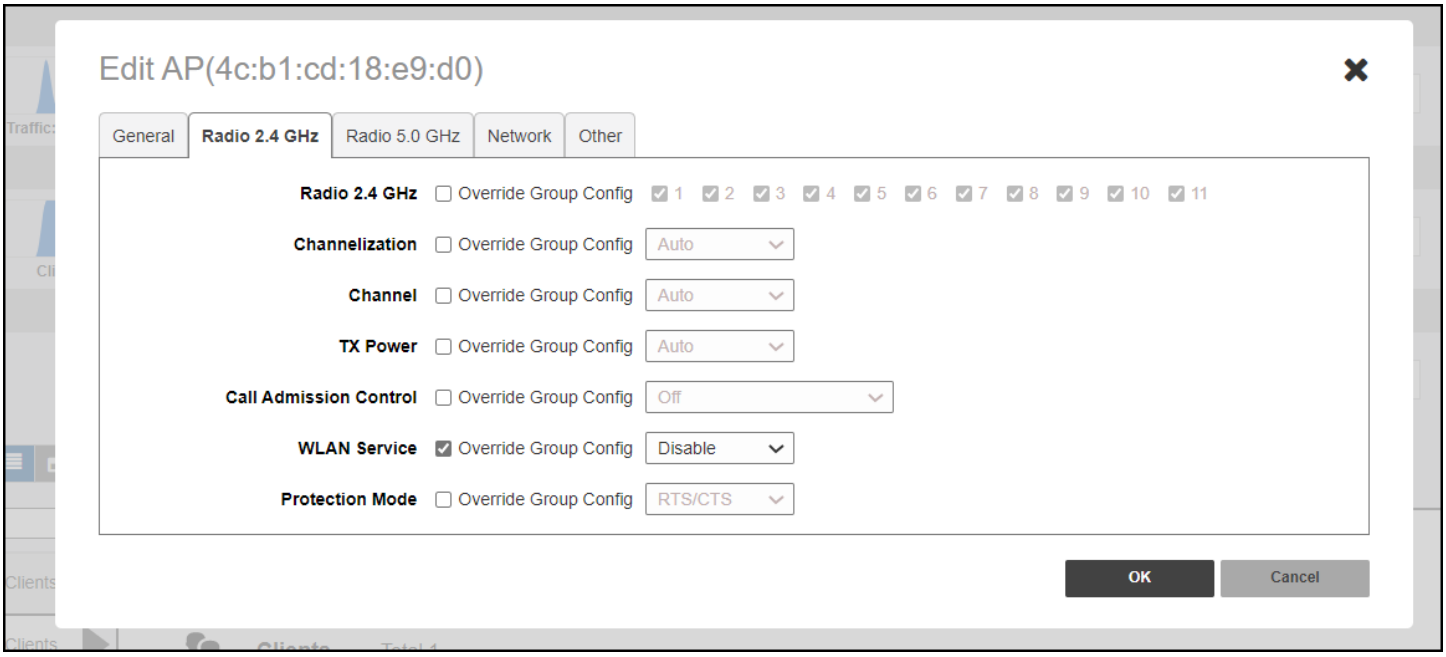
2. Configure the following global AP settings according to your preferences:
   - **Radio (2.4G)**: Configure options for the 2.4 GHz radio on all Unleashed APs.
   - **Radio (5G)**: Configure options for the 5 GHz radio on all Unleashed APs.
   - **Other**: Configure Model-Specific controls including Max Clients by AP model, and whether to disable status LEDs.
3. Click **OK** to save your changes.

Radio (2.4G)

You can select or clear channels from which to choose during the automatic channel selection process or select a specific channel on which to operate, or enable **Call Admission Control** or **Spectralink Compatibility** for this radio.

Additionally, you can disable WLAN service for this radio entirely.

FIGURE 193 System Default AP Group: 2.4 GHz Radio Configuration

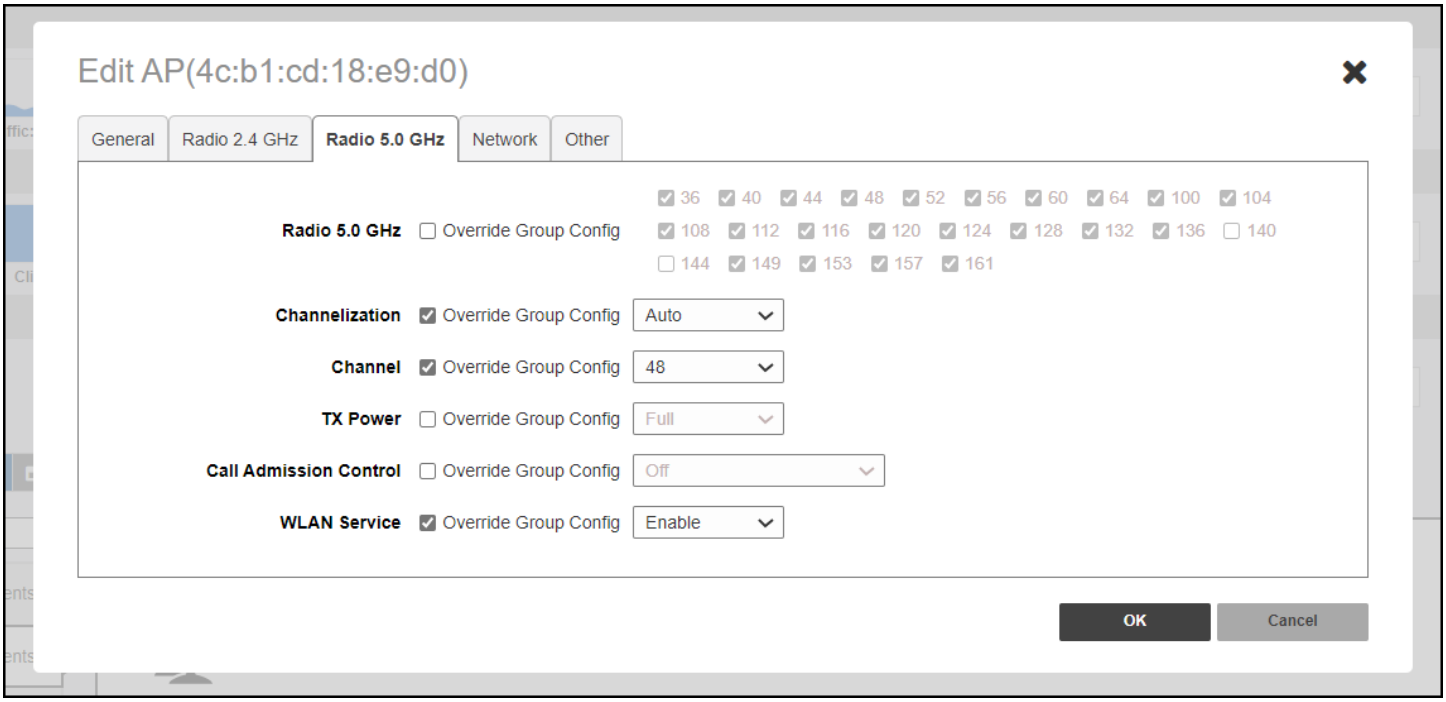


Radio (5G)

You can select or clear channels from which to choose during the automatic channel selection process or select a specific channel on which to operate, or enable **Call Admission Control** or **Spectralink Compatibility** for this radio.

Additionally, you can disable WLAN service for this radio entirely.

FIGURE 194 System Default AP Group: 5 GHz Radio Configuration

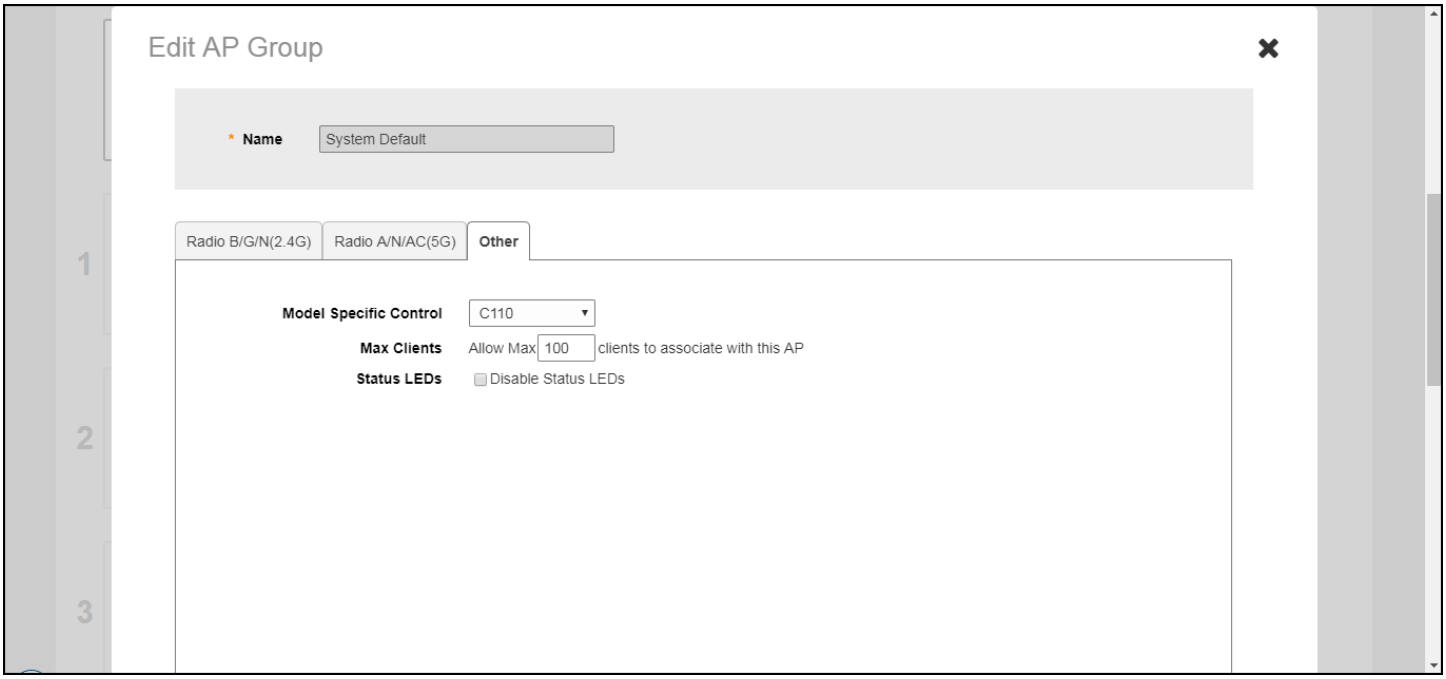


Other

The **Access Points > Summary > Edit > Other** page provides the following options:

- **Preferred Master**: Select a specific AP to be the Master AP and, if the preferred Master AP reboots, it will resume the role of Master AP again once it rejoins the Unleashed network. By default, there is no preference as to which AP should become the Master AP; the first AP that is deployed automatically becomes the Master AP. Using the Preferred Master setting, users can configure one AP to have priority. Any (non-mesh) AP can become the Master if the preferred Master is offline, but when the Preferred Master comes back online, it will assume the Master role again.
- **Model Specific Control**: Select which AP model to configure from the drop-down list. The options below can be configured independently for each Unleashed AP model. See Modifying Model Specific Controls on page 300.

FIGURE 195 Configuring other AP settings



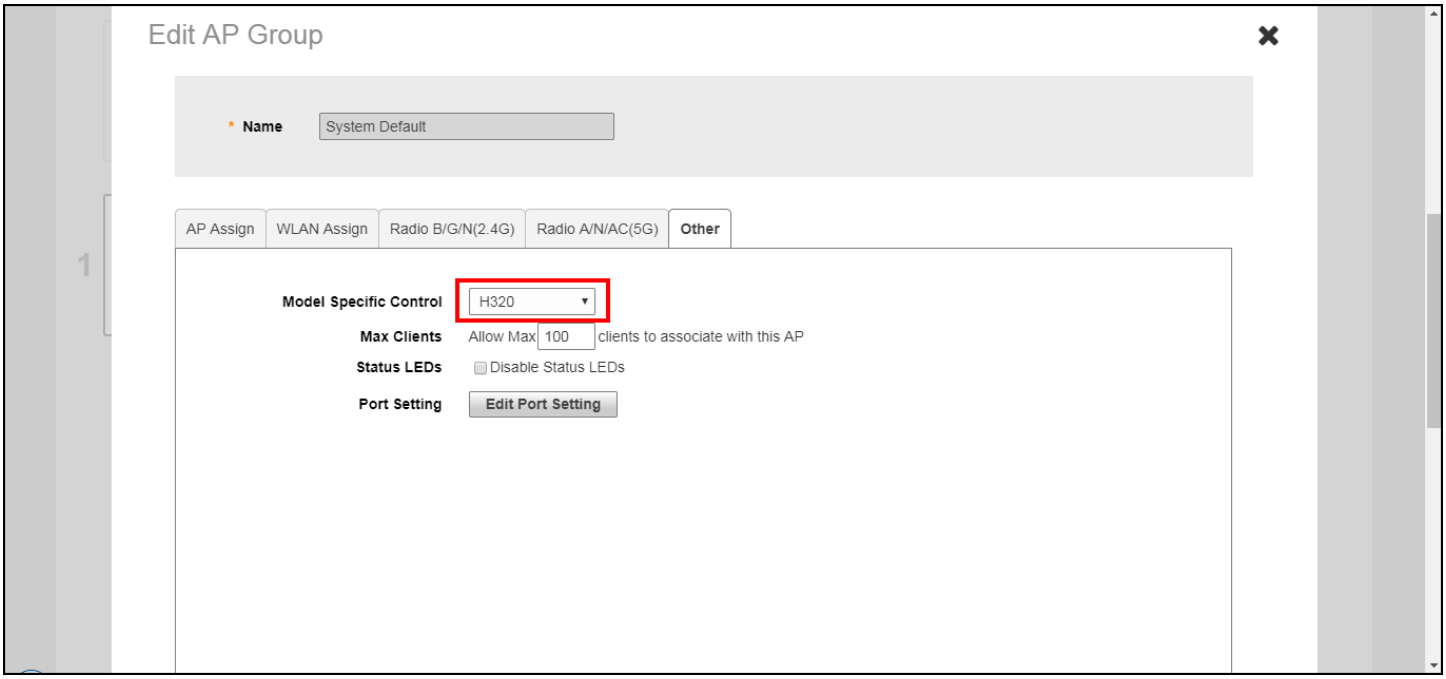
Modifying Model Specific Controls

The following settings can be applied to all APs of a particular model that are members of the AP group:

Some options are available for specific AP models only.

To configure model-specific settings for the AP group, select the AP model from the **Model Specific Control** list.

FIGURE 196 Model Specific Controls

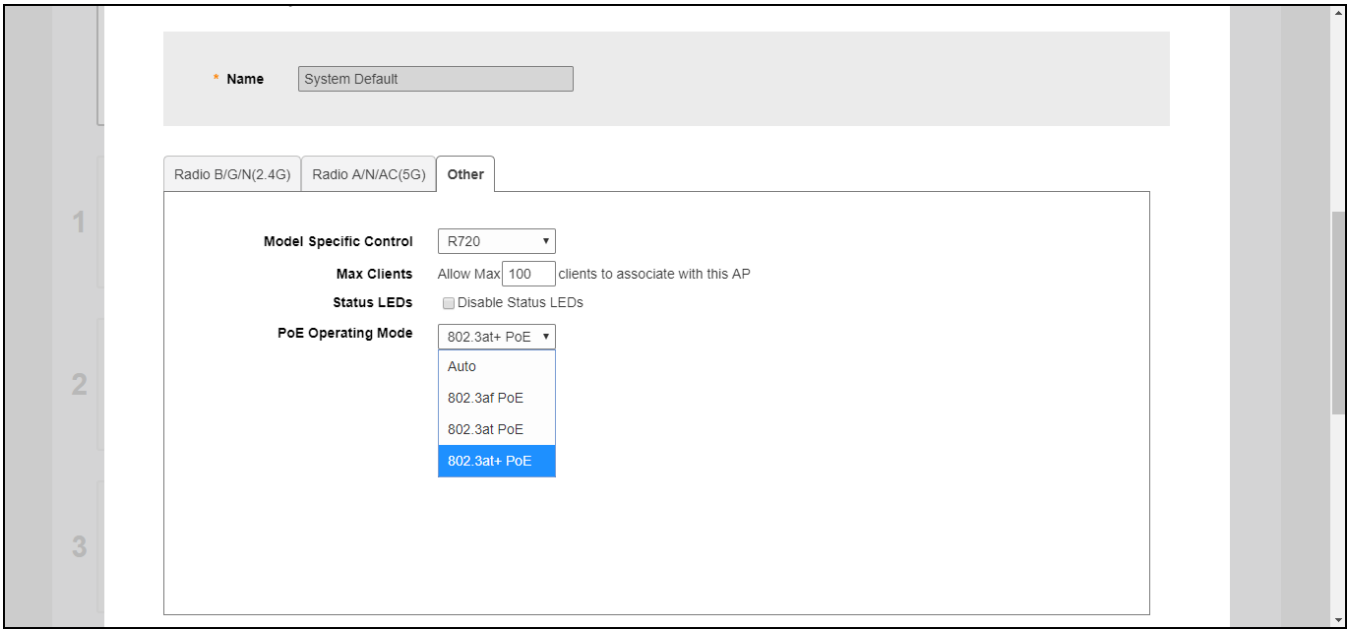


Configure any of the following settings for each model independently, and click **Finish** to save your changes:

- **Max Clients**: Set the maximum number of clients that can associate per AP. Note that different AP models have different maximum client limitations.
- **PoE Out Ports**: Enable PoE out ports (specific AP models only).
- **Status LEDs**: Disable the external LEDs on certain AP models. This can be useful if your APs are installed in a public location and you don't want to draw attention to them.
- **External Antenna**: On APs with external antenna options, select Enable for the external antenna to be enabled. When enabled, enter a gain value in the range of 0 to 90 dBi. Default is 3 dBi.
- **Port Settings**: Refer to Configuring AP Ethernet Ports on page 324 for more information on configuring AP-specific Ethernet port settings.
- **PoE Operating Mode**: Select PoE operating mode, Auto, 802.3af or 802.3at PoE (specific AP models only). Default is *Auto*. If 802.3af PoE is selected, the AP will operate in 802.3af mode (not 802.3at mode), and will consume less power than in 802.3at mode. However, when this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports.

  NOTE
  On some APs, an additional mode - 802.3at+ PoE - is available. This mode enables all features on the AP but requires an Ethernet switch that supports the 802.3at+ standard due to the higher power draw from the port to which the AP is connected. For a list of PoE operating modes by AP model, refer to Unleashed Access Point Power Supply Considerations on page 501.

FIGURE 197 PoE Operating Mode



Disabling Access Point LEDs

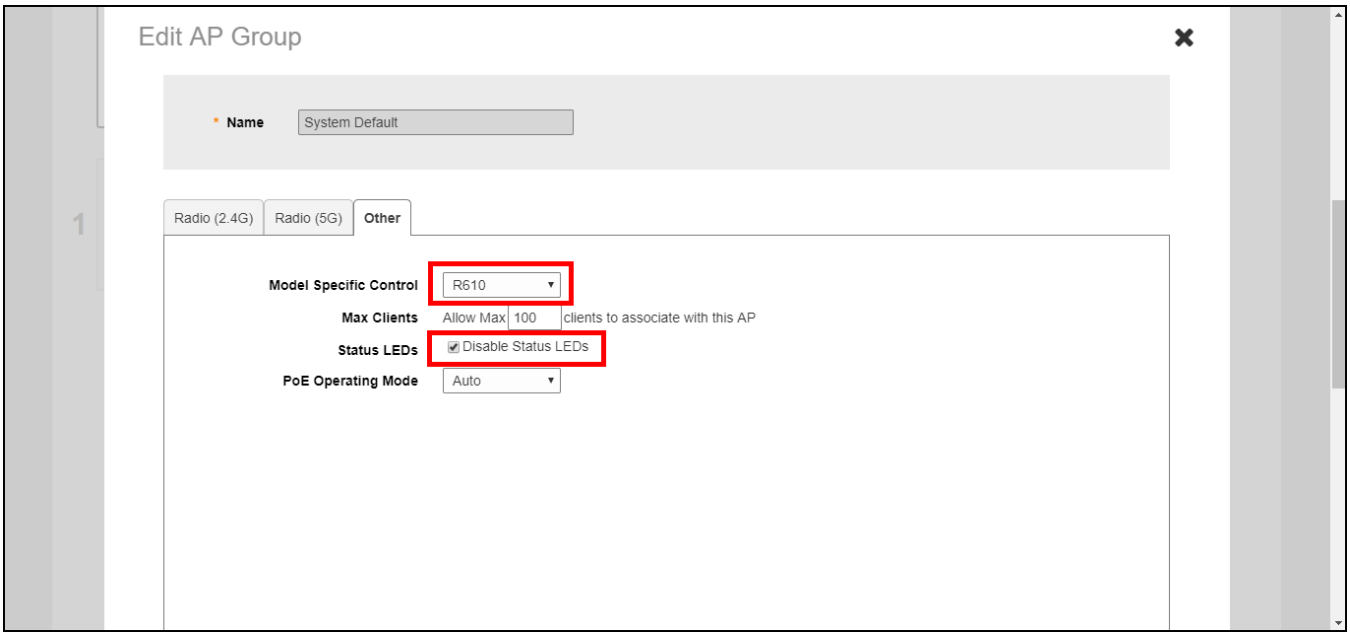
In some situations, customers may wish to disable the LED lights on the access points to avoid drawing attention to them, when installed in a public location, for example.

To disable status LEDs on all APs of a specific model:

1. Go to **Access Points > Summary > Edit > Other**.
2. Select the AP model from the list and enable the option **Disable Status LEDs**. The setting must be configured for each AP model individually.

3. Click **Finish** to save your changes.

FIGURE 198 Select model and enable the option "Disable Status LEDs"

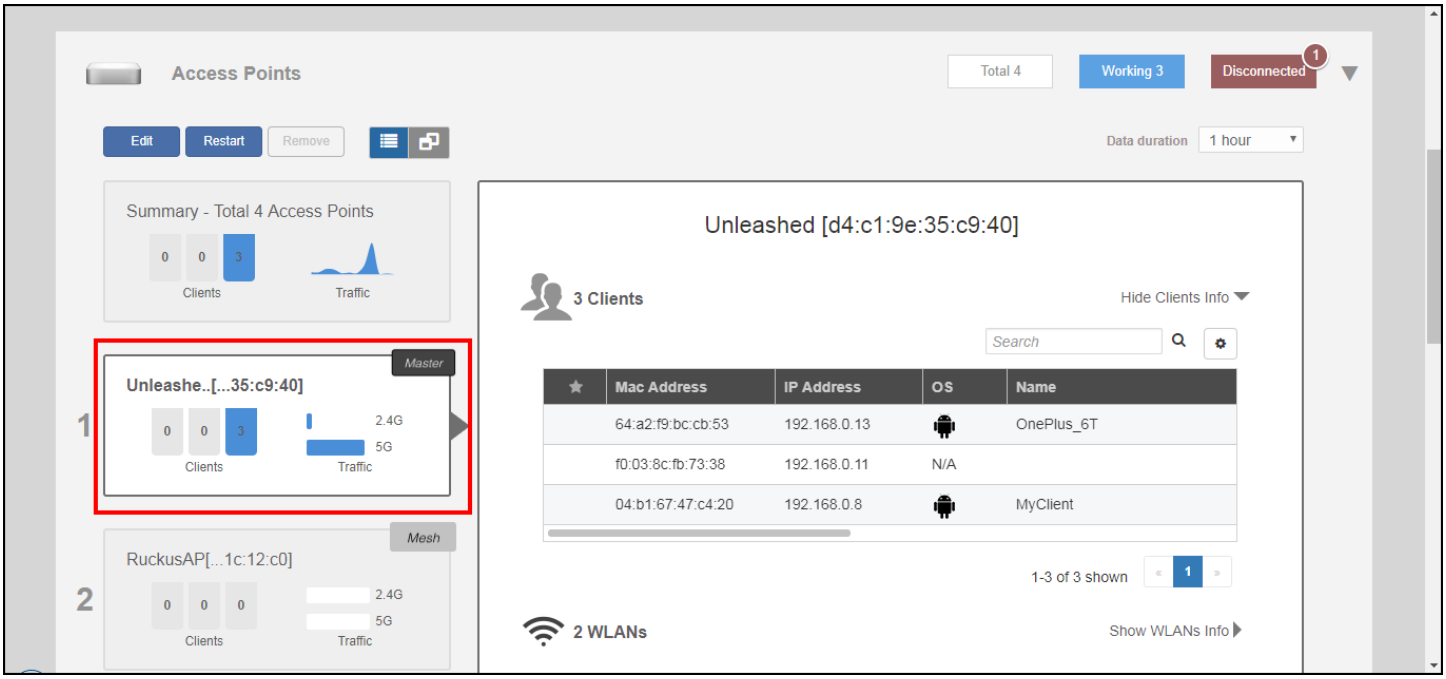


Monitoring an Individual AP

Click one of the AP boxes in the Access Points component to monitor and configure that specific AP individually.

You can edit, restart, or remove an AP from the network from the individual AP monitoring page. The individual AP monitoring page also includes graphs displaying signal quality and traffic statistics, and links to more detailed information on the AP and its connected clients.

FIGURE 199 Viewing Individual APs



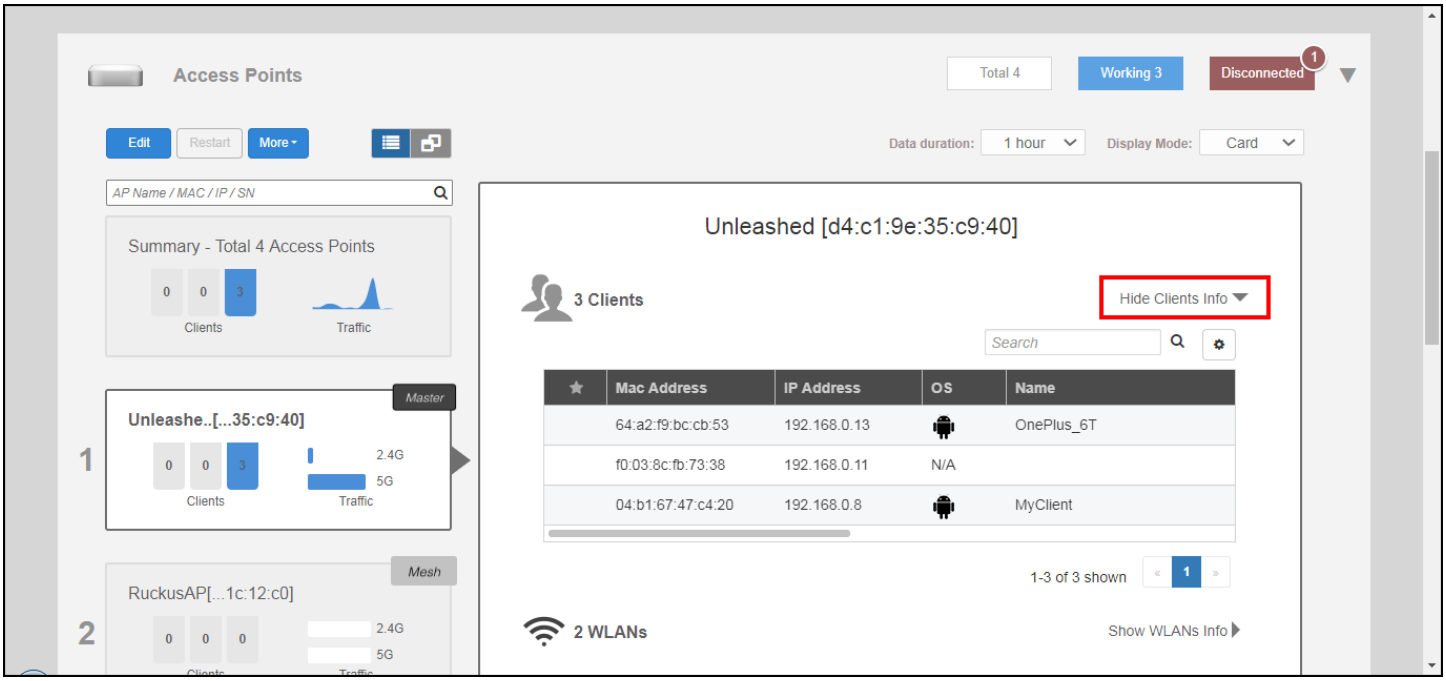
The individual AP monitoring screen contains the following elements:

- **Edit**: Click this button to configure an AP individually.
- **Restart**: Click this button to restart the AP.
- **Approve**: If auto-approval is disabled, click this button to approve the AP and allow it to join the network.
- **Remove**: Click this button to remove this AP from the network.
- **Show Clients Info**: Click this link to display a list of clients currently connected to the AP. Details for each client include MAC address, IP address, OS, Host Name, MAC address of the AP to which the client is currently connected, WLAN name, Signal Strength indicator, Auth status, and duration online.
- **Show AP Info**: Click this link to display AP-specific information including MAC address, IP address, external IP and port number, model name, serial number, and firmware version.
- **Client Status**: Displays a breakdown of client numbers by signal quality (Excellent, Moderate, or Poor) over time, in one-minute intervals.
- **Traffic**: Displays the total traffic (Tx + Rx) on the AP radio in one-minute intervals.

Show Client Info

Click the **Show Client Info** link to display a list of clients connected to this AP.

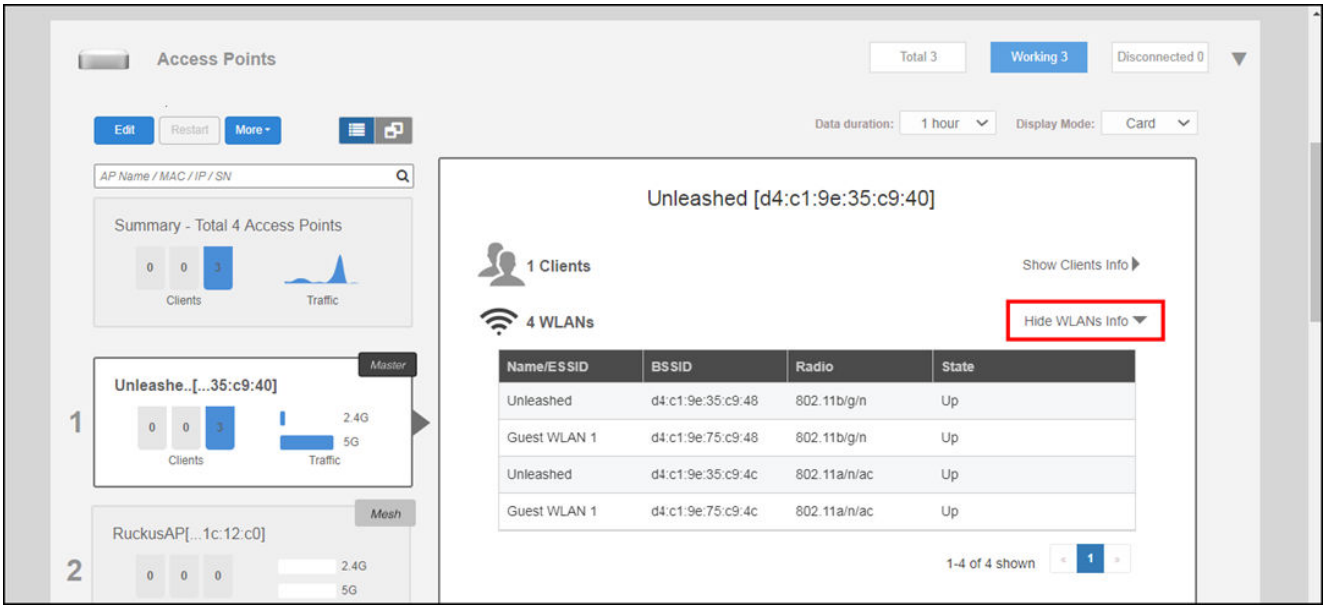
FIGURE 200 Show Client Info from AP page



Show WLANs Info

Click **Show WLANs Info** to display the list of WLANs that are currently deployed on this AP. The list displays the WLAN name (ESSID), BSSID (MAC address), radio, and state (up or down).

FIGURE 201 Showing WLAN Information for an Individual AP



Show AP Info

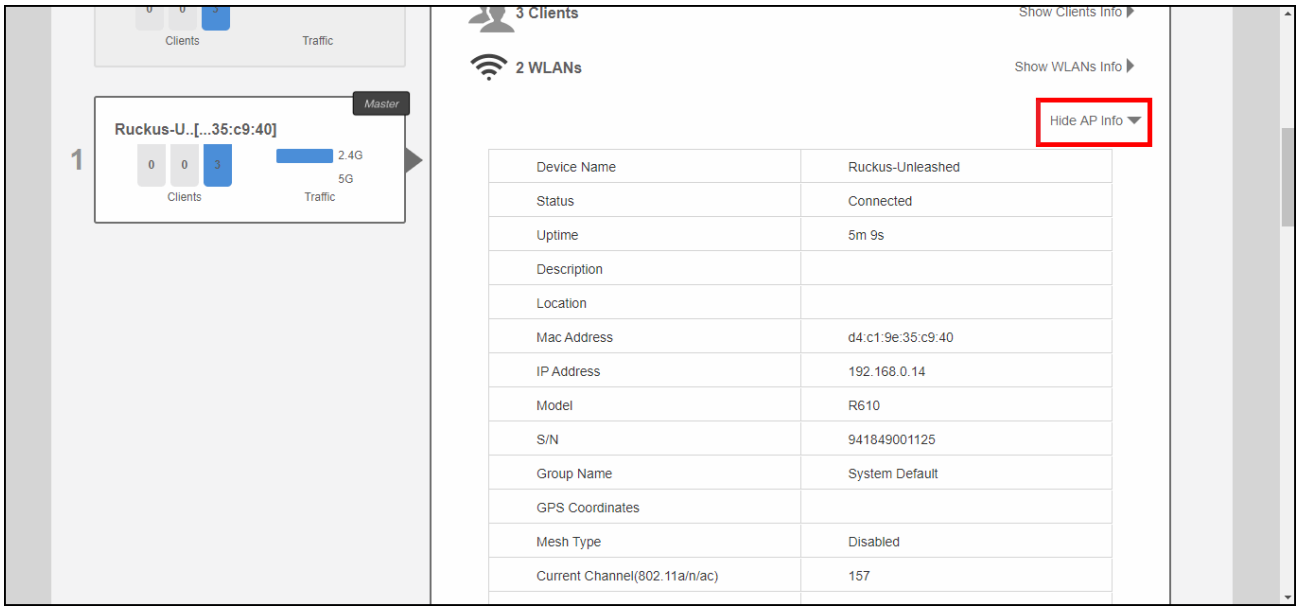
Click **Show AP Info** to display detailed information on this AP. The AP info page displays general information about the AP, including the radio channels in use, Mesh type, maximum number of clients, and firmware version. The **Save Logs** and **Speed Test** buttons are also available.

Click **Save Logs** to generate a log file (.txt) that can be useful for troubleshooting. Click **Speed Test** to measure the connection performance of the AP.

NOTE
Speed Test option is displayed for member APs only.

NOTE
The maximum number of clients (**Max Clients**) displayed for the Master AP may be lower than the configured maximum because the Master must perform additional tasks other than serving clients. The Master AP maximum client load varies by AP model. These limits apply only to the current Master AP. All other member APs honor the maximum number of clients set from the global AP model-specific controls page (**Access Points > Summary > Edit > Others > Max Clients**) .

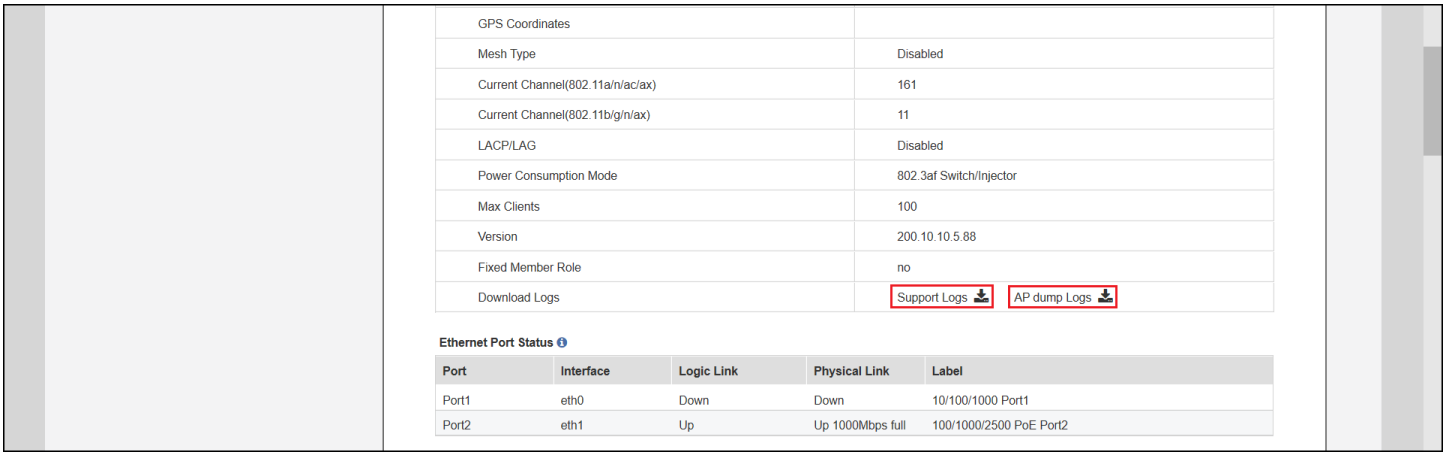
FIGURE 202 Showing AP Information for an Individual AP



For **Download Logs**, you can click **Support Logs** to save AP support log as a .txt file, and click **AP Dump Logs** to save the AP dump log as a .tar file on your computer.

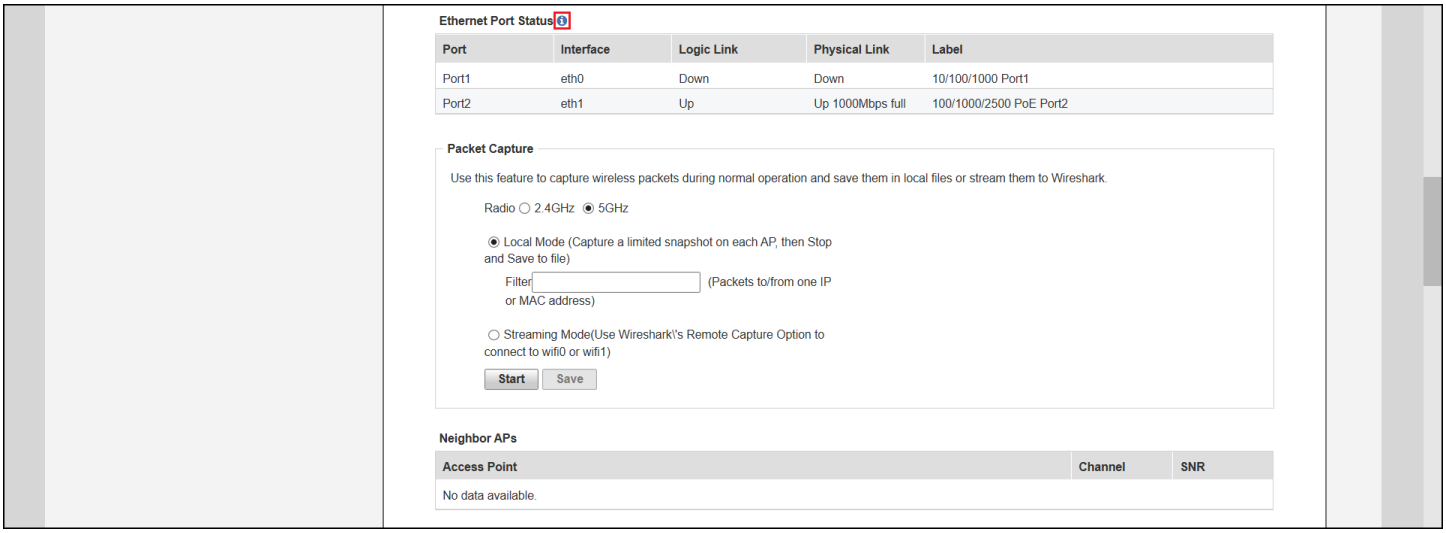
NOTE
AP Dump Logs and Download buttons are displayed only when an AP reboots unexpectedly.

FIGURE 203 Download Logs



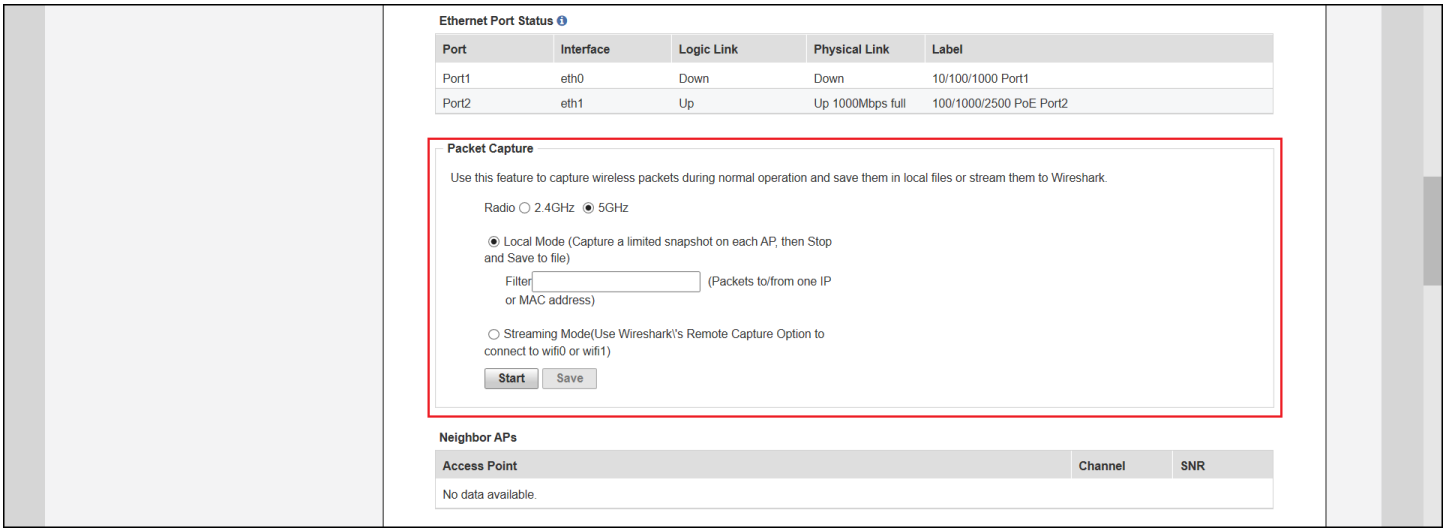
The table under **Ethernet Port Status** displays the current link status of the Ethernet ports on the AP. Hover over the "i" icon to display an illustration of the physical port locations on the AP.

FIGURE 204 Ethernet Port Status



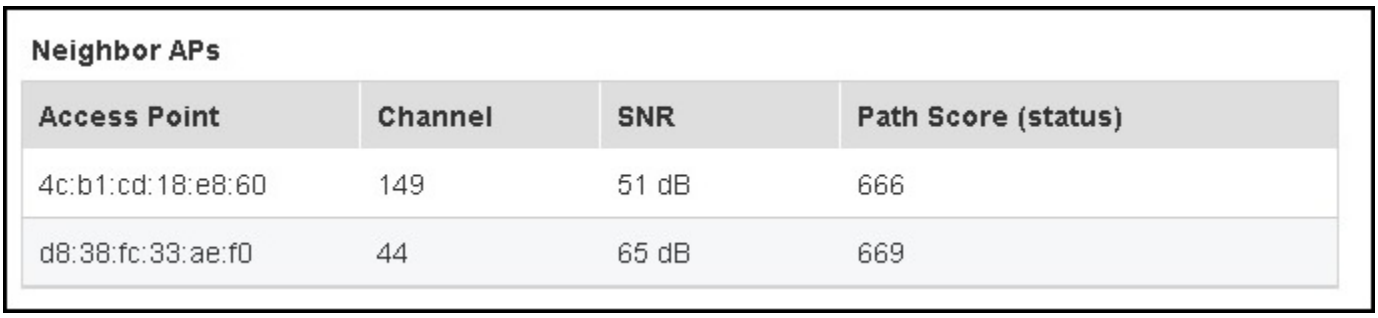
The *Packet Capture* section displays radio channels and capture modes. For more information, refer to Capturing Remote Packets on page 481.

FIGURE 205 Packet Capture



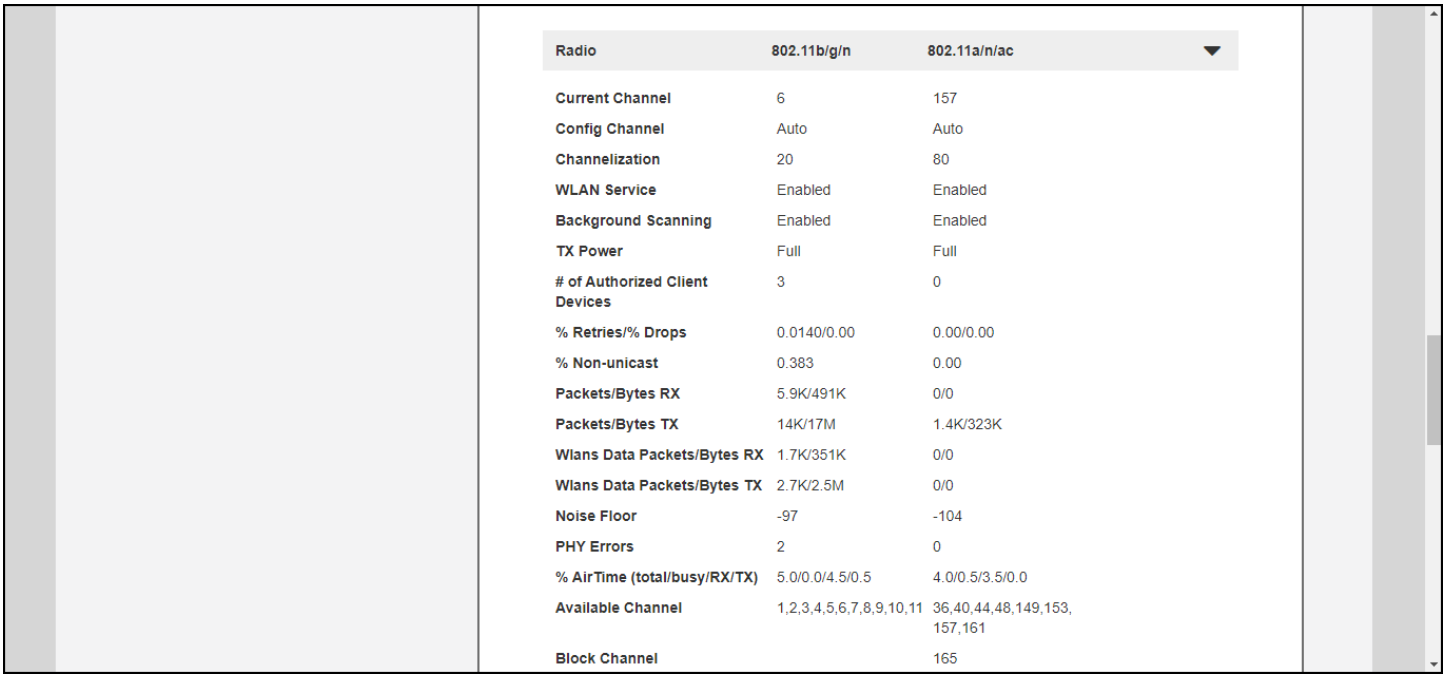
The *Neighbor APs* section displays channel, path score, and SNR of nearby APs.

FIGURE 206 Neighbor APs



The *Radio information* section provides channel and transmission details on the AP's 2.4 GHz and 5 GHz radios.

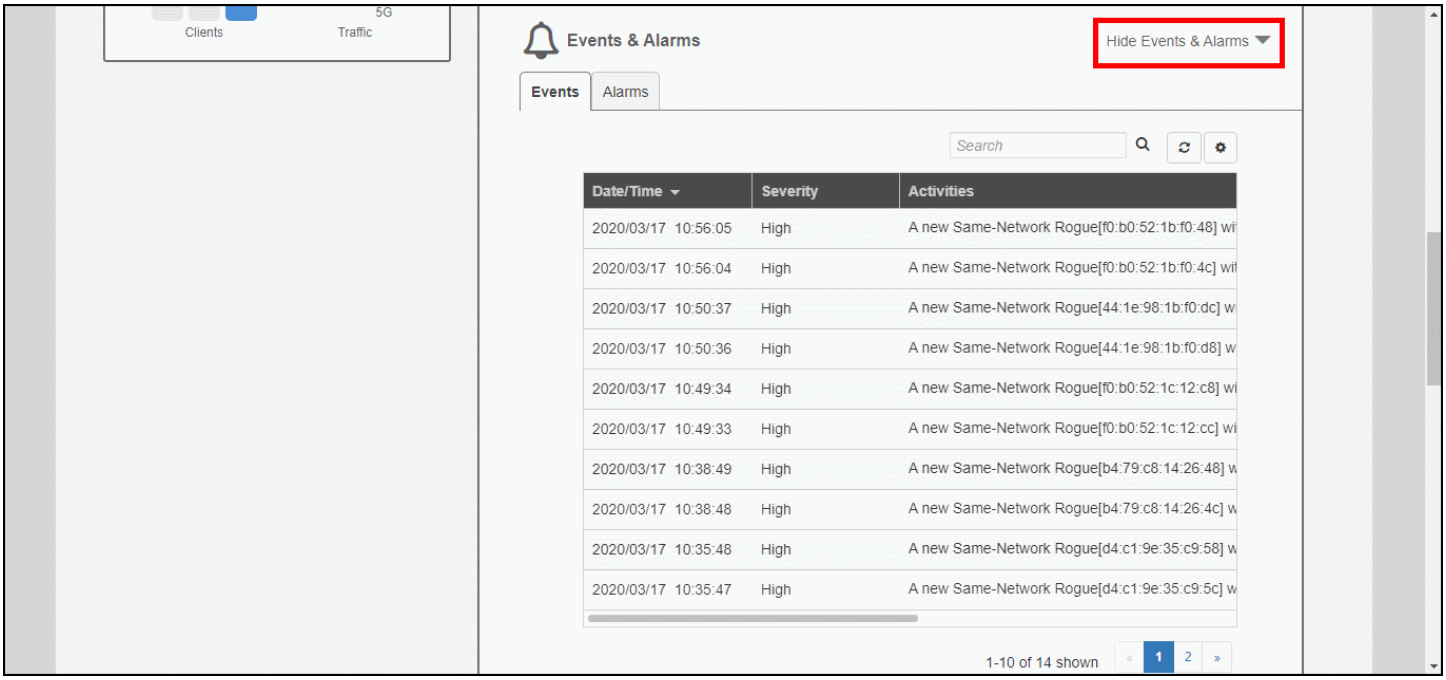
FIGURE 207 Radio information



Show Events and Alarms

Click **Show Events and Alarms** to view lists of event and alarm messages for this AP.

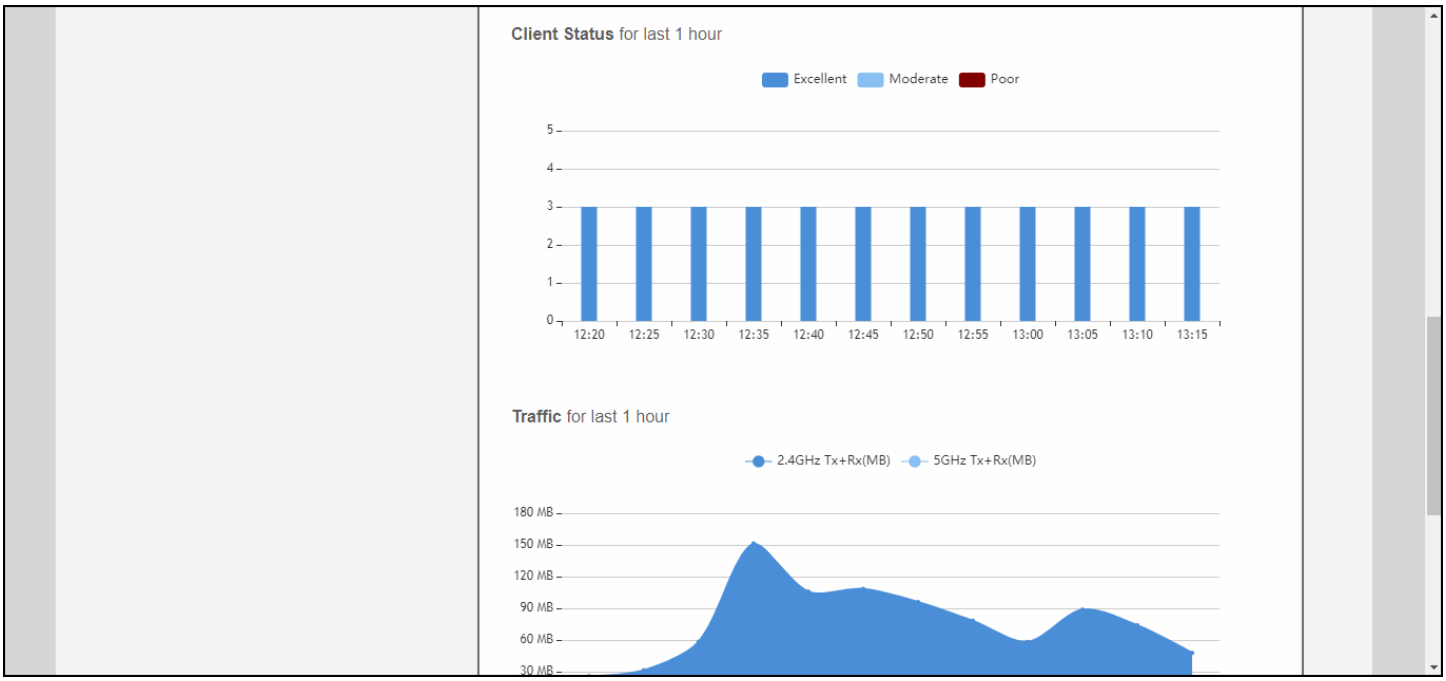
FIGURE 208 Show AP-specific Events & Alarms



Client Status and Traffic Graphs

The Client Status and Traffic graphs provide a graphical display of the number and signal quality of connected clients and transmit/receive traffic over the last hour.

FIGURE 209 Client status and traffic graphs



Configuring an Individual AP

To configure a specific AP, from the dashboard, **Access Points**, click the AP you want to configure, and click **Edit**.

FIGURE 210 Configuring an AP

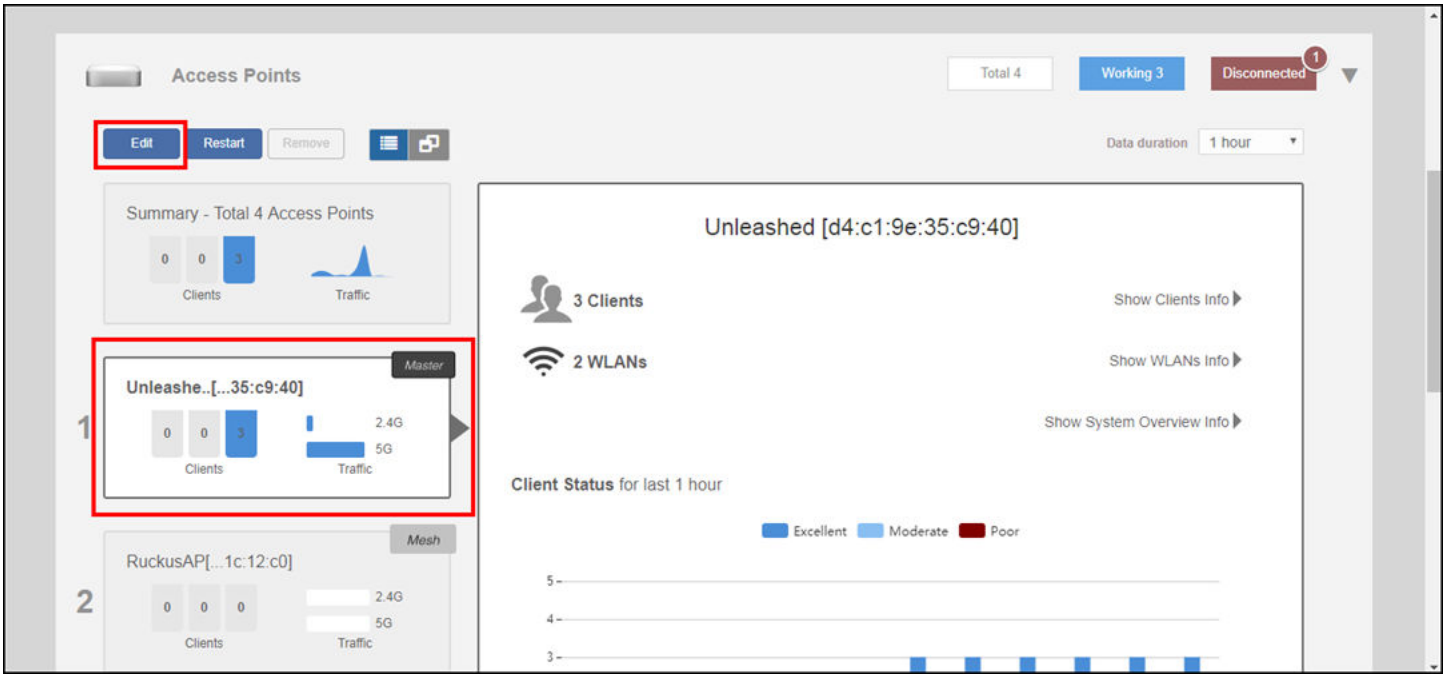
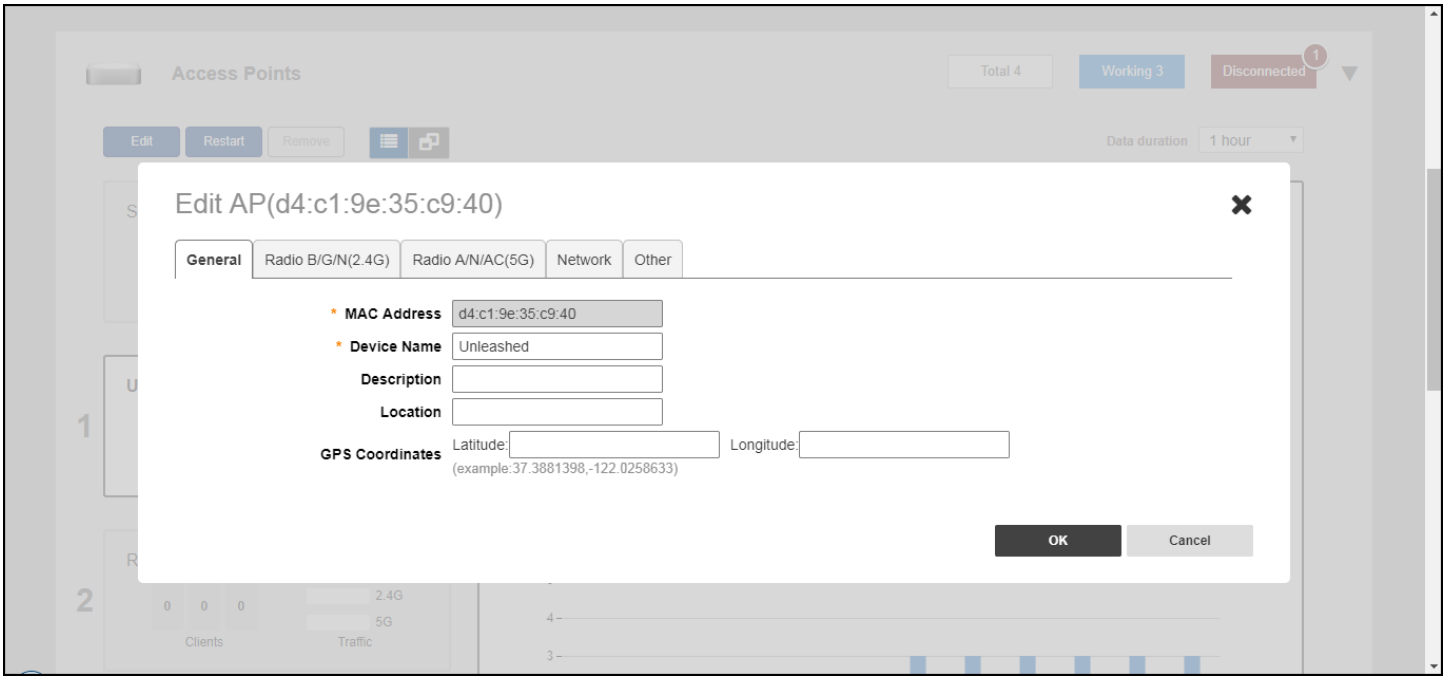


FIGURE 211 Editing an AP's Configuration Settings



In general, the settings available on the **Edit AP** page for an individual AP are the same as those for global AP settings (refer to Configuring Global AP Settings on page 297). Configuring these settings for an individual AP overrides the global AP settings.

However, some settings are only configurable on a per-AP basis, as follows:

- **General**: Configure the device name of the AP, the description, location, and GPS coordinates.
- **Radio B/G/N (2.4G)**: Enable or disable WLAN service for this radio.
- **Radio A/N/AC (5G)**: Enable or disable WLAN service for this radio.

  NOTE
  For the country code "US", 11ax and 11ac APs support channel 144. For the country codes "UK" and "JP", only 11ax APs support channel 144.

- **Network**: Configure a manual (static) IP address, or allow the AP to obtain an IP address using DHCP.

  NOTE
  You cannot configure the IP address settings for the current Master AP from the **Network** tab. You must go to **Admin & Services > System > IP Settings** to change the IP settings of the Master AP.

- **Other**: Designate this AP to serve as a Bonjour Gateway AP (refer to Bonjour Gateway on page 425), enable or disable the status LEDs of the AP, or override the PoE operating mode settings of the AP group, and configure a specific PoE power mode for this AP.

FIGURE 212 Configuring an AP with a Static IP Address from the AP's Edit > Network tab

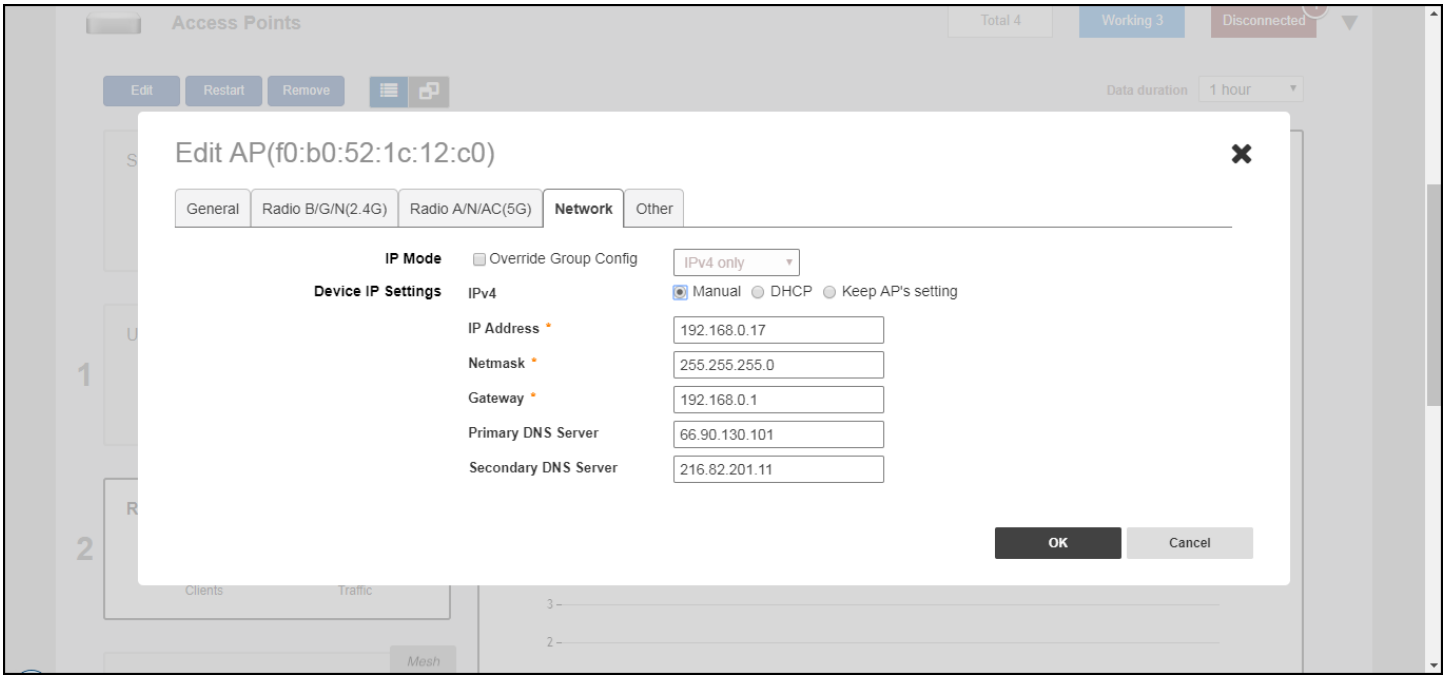
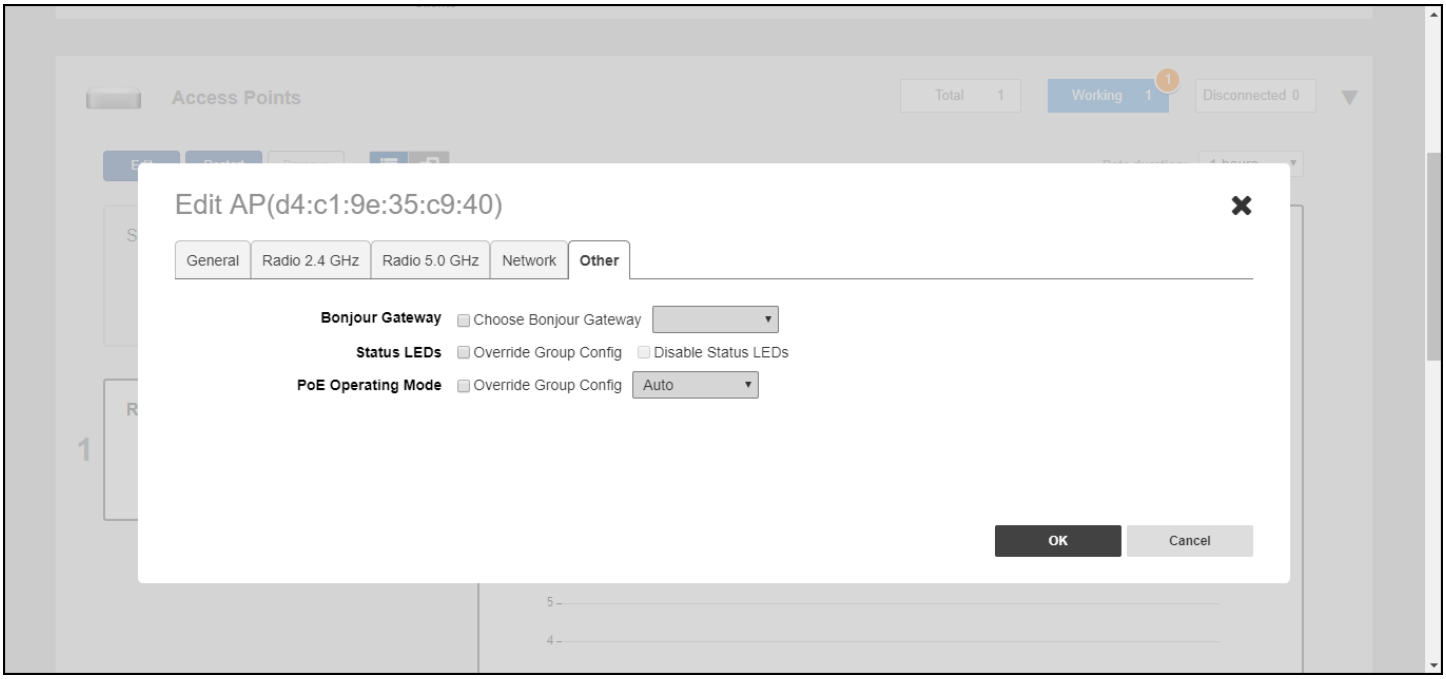


FIGURE 213 Other AP Settings

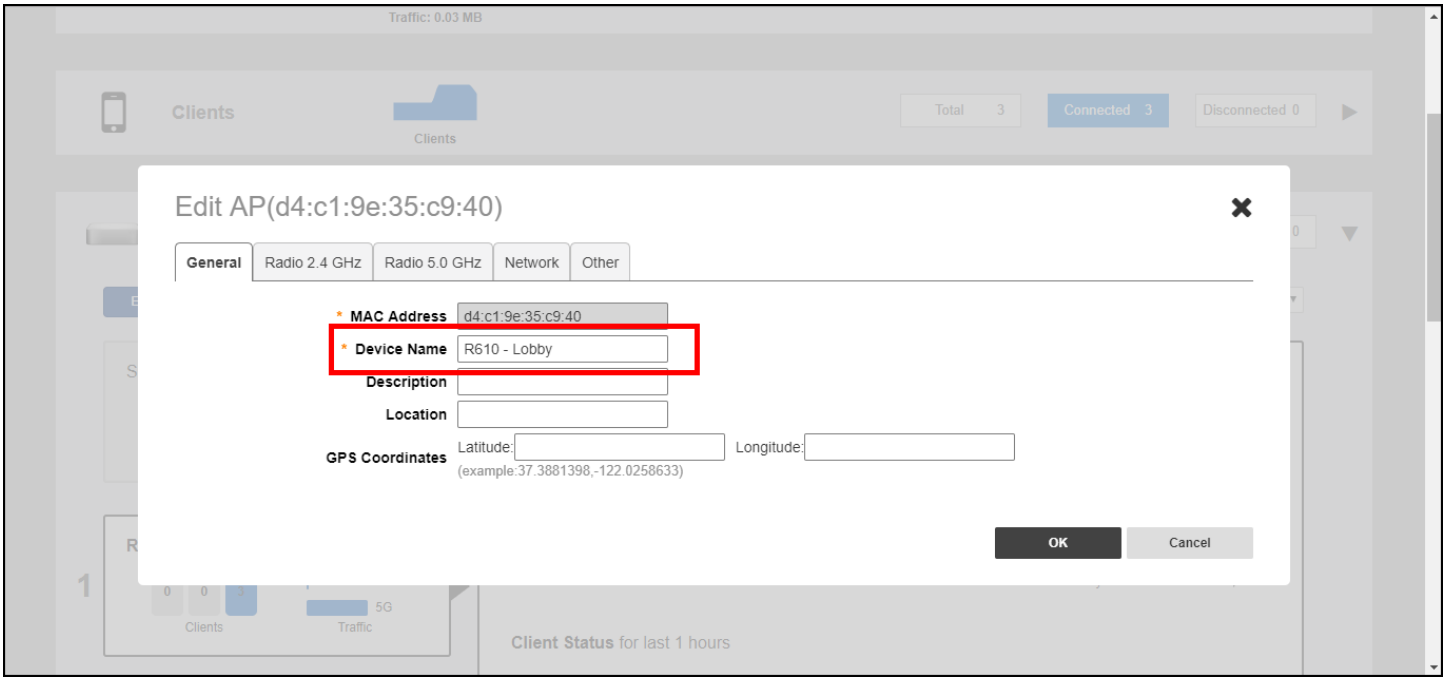


Renaming an AP

Renaming an AP allows the AP to be more easily identifiable in Unleashed dashboard components, tables, charts and graphs and other user interface elements.

To rename an AP, replace the **Device Name** field on the *Edit AP* form with a recognizable name for the AP.

FIGURE 214 Renaming an AP



Working with AP Groups

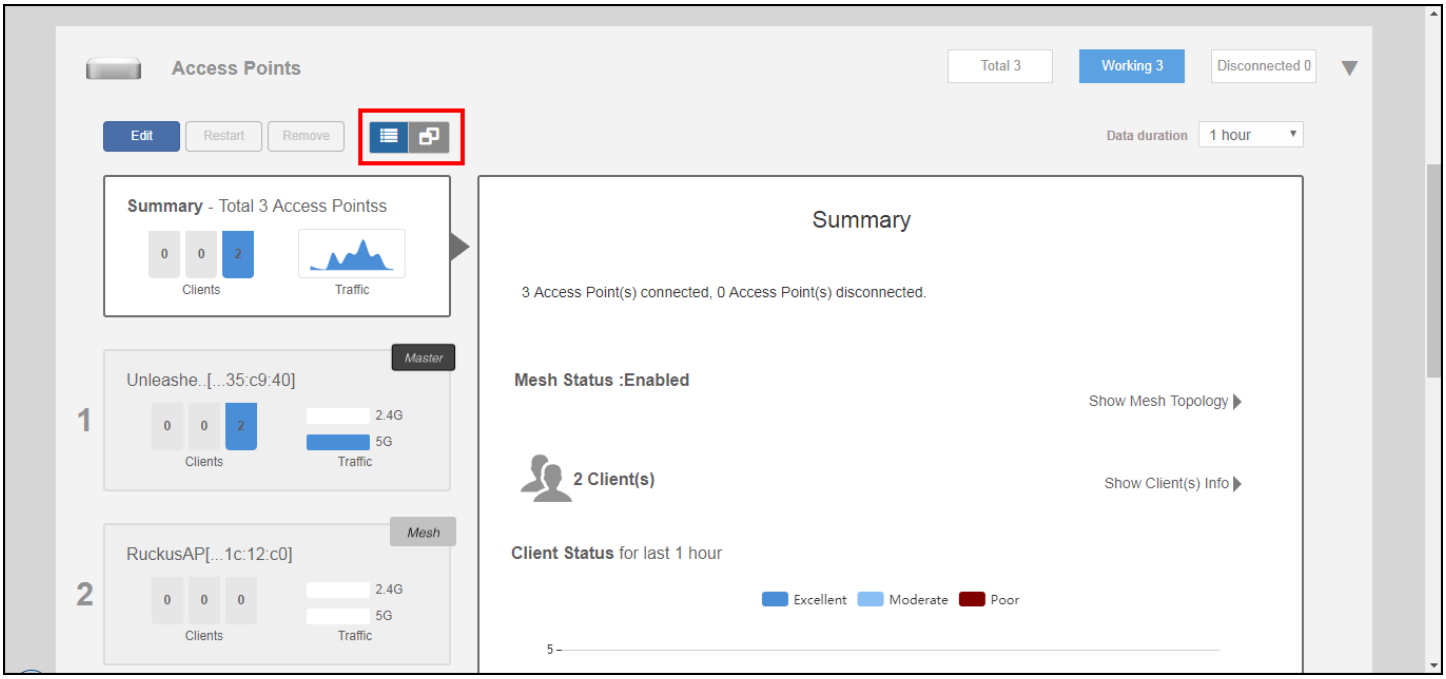
Access Point Groups can be used to define configuration options and apply them to groups of APs at once, without having to modify each AP's settings individually.

For each group, administrators can create a configuration profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group, or for all APs of a specific model in the group. By default, all AP's are members of the "System Default" AP group.

AP group configuration settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, leave the Tx Power Adjustment at *Auto* in the System Default AP Group, then go to the individual AP configuration page, and set the Tx Power setting to a lower setting.

AP group settings can be viewed and configured when the view mode on the *Access Points* screen is set to "AP Group."

FIGURE 215 Set View Mode to AP Group



Viewing AP Group Members

Select an AP group to view details on all APs that are members of the AP group.

To view AP group membership:

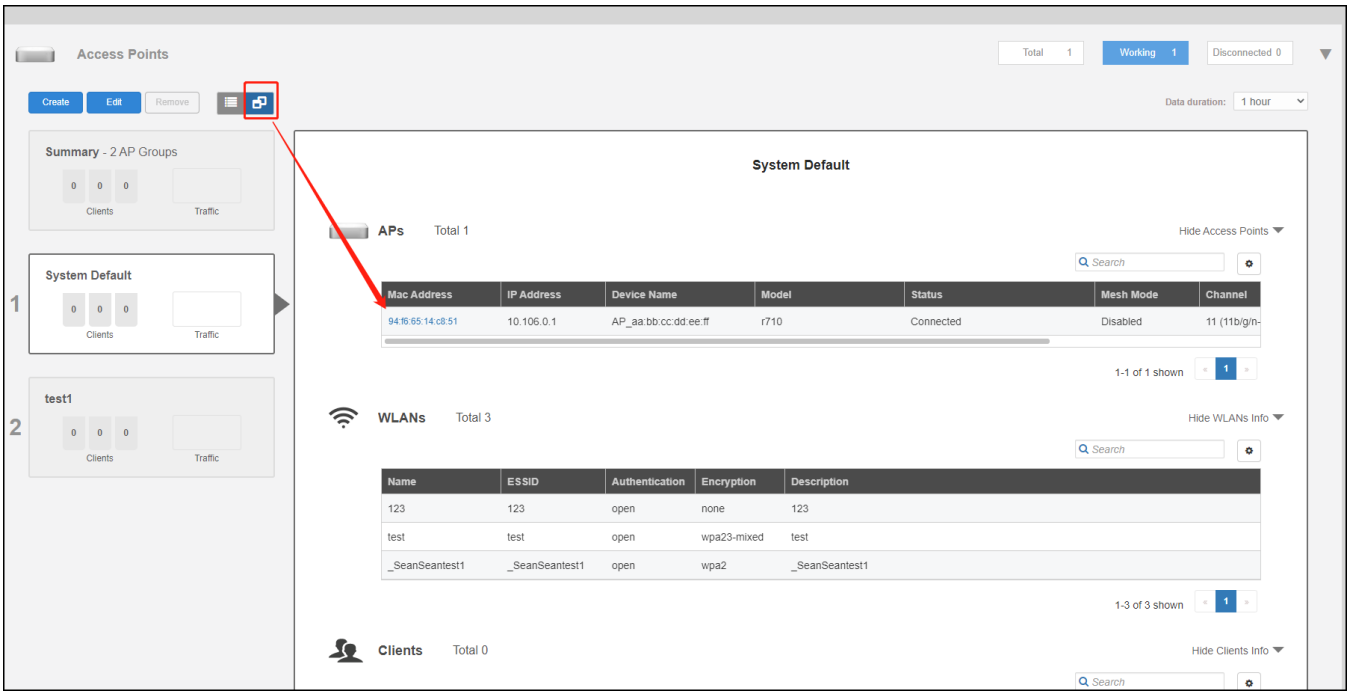
1. Go to **Access Points** and click the **Group View** button.

   You can view details of each member of the AP group, including its MAC address, IP address, Device Name, Model number, Status, Mesh Mode, Channel, and Serial Number.

2. In the AP table, click on the MAC address of the AP to view the AP detail page of each AP.

   NOTE
   By default, only AP group view is displayed if there are more than 25 APs in the network.

FIGURE 216 Viewing Members of an AP Group



Modifying the System Default AP Group

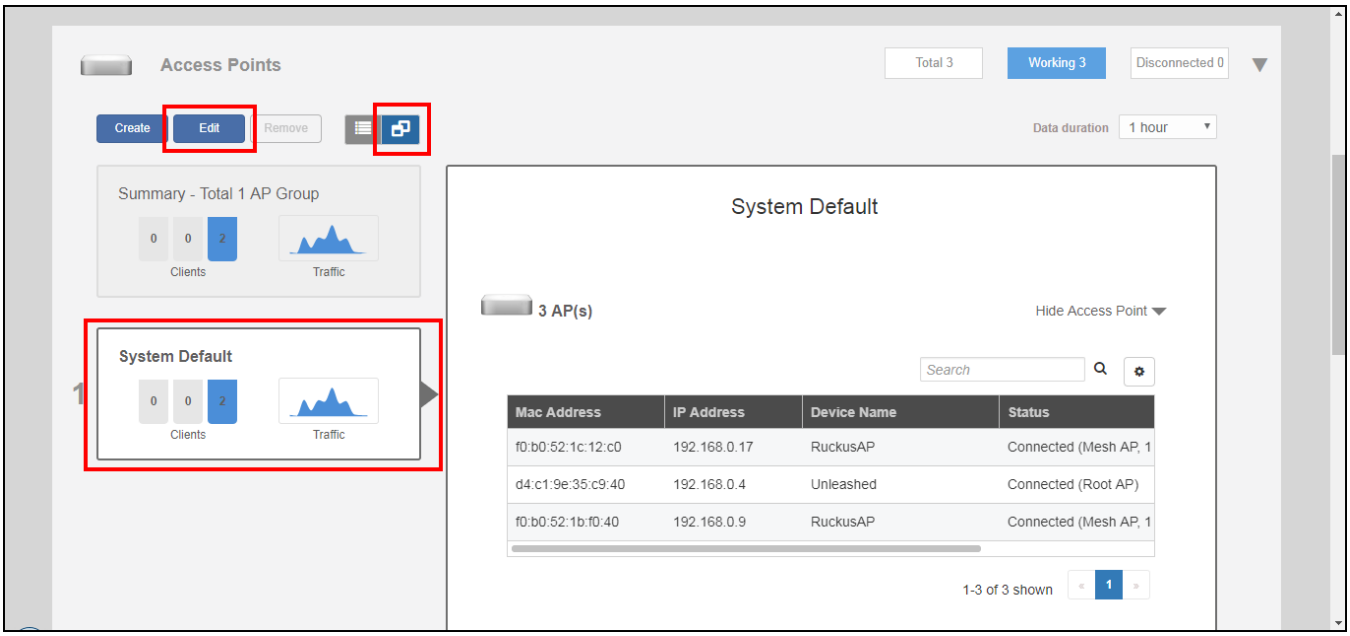
If you want to configure global settings for default behavior for all access points, modify the System Default AP group and apply settings to all APs at once.

To modify the System Default Access Point group and apply global configuration:

1. Go to **Access Points**.

2. Select the **Access Point Groups** view, select the **System Default** access point group, and click the **Edit** button.

FIGURE 217 Clicking Edit to Configure the AP Group



The *Edit AP Group* form appears.

3. Assign APs to or from this AP group using the left and right arrows on the *AP Assign* tab.
4. Assign WLANs to or from this AP group using the left and right arrows on the *WLAN Assign* tab.

5. On the *Radio B/G/N (2.4G)* and *Radio A/N/AC (5G)* tabs, modify any of the following settings that you want to apply to the System Default AP group.
   - **Channel Range**: To limit the available channels for 2.4 GHz, 5 GHz Indoor and 5 GHz Outdoor channel selection, deselect any channels that you do not want the APs to use.

     NOTE
     For country codes "US", "UK", and "JP", channel 144 is supported if DFS channel is enabled.

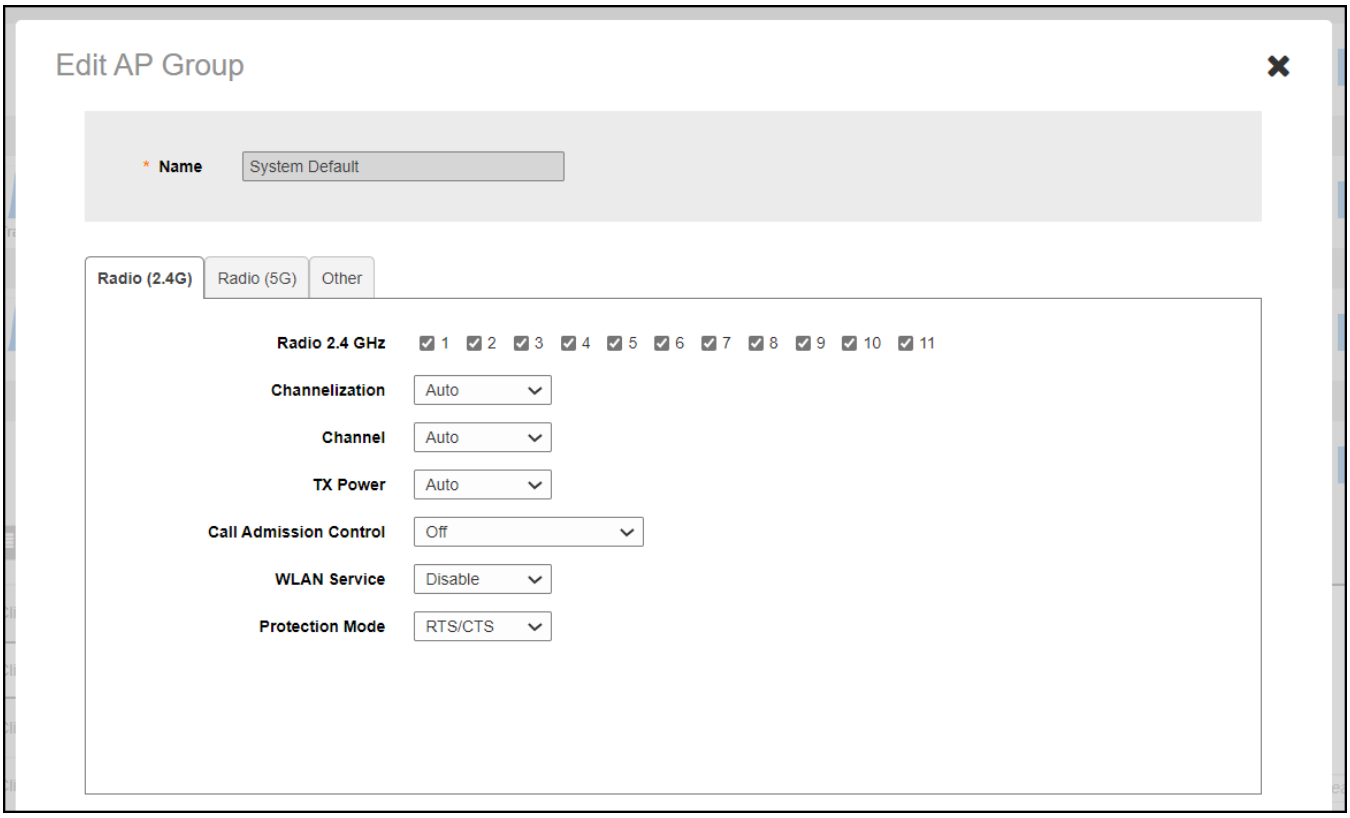
   - **Channelization**: Select Auto, 20MHz or 40MHz channel width for the 2.4 GHz radio, or Auto, 20, 40, or 80 MHz channel width for the 5 GHz radio.
   - **Channel**: Select Auto or manually assign a channel for the 2.4 GHz or 5 GHz radio.
   - **TX Power**: Allows you to manually set the transmit power on all 2.4 GHz or 5 GHz radios (default is Auto).

     Max = max allowable Tx power according to country regulations

     Min = 0dBm per chain for 11n APs, 2dBm per chain for 11ac APs
   - **Call Admission Control**: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/ Spectralink VIEW certification.
   - **WLAN Service**: This option allows users to disable WLAN service on the 2.4 or 5 GHz radios on all APs in the AP group.
   - **Protection Mode**: If you activate Protection Mode, you control how 802.11 devices know when they should communicate with another device. The use of RTS/CTS (Request to Send/Clear to Send) reduces collisions and increases the performance of the network if hidden stations are present. However, RTS/CTS (and CTS-only) introduce overhead and may in fact reduce overall performance in some situations. Through the proper use of RTS/CTS and CTS-only, you can fine-tune the operation of your wireless LAN depending on the physical operating environment.
     - **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification.
     - **RTS/CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.
     - **None**: Choose this option to disable both RTS and CTS acknowledgment.
6. On the *Other* tab, modify settings for all APs of a specific model in the System Default AP group. For more information on model-specific controls, see Modifying Model Specific Controls on page 300.
   - **Model Specific Control**: Select the AP model to which the settings will apply.
     - **Max Clients**: Set the maximum number of clients that can associate per AP. Note that different AP models have different maximum client limitations.
     - **Status LEDs**: When managed by ZoneDirector, you can disable the external LEDs on certain AP models. This can be useful if your APs are installed in a public location and you don't want to draw attention to them.
     - **PoE Operating Mode**: Options vary depending on AP model selected in *Model Specific Control*. For a list of PoE operating modes by AP model, refer to Unleashed Access Point Power Supply Considerations on page 501.
     - **Port Setting**: Refer to Configuring AP Ethernet Ports on page 324 for more information on configuring AP-specific Ethernet port settings.

7. Click **Finish** to save your changes.

FIGURE 218 Configuring AP Group Settings



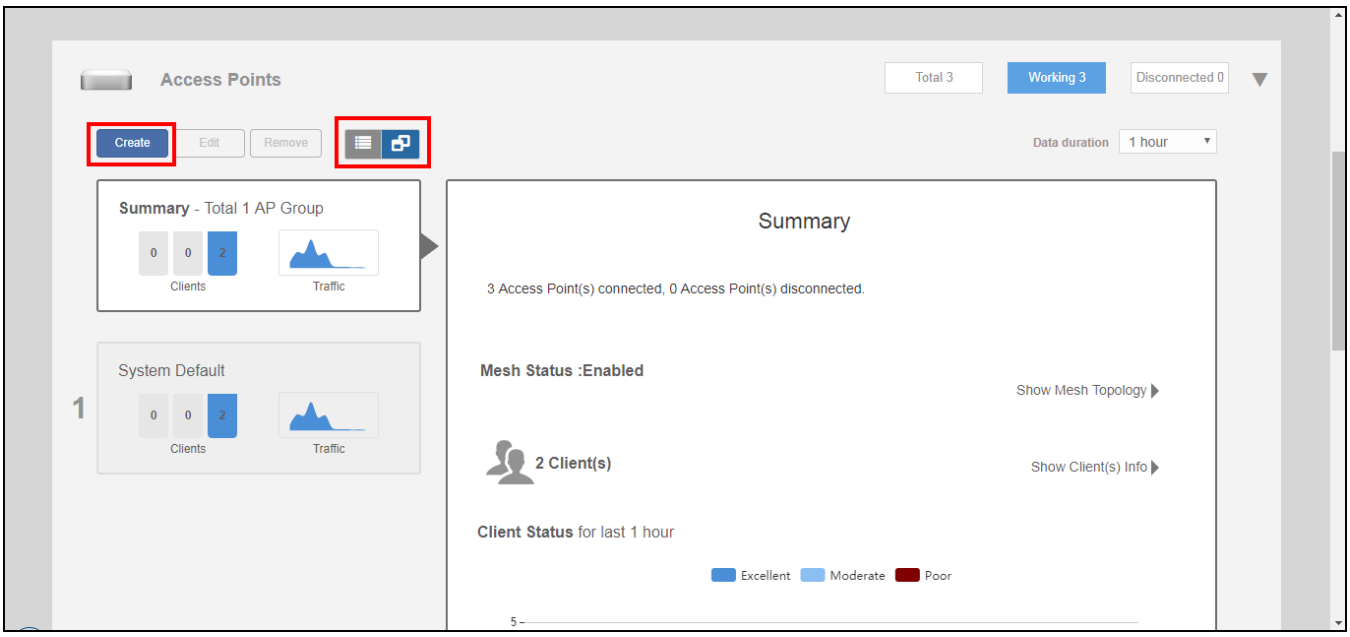
Creating a New AP Group

Create new AP groups to apply custom settings to a group of APs distinct from the system default group's settings.

To create a new AP group:

1. Go to **Access Points > AP Groups**, and click **Create**.

   FIGURE 219 Creating a New AP Group



   The *Create AP Group* form appears.

2. Assign APs to or from this AP group using the left and right arrows on the *Step 1 - Assign APs* screen.
3. Assign WLANs to or from this AP group using the left and right arrows on the *Step 2 - Assign WLANs* screen.

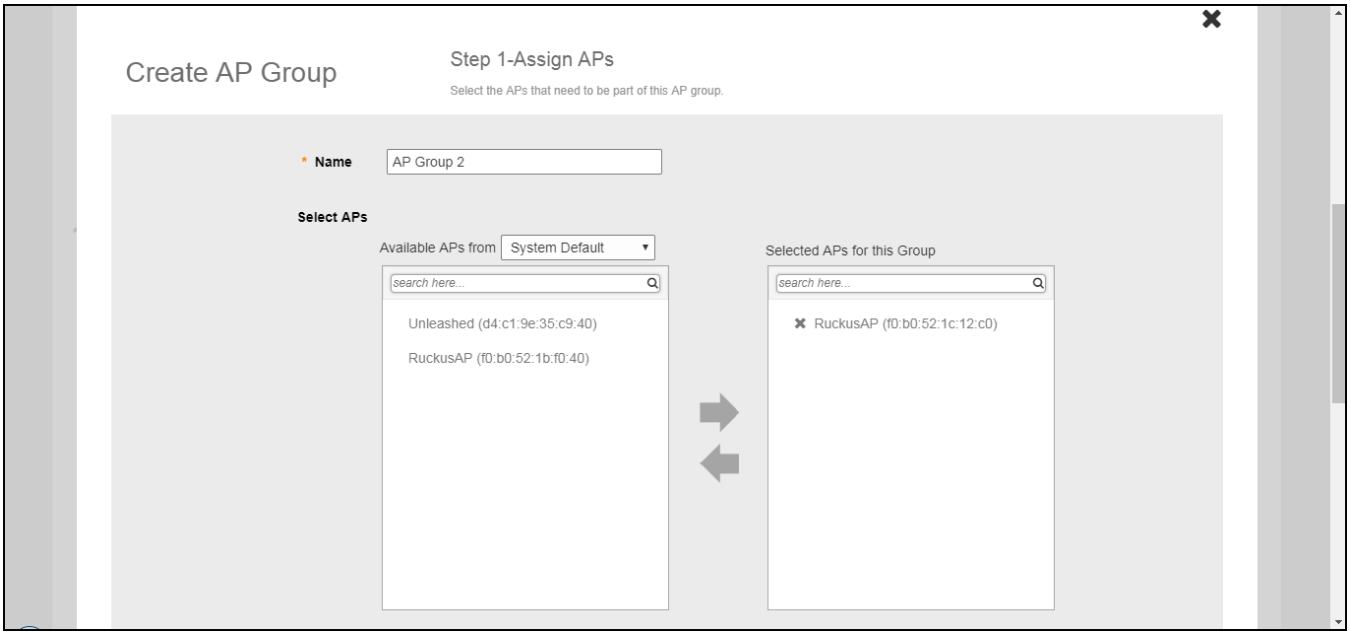
4. On the *Radio B/G/N (2.4G)* and *Radio A/N/AC (5G)* tabs, modify any of the following settings that you want to apply to the group:
   - **Channel Range**: To limit the available channels for 2.4 GHz, 5 GHz Indoor and 5 GHz Outdoor channel selection, deselect any channels that you do not want the APs to use.
   - **Channelization**: Select Auto, 20MHz or 40MHz channel width for the 2.4 GHz radio, or Auto, 20, 40, or 80 MHz channel width for the 5 GHz radio.
   - **Channel**: Select Auto or manually assign a channel for the 2.4 GHz or 5 GHz radio.
   - **TX Power**: Allows you to manually set the transmit power on all 2.4 GHz or 5 GHz radios (default is Auto).

     Max = max allowable Tx power according to country regulations

     Min = 0dBm per chain for 11n APs, 2dBm per chain for 11ac APs
   - **Call Admission Control**: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/ Spectralink VIEW certification.
   - **WLAN Service**: This option allows users to disable WLAN service on the 2.4 or 5 GHz radios on all APs in the AP group.
   - **Protection Mode**: Protection Mode allows control over how 802.11 devices know when they should communicate with another device. The use of RTS/CTS (Request to Send/Clear to Send) reduces collisions and increases the performance of the network if hidden stations are present. However, RTS/CTS (and CTS-only) introduce overhead and may in fact reduce overall performance in some situations. Through the proper use of RTS/CTS and CTS-only, you can fine-tune the operation of your wireless LAN depending on the physical operating environment.
     - **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification.
     - **RTS/CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.
     - **None**: Choose this option to disable both RTS and CTS acknowledgment.

5. On the *Other* tab, modify any of the following settings that you want to apply to the System Default AP group:
   - **Model Specific Control**: Select the AP model to which the settings will apply. For more information, see *Modifying Model Specific Controls*.
   - **Max Clients**: Set the maximum number of clients that can associate per AP. Note that different AP models have different maximum client limitations.
   - **Status LEDs**: When managed by ZoneDirector, you can disable the external LEDs on certain AP models. This can be useful if your APs are installed in a public location and you don't want to draw attention to them.
   - **PoE Operating Mode**: Options vary depending on AP model selected in Model Specific Control. For a list of PoE operating modes by AP model, refer to *Unleashed Access Point Power Supply Considerations*.
   - **Port Setting**: Refer to *Configuring AP Ethernet Ports* for more information on configuring AP-specific Ethernet port settings.

FIGURE 220 Create new AP group



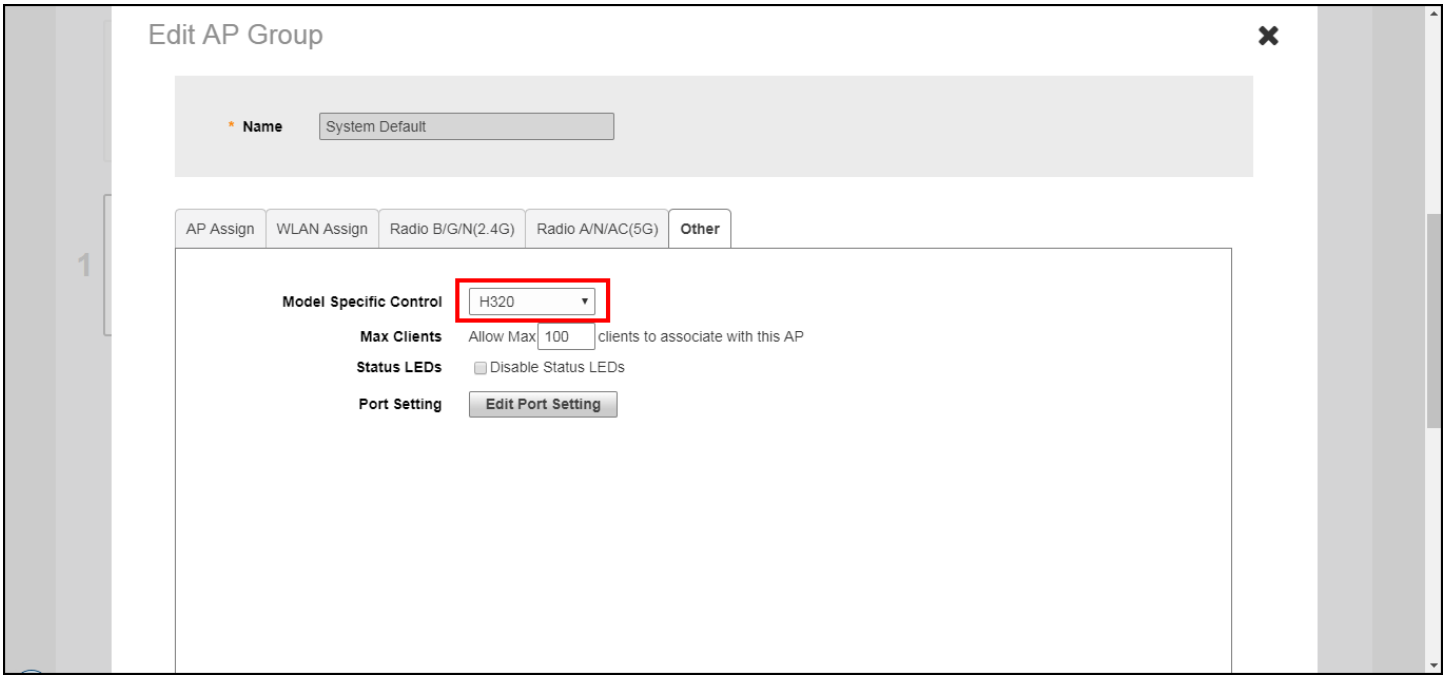
Modifying Model Specific Controls

The following settings can be applied to all APs of a particular model that are members of the AP group:

Some options are available for specific AP models only.

To configure model-specific settings for the AP group, select the AP model from the **Model Specific Control** list.

FIGURE 221 Model Specific Controls

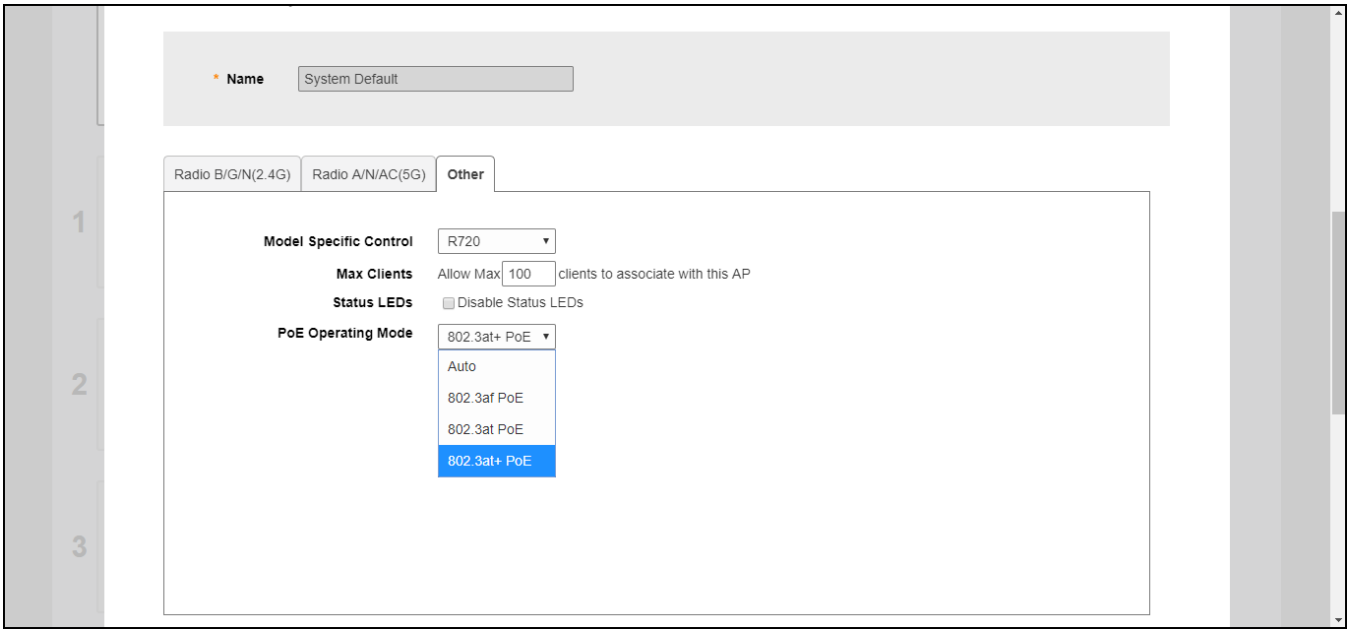


Configure any of the following settings for each model independently, and click **Finish** to save your changes:

- **Max Clients**: Set the maximum number of clients that can associate per AP. Note that different AP models have different maximum client limitations.
- **PoE Out Ports**: Enable PoE out ports (specific AP models only).
- **Status LEDs**: Disable the external LEDs on certain AP models. This can be useful if your APs are installed in a public location and you don't want to draw attention to them.
- **External Antenna**: On APs with external antenna options, select Enable for the external antenna to be enabled. When enabled, enter a gain value in the range of 0 to 90 dBi. Default is 3 dBi.
- **Port Settings**: Refer to Configuring AP Ethernet Ports on page 324 for more information on configuring AP-specific Ethernet port settings.
- **PoE Operating Mode**: Select PoE operating mode, Auto, 802.3af or 802.3at PoE (specific AP models only). Default is *Auto*. If 802.3af PoE is selected, the AP will operate in 802.3af mode (not 802.3at mode), and will consume less power than in 802.3at mode. However, when this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports.

  NOTE
  On some APs, an additional mode - 802.3at+ PoE - is available. This mode enables all features on the AP but requires an Ethernet switch that supports the 802.3at+ standard due to the higher power draw from the port to which the AP is connected. For a list of PoE operating modes by AP model, refer to Unleashed Access Point Power Supply Considerations on page 501.

FIGURE 222 PoE Operating Mode



Configuring AP Ethernet Ports

You can use AP groups to configure Ethernet ports on all APs of a certain model.

NOTE
Currently, only Unleashed H320 and H510 wall-plate APs provide Ethernet port configuration options.

To configure Ethernet ports for all APs of the same model:

1. Go to **Access Points**.
2. In the **AP Groups** view, click **Edit** for the group you want to configure.
3. On the **Other** tab, locate the **Model Specific Control** section, and select the AP model that you want to configure from the list.
4. Click the **Port Setting** button. The page refreshes to display the Ethernet ports on the AP model currently selected.
5. Deselect the check box next to **Enable** to disable this LAN port entirely. All ports are enabled by default.
6. Select **DHCP_Opt82** if you want to enable this option for this port (see *DHCP Option 82*).
7. For any enabled ports, you can choose whether the port will be used as a **Trunk Port**, an **Access Port** or a **General Port**. The following restrictions apply:
   - All APs must be configured with at least one Trunk Port.
   - For Wall Plate APs (such as the H510), the LAN5/Uplink port on the rear of the AP is defined as a Trunk Port and is not configurable. The front-facing LAN ports are configurable.
   - For all other APs, you can configure each port individually as either a Trunk Port, Access Port or General Port. (See *Designating Ethernet Port Type* for more information.)
8. To segment this port's traffic into a separate VLAN from the native VLAN, use the VLAN **Untag ID** field.
9. In **Guest VLAN**, enter the VLAN ID for the guest VLAN, if configured.

10. In **Dynamic VLAN**, enable the check box to enable dynamic VLAN assignment based on RADIUS settings.

FIGURE 223 Configuring AP Ethernet Ports - H510

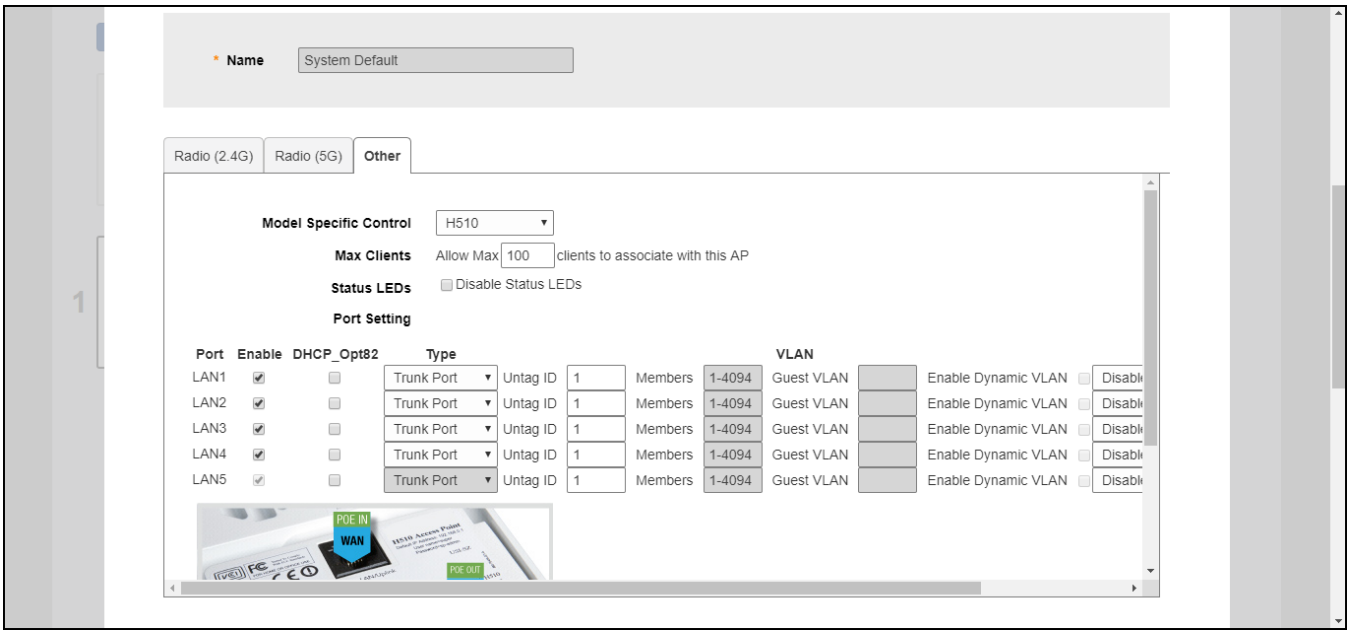
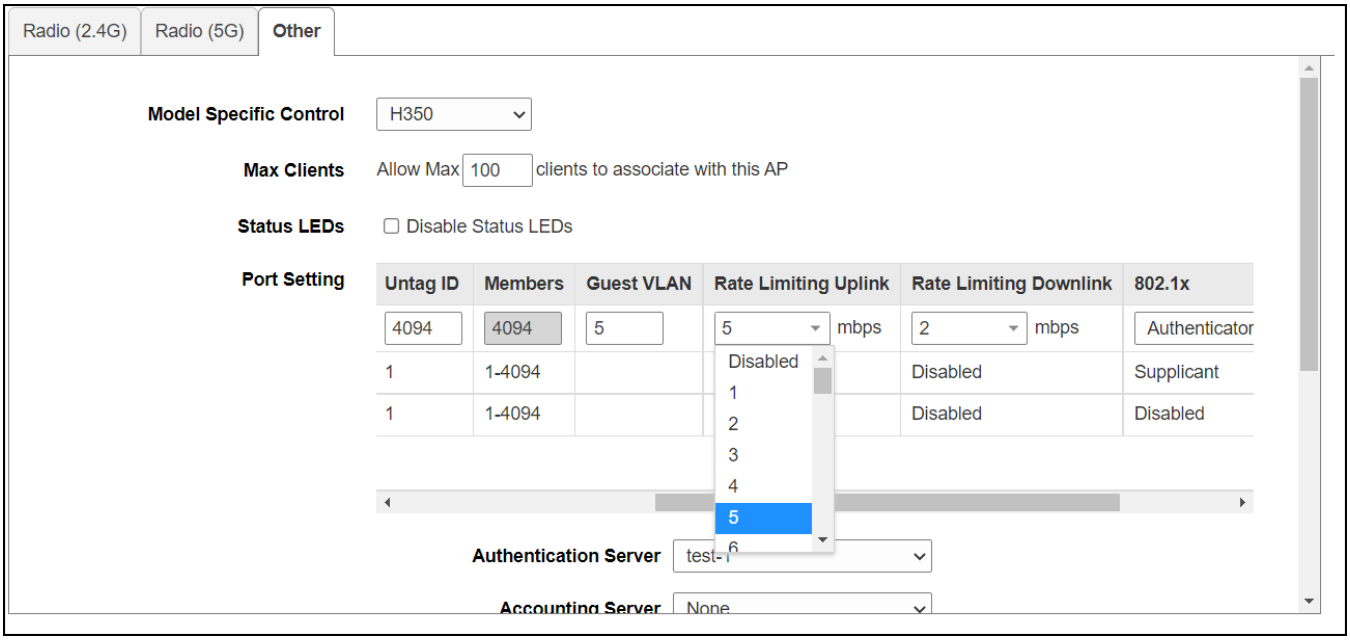


FIGURE 224 Configuring AP Ethernet Ports - H350



11. In **Rate Limiting Uplink** and **Rate Limiting Downlink**, select a value starting from 1 through 500 (Mbps).

    NOTE
    Memory type of 11ax and cypress is 500 Mbps, and other APs (QCA, dakota, mips) is 200 Mpbs.

    NOTE
    Rate Limit supports maximum of 100 clients per WLAN. If the number of clients is more than 100, it will run out of memory of AP.

12. In **802.1X**, select whether the port will be used as an 802.1X Supplicant, Authenticator (port-based or MAC-based), or whether 802.1X is disabled on the port. AP Ethernet ports can be individually configured to serve as either an 802.1X supplicant (authenticating the AP to an upstream authenticator switch port), or as an 802.1X authenticator (receiving 802.1X authentication requests from downstream supplicants). A single port cannot provide both supplicant and authenticator functionality at the same time.
    - **Disabled**: 802.1X authentication is disabled for this port.
    - **Supplicant**: This port authenticates itself to an upstream Authenticator port.
    - **Authenticator (Port-Based)**: This port accepts auth requests from downstream stations. In Port-based mode, only a single MAC host must be authenticated for all hosts to be granted access to the network.
    - **Authenticator (MAC-Based)**: This port accepts auth requests from downstream stations. In MAC-based mode, each MAC host is individually authenticated. Each newly-learned MAC address triggers an EAPOL request-identify frame.

    For more information on port based 802.1X, see *Using Port Based 802.1X*.
13. In **Authenticator** (options appear if any port is configured as an Authenticator), select an **Authentication Server** and **Accounting Server** against which to authenticate clients from the drop-down list.

    Optionally, **Enable MAC authentication bypass (Use device MAC address as username and password)** to allow specific devices to bypass 802.1X authentication.
14. In **Supplicant** (options appear if any port is configured as a Supplicant), select the supplicant authentication method:
    - **MAC Address**: Use the station's MAC address as the user name and password.
    - **User Name** and **Password**: Enter the login info for authenticating this supplicant port to an upstream authenticator port.

15. Click **Finish** to save your changes.

FIGURE 225 H510 Port Settings: Enable, DHCP Option 82, Port Type, and VLAN Untag ID

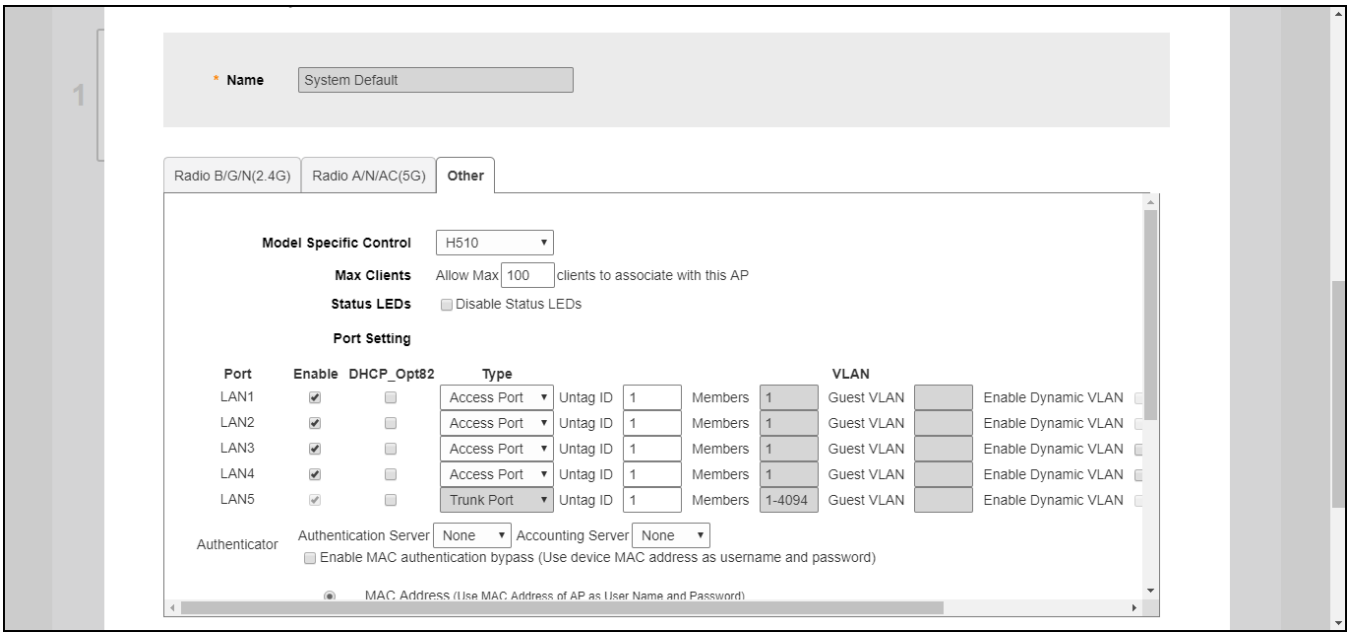


FIGURE 226 H510 Port Settings: Guest VLAN, Dynamic VLAN and 802.1X

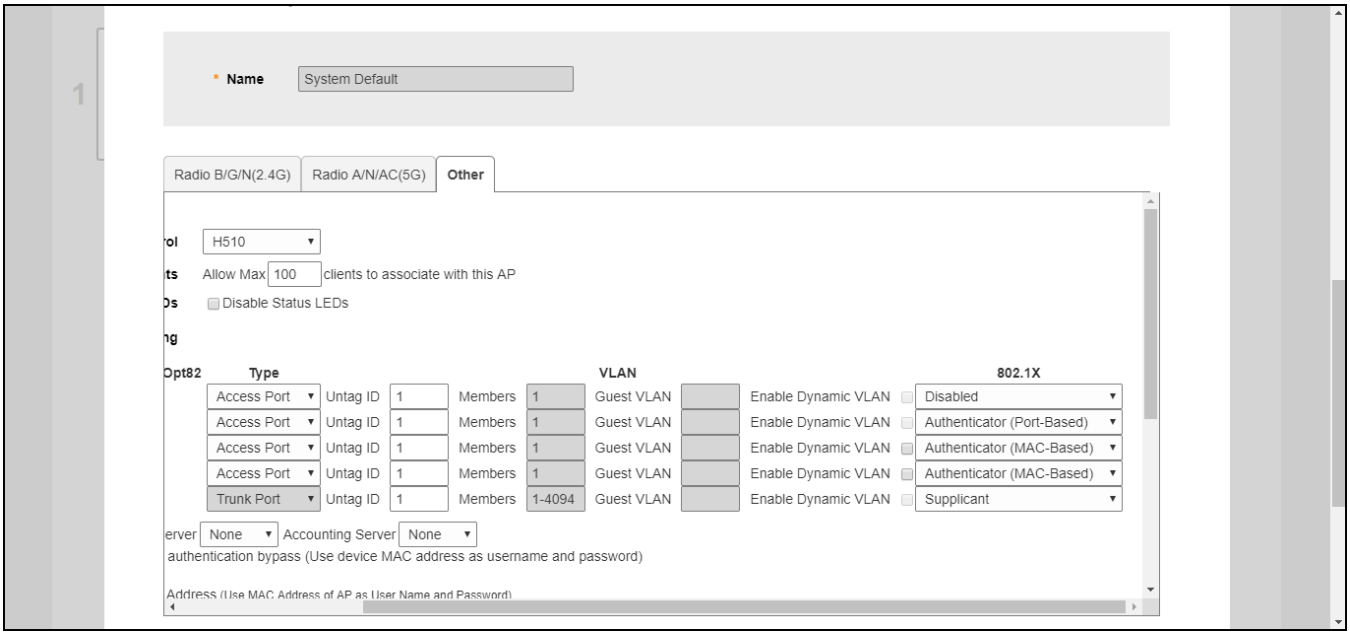
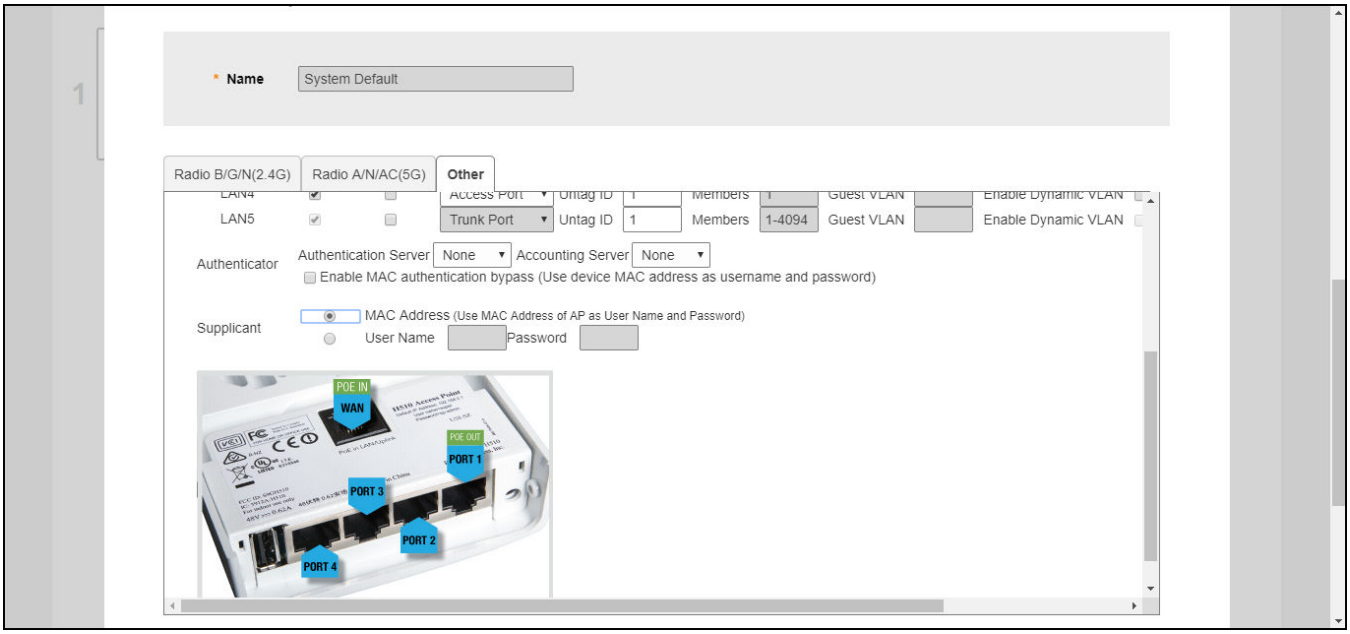


FIGURE 227 H510 Authenticator and Supplicant Settings



Designating Ethernet Port Type

Ethernet ports are defined as one of the following port types:

- Trunk Ports
- Access Ports
- General Ports

All three port types are used to define how to manage the following two aspects of VLAN processing:

- Which VLANs are processed vs. dropped
- What to do with untagged packets (in other words, Native VLAN)

For most RUCKUS APs, you can set which ports you want to be your Access, Trunk and General Ports from the Unleashed web interface, as long as at least one port on each AP is designated as a Trunk Port.

NOTE
By default, all ports are enabled as Trunk Ports with Untag VLAN set as 1 (except for Wall Plate APs, such as H510, whose four front-bottom ports are enabled as Access Ports by default, and whose rear port is a Trunk Port and is non-configurable).

If configured as an Access Port, all untagged ingress traffic is sent to the configured Untag VLAN, and all egress traffic is sent untagged. If configured as a Trunk Port, all untagged ingress traffic is the configured Untag VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.

The default Untag VLAN for each port is VLAN 1. Change the Untag VLAN to:

- Segment all ingress traffic on this Access Port to a specific VLAN
- Redefine the Native VLAN on this Trunk Port to match your network configuration

Trunk Ports

Trunk links are required to pass VLAN information between switches. Trunking is a function that must be enabled on both sides of a link. If two switches are connected together, for example, both switch ports must be configured as trunk ports. The Trunk port is a member of all the VLANs that exist on the AP/switch and carries traffic for all VLANs between switches.

For a Trunk port, the VLAN Untag ID field is used to define the native VLAN - the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the AP Trunk port's VLAN Untag ID with the native VLAN used throughout your network.

Access Ports

Access ports provide access to the network and can be configured as members of a specific VLAN, thereby separating the traffic on these ports from traffic on other VLANs.

All Access Ports are set to Untag (native) VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. When untagged frames from a client arrive at an AP's Access Port, they are given an 802.1Q VLAN header with "1" as their VLAN ID before being passed onto the wired network.

When VLAN 1 traffic arrives destined for the client, the VLAN tag is removed and it is sent as plain (untagged) 802.11 traffic. When any tagged traffic other than VLAN 1 traffic arrives at the same Access Port, it is dropped rather than forwarded to the client.

To remove ports from the native VLAN and assign them to specific VLANs, select Access Portand enter any valid VLAN ID in the VLAN IDfield (valid VLAN IDs are 2-4094).

The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

TABLE 34 Access Ports with VLANs configured

VLAN Settings	Incoming Traffic (from the client)	Outgoing Traffic (to the client)
Access Port, Untag VLAN 1	All incoming traffic is native VLAN (VLAN 1).	All outgoing traffic on the port is sent untagged.
Access Port, Untag VLAN [2-4094]	All incoming traffic is sent to the VLANs specified.	Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped.

General Ports

General ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned. General ports function similarly to Trunk ports, except that where Trunk ports pass all VLAN traffic, General ports pass only the VLAN traffic that is defined by the user.

To configure an AP Ethernet port as a General port, select General Port and enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

> **NOTE**
> You must also include the Untag (native) VLAN ID in the Members field when defining the VLANs that a General port will pass. For example, if you enter 1 as the Untag VLAN ID and want the port to pass traffic on VLANs 200 and 300, you would enter: **1,200,300**.

Using Port Based 802.1X

802.1X authentication provides the ability to secure the network and optionally bind service policies for an authenticated user.

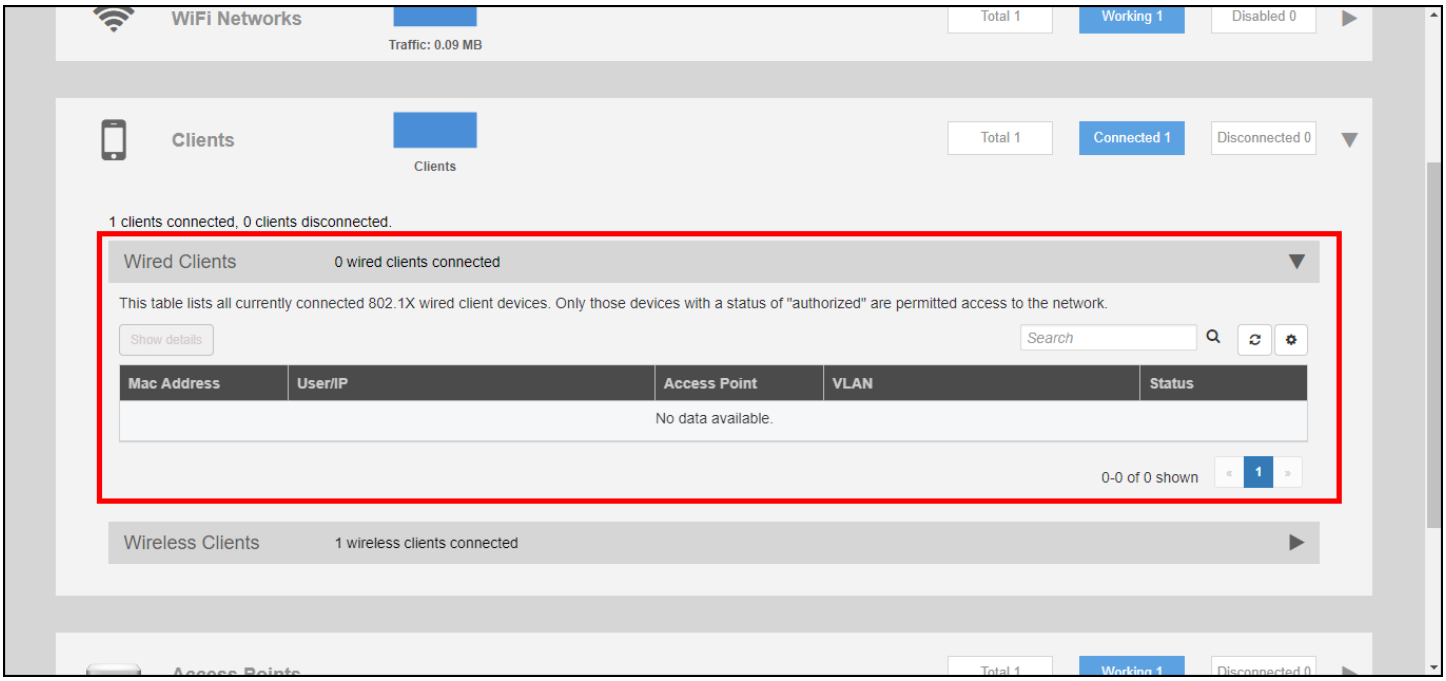
> **NOTE**
> 802.1X port settings are unavailable when mesh mode is enabled.

802.1X provides logical port control and leverages the EAP authentication and RADIUS protocols to allow the network policy to be effectively applied in real time, no matter where the user connects to the network.

AP Ethernet ports can be individually configured to serve as either an 802.1X supplicant (authenticating the AP to an upstream authenticator switch port), or as an 802.1X authenticator (receiving 802.1X authentication requests from downstream supplicants). A single port cannot provide both supplicant and authenticator functionality at the same time.

If port based 802.1X is enabled on any ports, you can monitor connected wired clients by expanding the **Clients** Dashboard component and clicking **Wired Clients** to display a list of authenticated 802.1X wired clients.

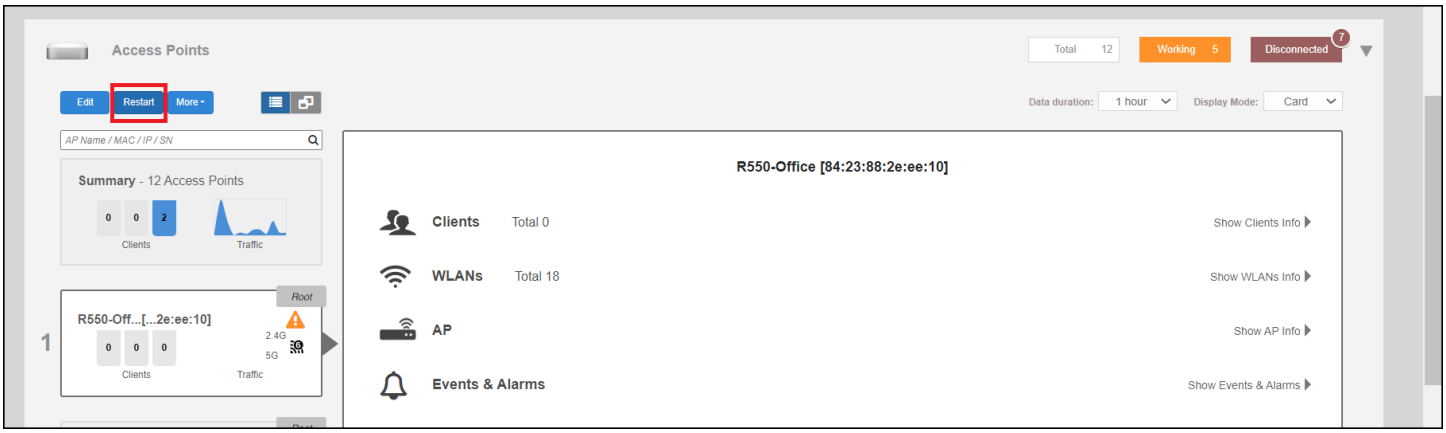
FIGURE 228 Monitor currently connected 802.1X wired clients



Restarting an AP

To restart an AP, expand the Access Points section, click the AP's box on the left side, then click **Restart**.

FIGURE 229 Click Restart to reboot a single AP



NOTE
Restarting the Unleashed Master AP will prompt you to click **OK** to confirm, as the network will experience a brief service interruption during the restart process. Additionally, restarting the Master AP will force another AP to assume the role of Master (when more than one Unleashed AP exists on the network).

Removing an AP

To remove a member AP from the Unleashed network, expand the Access Points section, click the AP's box on the left side, then click **Remove**.

Once removed, the **Approve** button becomes available. Click **Approve** to allow the AP to rejoin the Unleashed network.

FIGURE 230 Removing an AP

ICX Switch Management

- ICX Switch Management Overview 333
- Preparing an ICX Switch for Unleashed Management 334
- Approving a New Switch to Join Unleashed 337
- Monitoring Connected ICX Switches 340
- Managing Switch Ports 342
- Backup and Restore Switch Configuration 345
- Upgrading ICX Switch Firmware 348

ICX Switch Management Overview

Beginning with Unleashed release 200.8, the administrator can monitor and manage RUCKUS ICX switches and routers in the ICX 7000 series and above. Unleashed can manage up to 8 switches at a time.

ICX switch management allows you to monitor status, view usage statistics, and perform basic management operations including configuration backup and firmware management.

The following capabilities are supported:

- ICX switch registration and authentication
- Switch inventory (including model, firmware version, and last backup)
- Health and performance monitoring (status, traffic stats, errors, clients) with alarms
- Switch configuration file backup and restore
- Firmware upgrades

Requirements

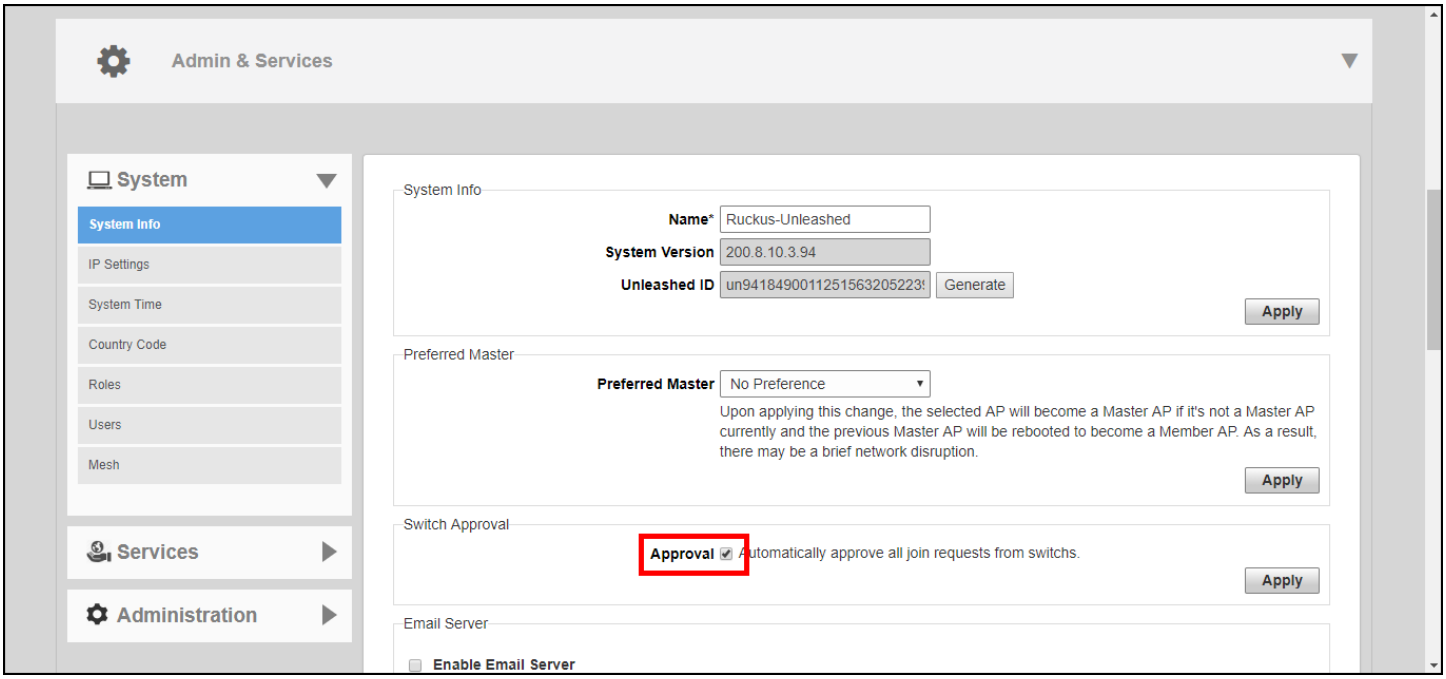
> **NOTE**
> For more information on ICX device capabilities and configuration, refer to the RUCKUS FastIron documentation set available at the following URL:
> https://support.ruckuswireless.com. On the site, select **Products > RUCKUS ICX Switches > Technical Documents**, and choose the platform and document of interest.

The following items are required to manage ICX devices:

- The ICX switch must be running FastIron software version **08.0.90** or higher.
- The Unleashed Master AP's IP address must be reachable by the ICX device through the Management interface or through router interfaces.
- ICX devices will be automatically discovered by the Unleashed Master. If automatic switch approval is enabled, all ICX switches discovered on the network will be listed in the *Switches* dashboard component. To disable automatic approval, go to **Admin & Services > System > System Info > Switch Approval** and disable the **Approval** option.

ICX devices running either router or switch images can be managed by Unleashed.

FIGURE 231 Switch auto approval



Preparing an ICX Switch for Unleashed Management

Unleashed uses LLDP (Link Layer Discovery Protocol) for communication with the ICX switch. Preparing the switch for Unleashed management requires that the device is running compatible firmware that supports LLDP and that its management IP address and login name and password are discoverable by the Unleashed Master AP.

The easiest way to do this is to reset the switch to factory default settings and allow Unleashed to auto-discover and auto-configure the switch for Unleashed management.

Beginning with ICX version 8.0.90, ICX switches in factory default state use the default user name and password **super/sp-admin**. When the Unleashed Master AP connects to an ICX switch via LLDP, it will attempt to log in using this default username and password. If successful, Unleashed will automatically change the ICX login to match the Unleashed admin login name and password.

To prepare an ICX switch for Unleashed management:

1. Confirm that the switch is running FastIron firmware version 08.0.90 or later using the following command:

```
SSH@ICX7150-C12-Switch#show version
  Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 1: compiled on Jun  6 2019 at 20:57:00 labeled as SPS08091
      (28774816 bytes) from Primary SPS08091.bin (UFI)
        SW: Version 08.0.91T211
      Compressed Primary Boot Code size = 786944, Version:10.1.16T225 (mnz10116)
       Compiled on Sat May 25 10:09:26 2019
...
...
```

2. If your device is running an earlier version, you must upgrade to version 08.0.90 or later. Refer to the *Release Notes*, *Upgrade Guide* and *Installation Guide* for the relevant FastIron release for upgrade instructions.

   NOTE
   Upgrading to a more recent release may require several steps (depending on the version of the original firmware) as each release has different upgrade requirements. Be sure to carefully read the FastIron documents to ensure a successful upgrade.

3. An ICX switch running 08.0.90 or later firmware in factory default state will attempt to register with an Unleashed Master AP via LLDP. An easy way to prepare a switch for Unleashed management is to reset the switch to factory default state. Use the following command to restore the switch to factory default settings:

```
SSH@ICX7150-C12-Switch#erase system factory-default
 System will go for reload after factory reset. Please enter 'y' to confirm, 'n' to exit :
(enter 'y' or 'n'): y
************************************************************
*               Factory Reset Alert                        *
************************************************************
* Please pay attention to the details listed below          *
* 1. uboot params will be erased, you might want to         *
* backup the uboot params                                   *
* stop at uboot and do 'printenv' to read uboot params      *
* 2. All configuration will be erased, you might want to    *
* backup the config                                         *
* 3. Core Files, Logs will be erased                        *
* 4. SAU license will be restored to original SKU           *
* use show license sau for more detials                     *
* 5. XML license will be erased                             *
************************************************************

************************************************************
 I have read the alert and factory reset can be performed now.
 Please enter 'y' to confirm, 'n' to exit :
************************************************************
(enter 'y' or 'n'):
```

4. When the factory reset is complete, the switch will reboot and perform LLDP neighbor discovery.
5. If **Auto Approval** is enabled (*Admin & Services > System > System Info > Switch Approval*), Unleashed will automatically approve the switch join request. If disabled, you must manually approve each switch join request.
6. The switch should now be visible on the Unleashed dashboard as connected, or "Pending" if auto-approval is disabled.
7. If the switch does not appear on the Unleashed dashboard after performing a factory reset, there are a number of possible explanations:
   - LLDP info does not exist: This typically indicates the switch is not running compatible firmware. Upgrade to 08.0.90 or later.
   - LLDP info exists, but Management IP info does not exist: This typically indicates the switch is in router mode. In this case, the admin must obtain the IP address from the router or DHCP server and then click the **Add** button to configure the IP address, admin name and password for the switch.
8. Use the following command to verify whether or not LLDP neighbor information exists:

```
SSH@ICX7150-C12-Switch#show lldp neighbors
Lcl Port Chassis ID      Port ID         Port Description           System Name
1/1/1    348f.2712.c950  348f.2712.c950  eth0                         RuckusAP
1/1/3    d4c1.9e35.c940  d4c1.9e35.c940  eth0                         Ruckus-Unleas~
SSH@ICX7150-C12-Switch#
```

9. Additionally, you can verify whether the AP can receive LLDP information from its neighbors using the AP CLI. To check the AP's LLDP info, use the following command:

```
ruckus(ap-mode)# get lldp neighbors
------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface:    eth0, via: LLDP, RID: 1, Time: 3 days, 02:55:58
  Chassis:
    ChassisID:    mac 78:a6:e1:2e:03:ce
    SysName:      ICX7150-C12-Switch
    SysDescr:     Not received
    MgmtIP:       192.168.0.24
    Capability:   Bridge, on
  Port:
    PortID:       mac 78:a6:e1:2e:03:d0
    PortDescr:    GigabitEthernet1/1/3
    MFS:          1522
    PMD autoneg:  supported: yes, enabled: yes
      Adv:          10Base-T, HD: yes, FD: yes
      Adv:          100Base-TX, HD: yes, FD: yes
      Adv:          1000Base-T, HD: yes, FD: yes
      MAU oper type: 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode
    MDI Power:    supported: yes, enabled: yes, pair control: no
      Device type:  PSE
      Power pairs:  signal
      Class:        class 4
      Power type:   2
      Power Source: unknown
      Power Priority: low
      PD requested power Value: 26200
      PSE allocated power Value: 26200
    UPOE:         0
------------------------------------------------------------------------------
OK
ruckus(ap-mode)#
```

10. After approval, if the switch is in factory default state, Unleashed will log in to the switch and change the default username/password to the Unleashed admin login name and password, and begin managing the switch.
11. If the switch is not in factory default state, select the switch in "Pending" state and click **Approve**, then enter the Admin Name and Password to authenticate to the switch and then manage it automatically.
12. If the Unleashed login name and password are changed via the web interface, the new login will be synched to any connected switches that registered with Unleashed in factory default state. Connected switches that registered as non-factory default switches will remain unchanged and will require the user to manually approve them and enter the new user name and password.

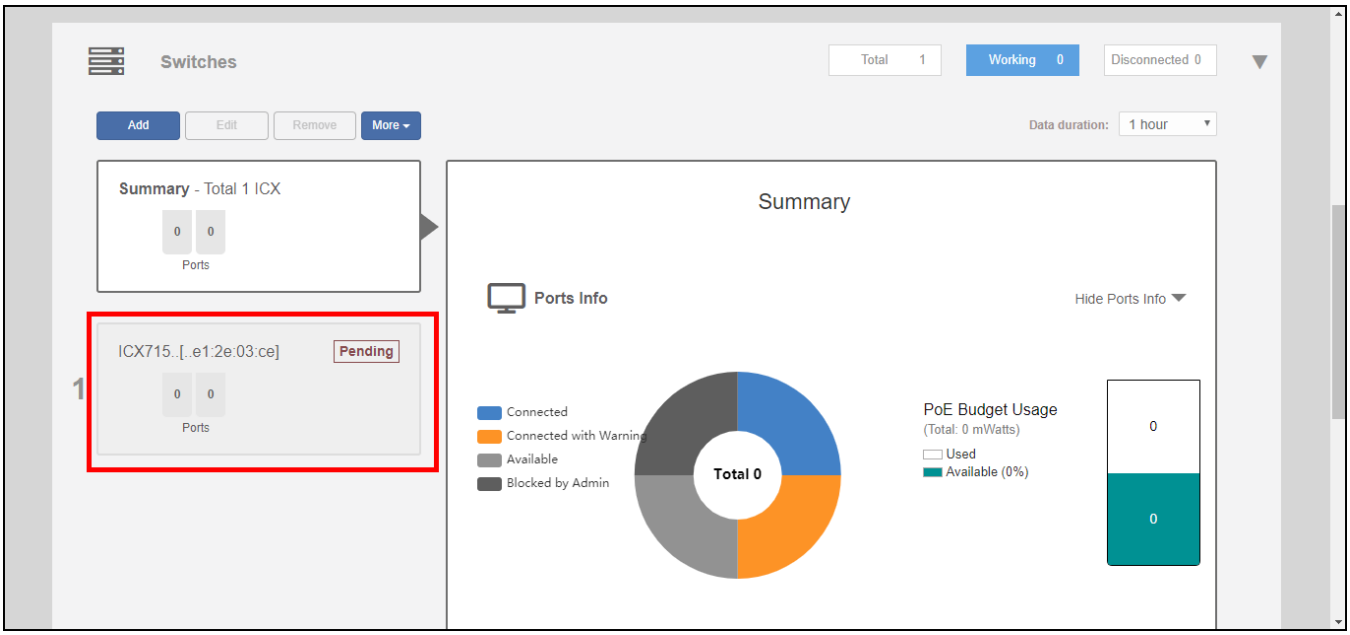
Approving a New Switch to Join Unleashed

Once an ICX switch has been discovered, it is listed in the web interface as "pending" until the administrator approves the join request by entering the switch admin user name and password (if auto-approval is disabled).

To approve a new switch to join Unleashed management:

1. Expand the **Switches** component, and select a switch that is marked as "Pending" in the list on the left side of the page.

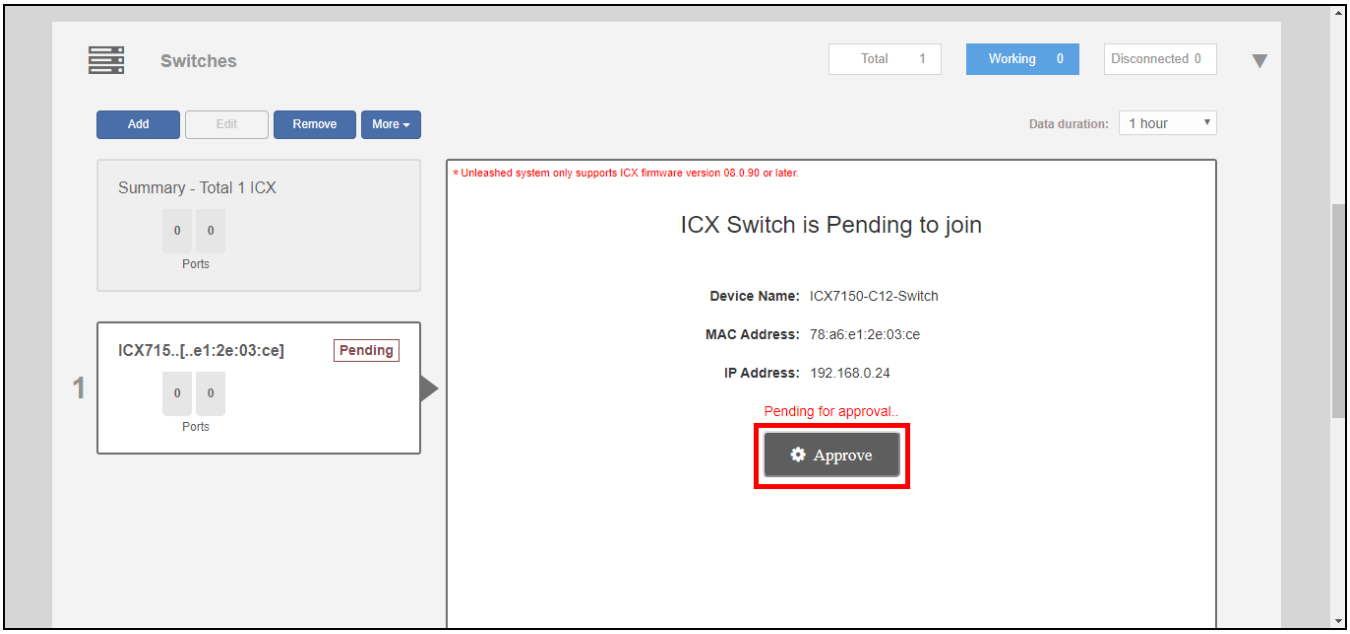
   FIGURE 232 Select a switch that is pending approval



NOTE
RUCKUS Unleashed does not recognize older versions of ICX switches and displays the following warning message: "Unleashed system only supports ICX firmware version 08.0.90 or later."

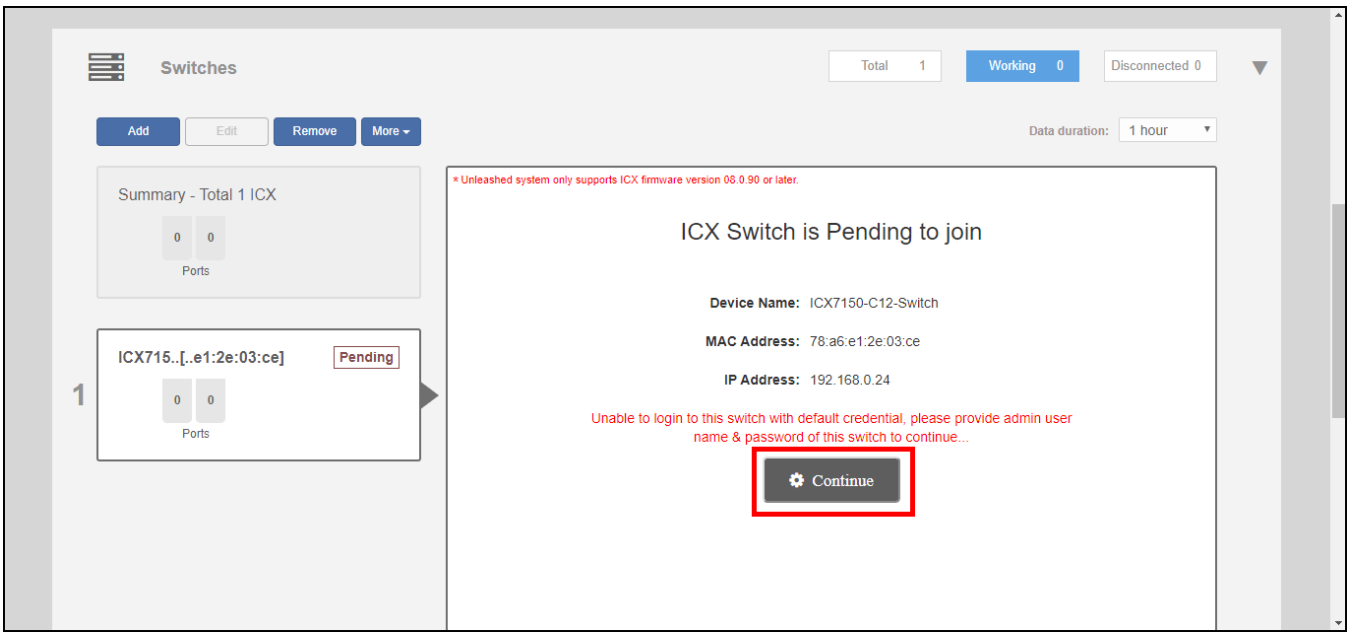
2. Click **Approve**. If the switch is in factory default state, it will automatically connect and be listed among the connected switch devices once the connection is established and the page is refreshed.

FIGURE 233 Click Approve



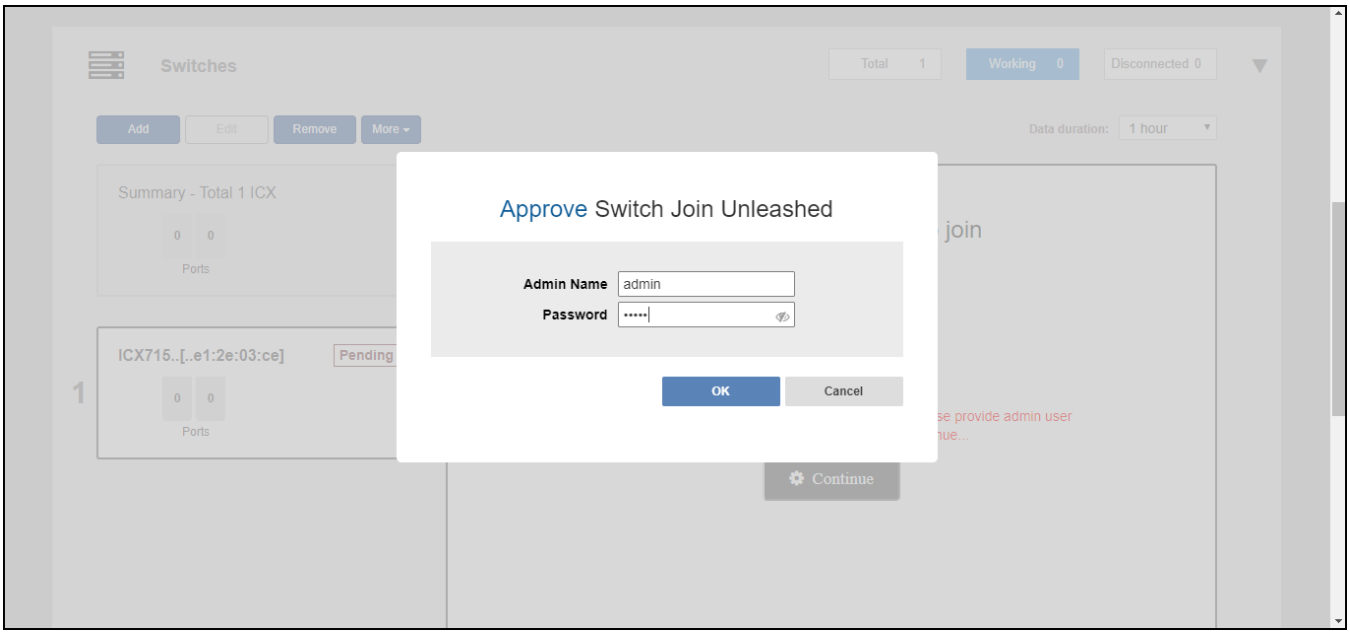
3. If the switch is not in factory default state, the Unleashed Master is unable to login using the default user name and password, and the following message appears. Click **Continue** to manually enter the login credentials.

FIGURE 234 Click Continue



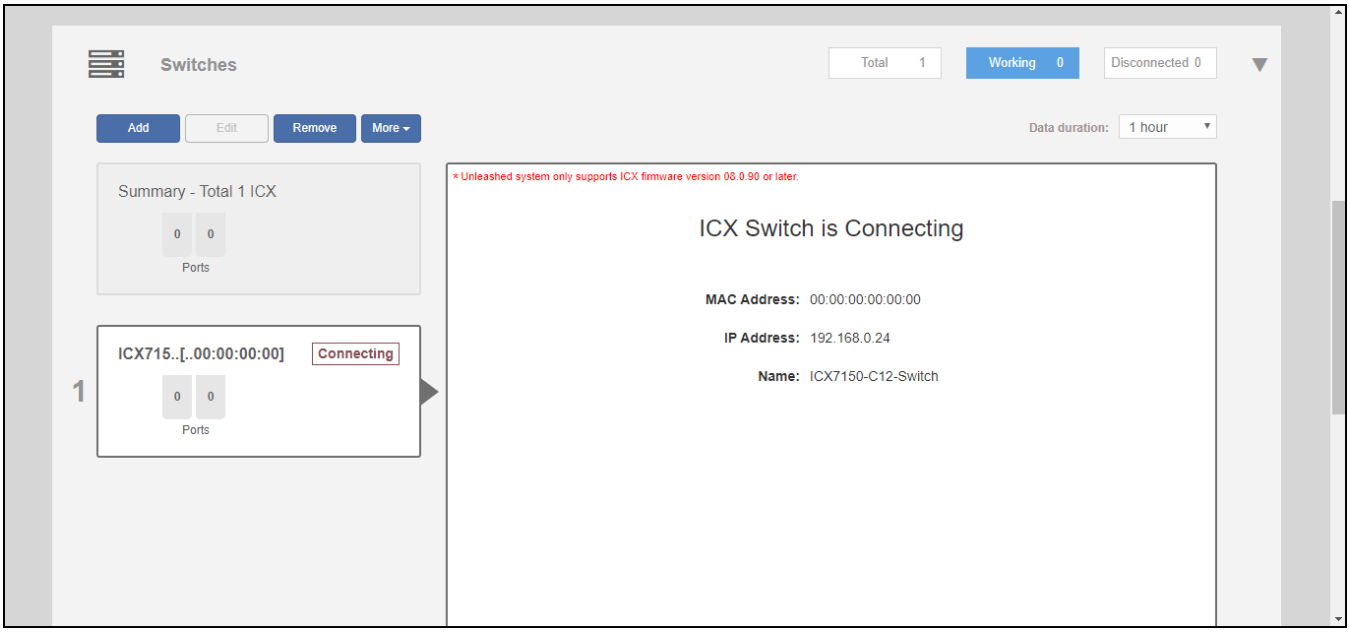
4. In the *Approve Switch to Join Unleashed* dialog that appears, enter the **Admin Name** and **Password** to authenticate to the switch.

FIGURE 235 Enter admin user name and password for switch authentication



5. Click **OK**. Unleashed immediately attempts to verify and approve the switch. If successful, the switch status will change to **Connecting** before joining Unleashed.

FIGURE 236 ICX switch connecting



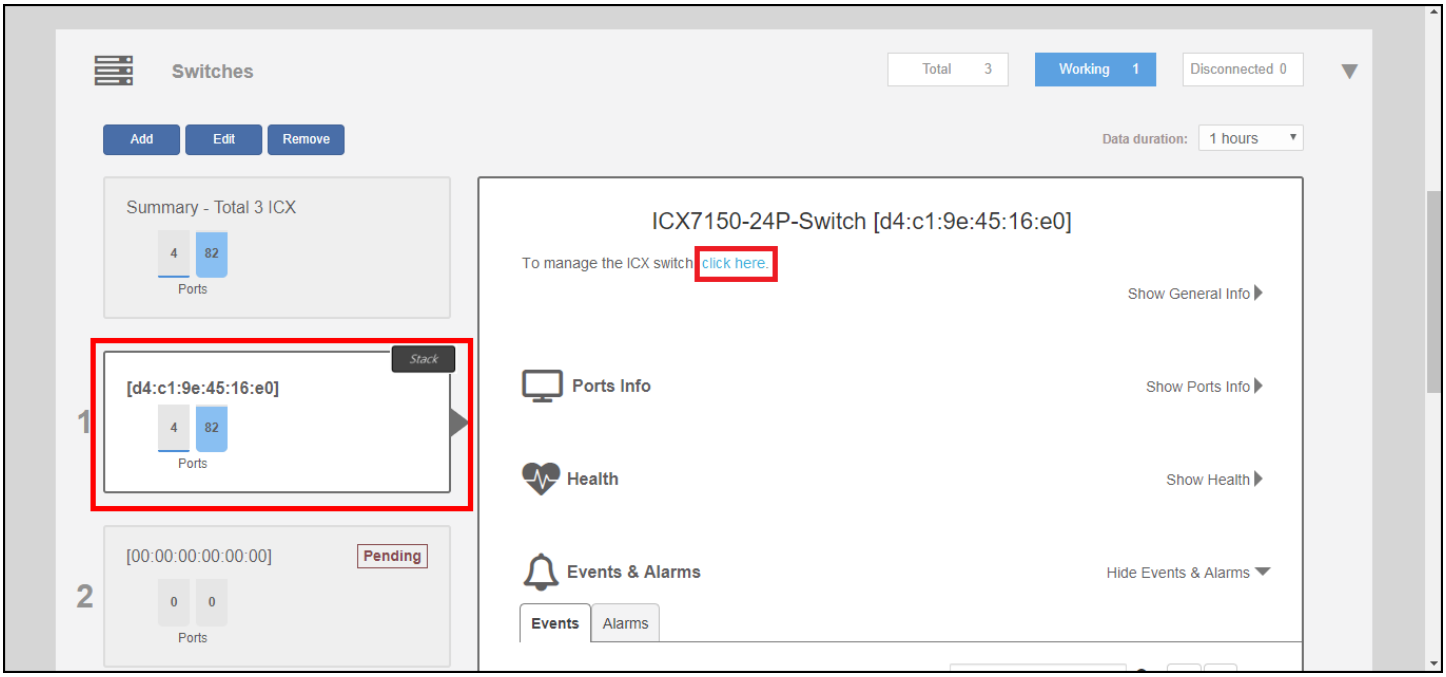
Monitoring Connected ICX Switches

Expand the **Switches** dashboard component and select a connected switch to view general information, port status, health details, and events and alarms on the selected switch.

The following details are displayed when the links are expanded:

- **General Info**: Displays general device information such as device name, IP address, MAC address, software version, and uptime.
- **Ports Info**: Displays the number of ports used and available, PoE power budget usage, and details on specific ports when selected from the port diagram or port list.
- **Health**: Displays hardware status information such as CPU and memory utilization.
- **Events & Alarms**: Displays a list of alarm and event system messages.

FIGURE 237 Selecting a Switch to Monitor Details

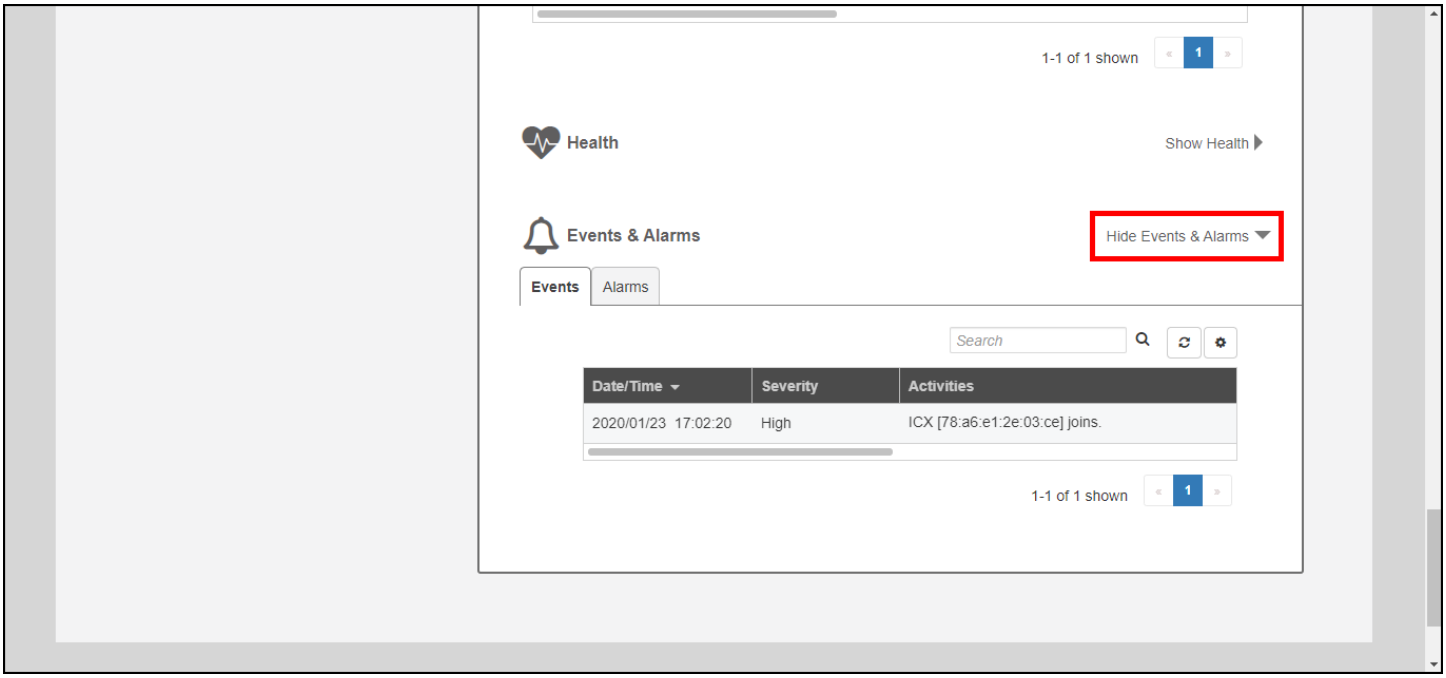


Click **Show Health** to view the switch's health status information, including CPU and memory utilization, power supply usage, and temperature details. Hover over a segment of the charts to view time-specific details.

FIGURE 238 Monitoring Switch Health Details

Click **Show Events & Alarms** to expand the section and view switch event and alarm lists.

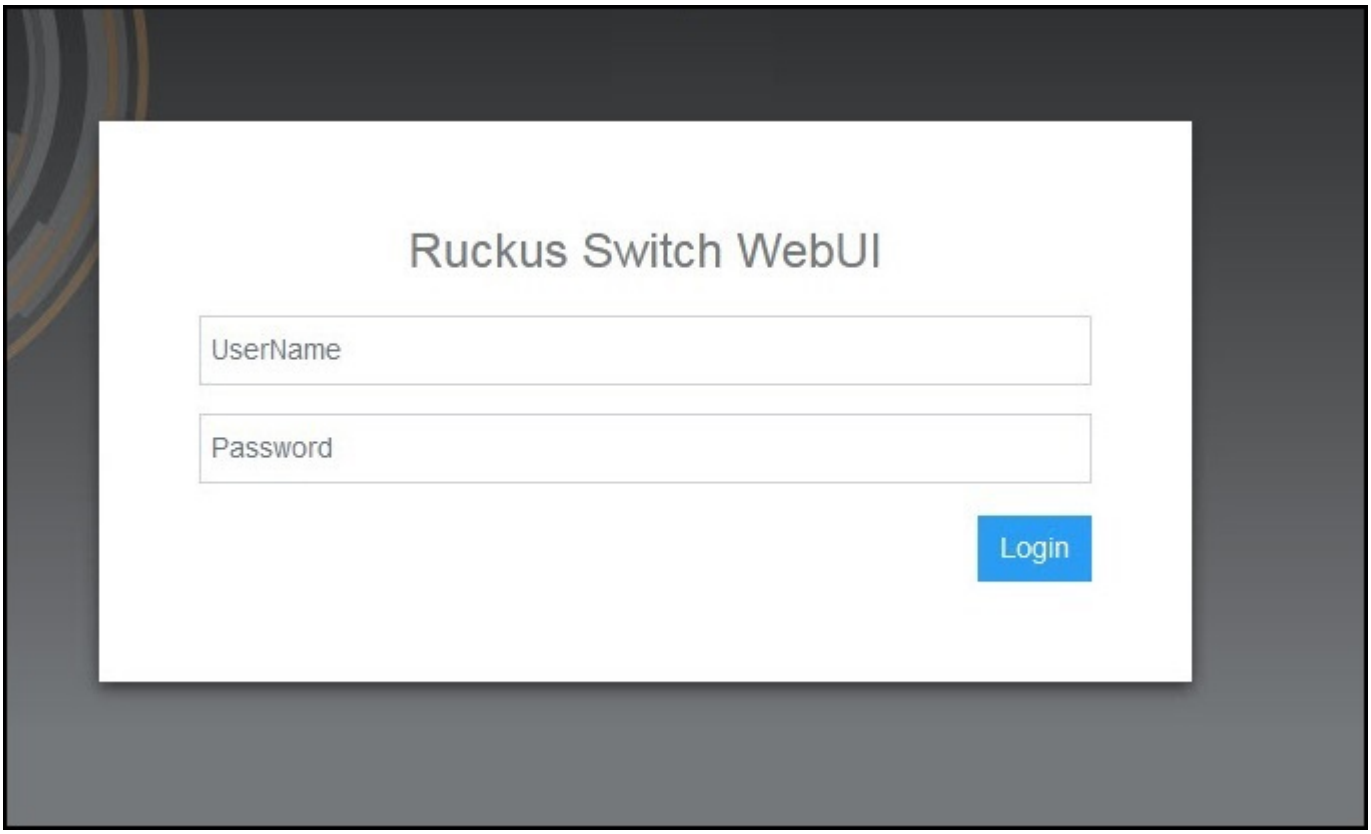
FIGURE 239 Viewing Switch Event and Alarm Lists



Accessing the RUCKUS Switch Home Page

To access the RUCKUS switch home page from within Unleashed without manual login, click the **To manage the ICX switch, click here** link. Enter the user name and password, and click **Login** to log in to the RUCKUS switch home page.

FIGURE 240 Logging In to the RUCKUS Switch Home Page



NOTE

- Access to the RUCKUS switch home page is supported only for ICX firmware version 9.0.0 or later.
- Access to the RUCKUS switch home page redirection is available only when an ICX switch is connected.
- You can extend the available redirection window time. The standard available redirection window time is 10 minutes.

Managing Switch Ports

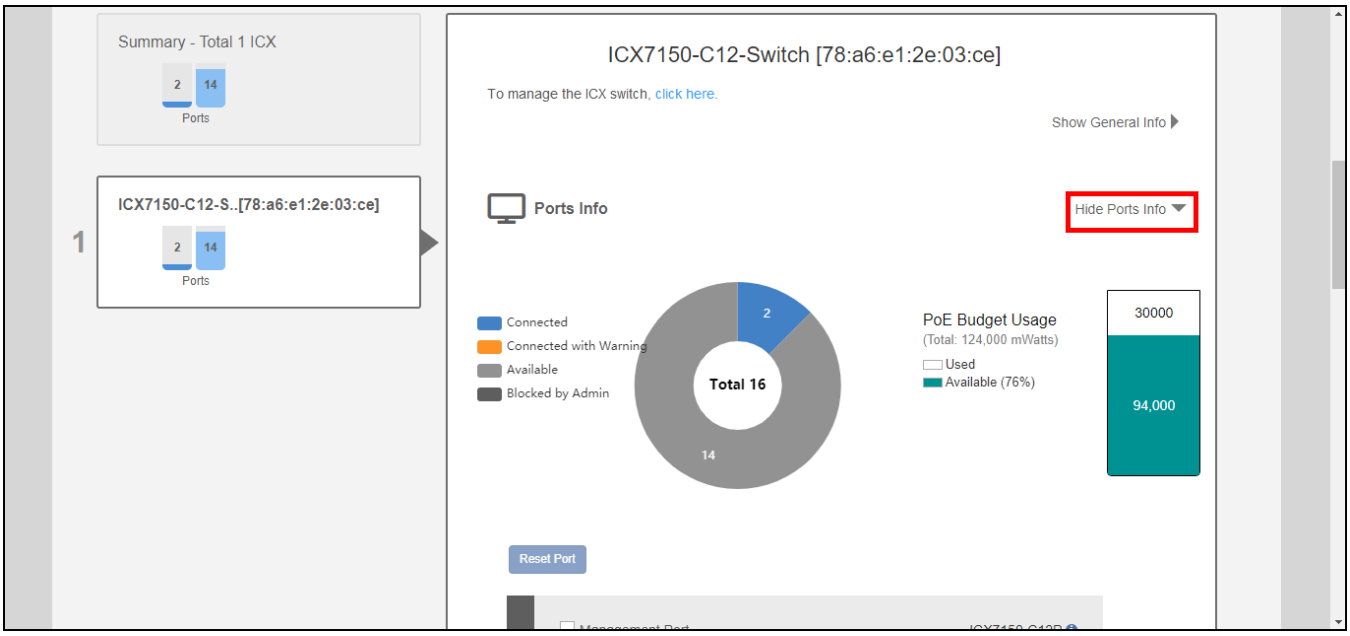
The "Ports Info" link expands to display information on overall switch status such as the number of ports used and available and PoE power budget usage. Individual switch ports can be managed by selecting the specific port from the switch port diagram or from the port list table below.

To manage ICX switch ports:

1. Expand the **Switches** dashboard component, and select a connected switch from the list on the left.

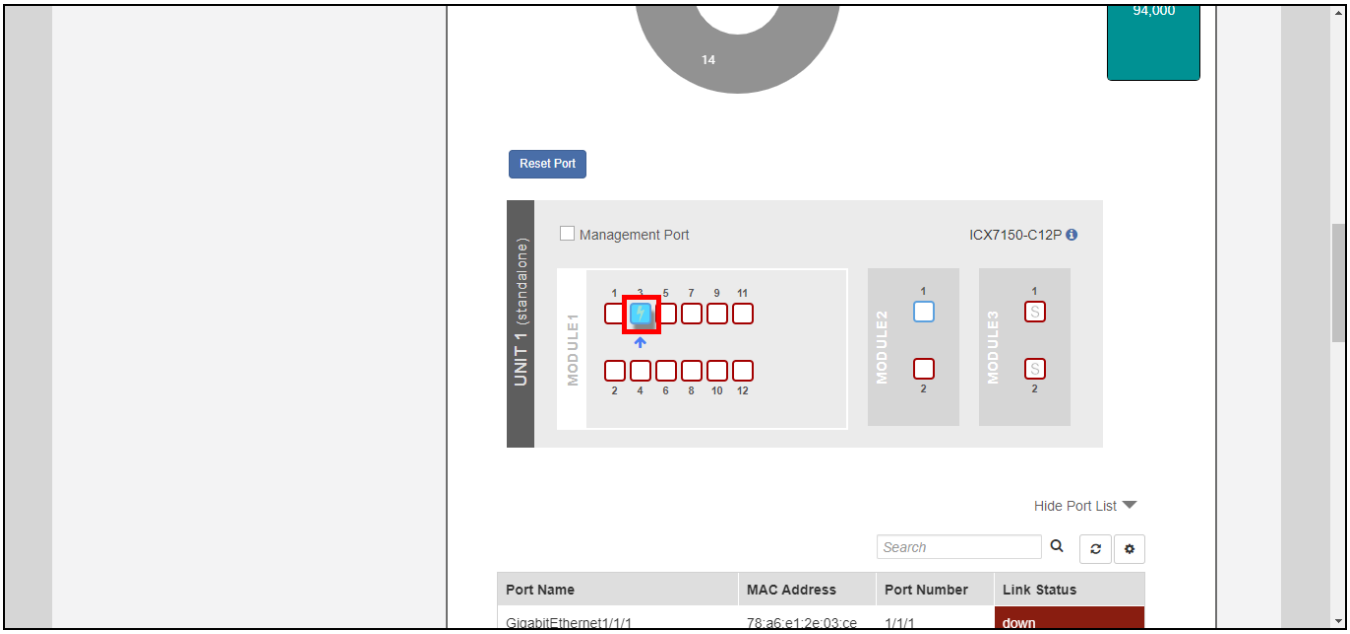
2. Click **Show Ports Info** to expand the port details view.

FIGURE 241 The "Ports Info" view displays summary info and per-port details



3. Select an individual port from the port diagram or port list table.

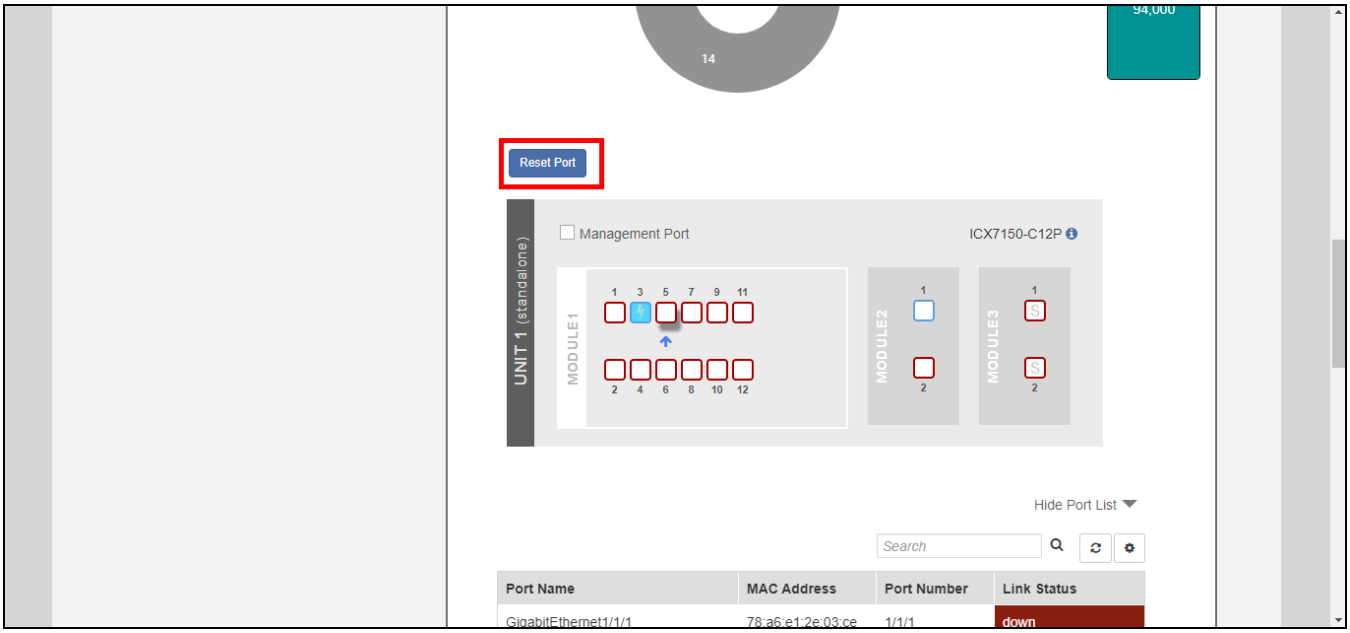
FIGURE 242 Select a switch port to display details on that port



4. Review the details in the switch port list for the port selected.

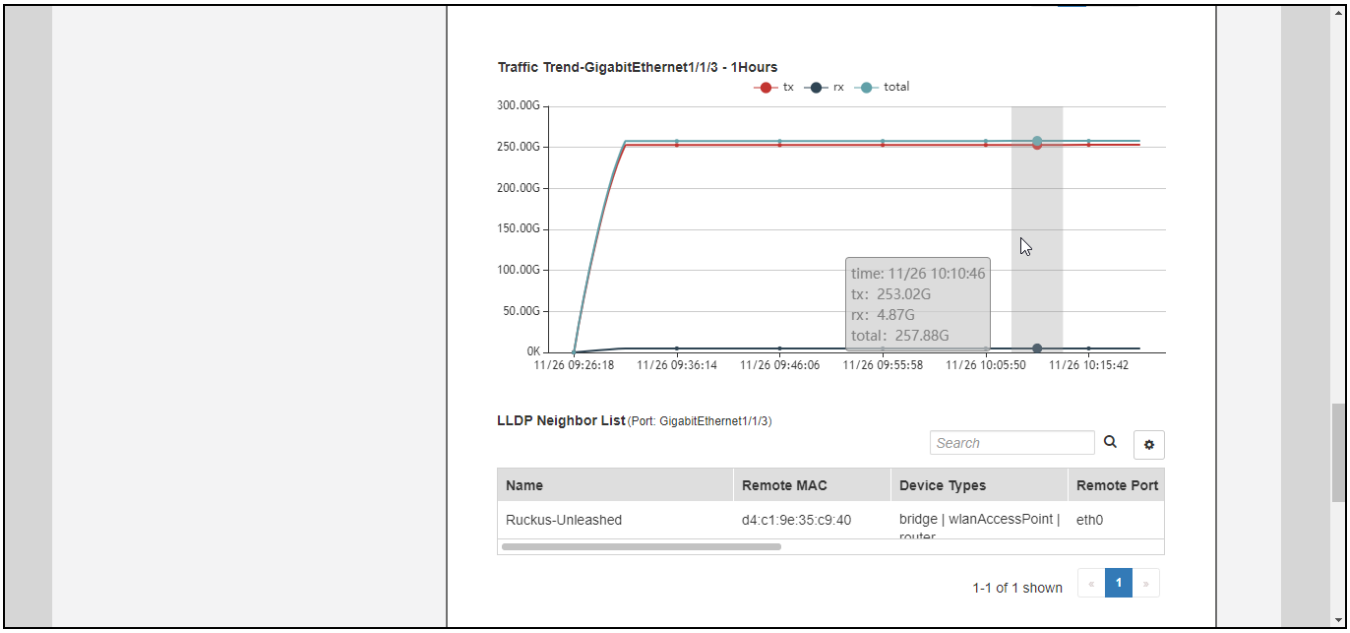
5. To reboot a device connected to a PoE switch port, click the **Reset Port** button. The port reset button can be used to power cycle a connected device by powering down and back up a PoE port.

FIGURE 243 Resetting a switch port



6. Scroll down to view the traffic trend chart and LLDP neighbor list for a port.

FIGURE 244 Viewing a port's traffic statistics and LLDP neighbors



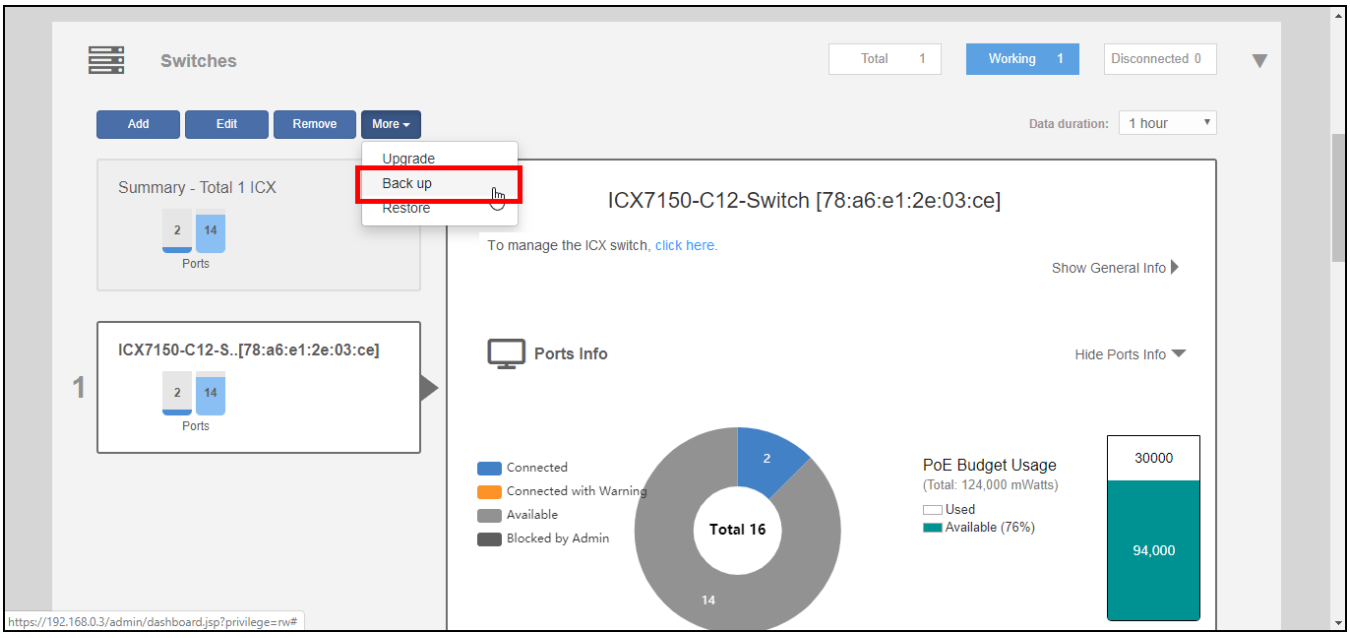
Backup and Restore Switch Configuration

Unleashed ICX switch management provides tools for performing a backup of current ICX switch configuration and restore to a previously saved configuration backup file.

Use the following procedure to perform a backup and restore of the current switch configuration:

1. Expand the *Switches* dashboard component and select a connected switch from the device list on the left.
2. Click **More > Back up**. The switch status displays *"Downloading"* as the configuration file is generated and prepared for download.

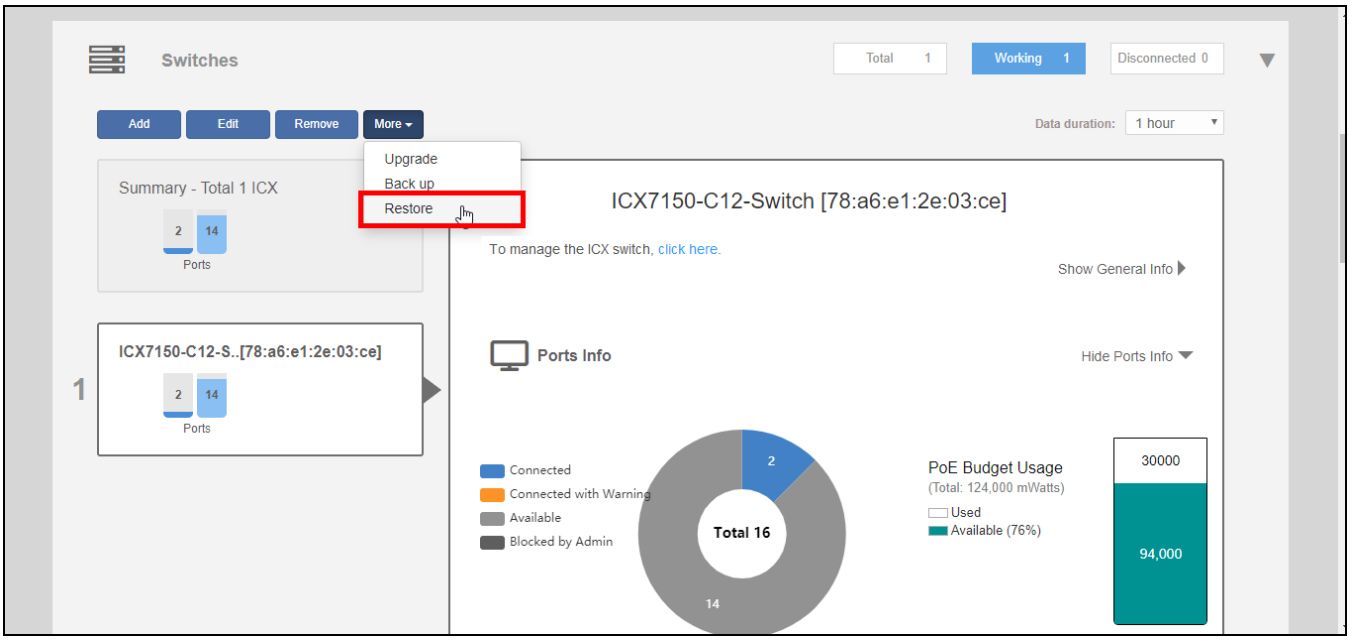
FIGURE 245 Backup Switch Configuration



3. When finished, the backup file is created as a .txt file that can be saved to your local computer.
4. Save the backup file to a convenient location.

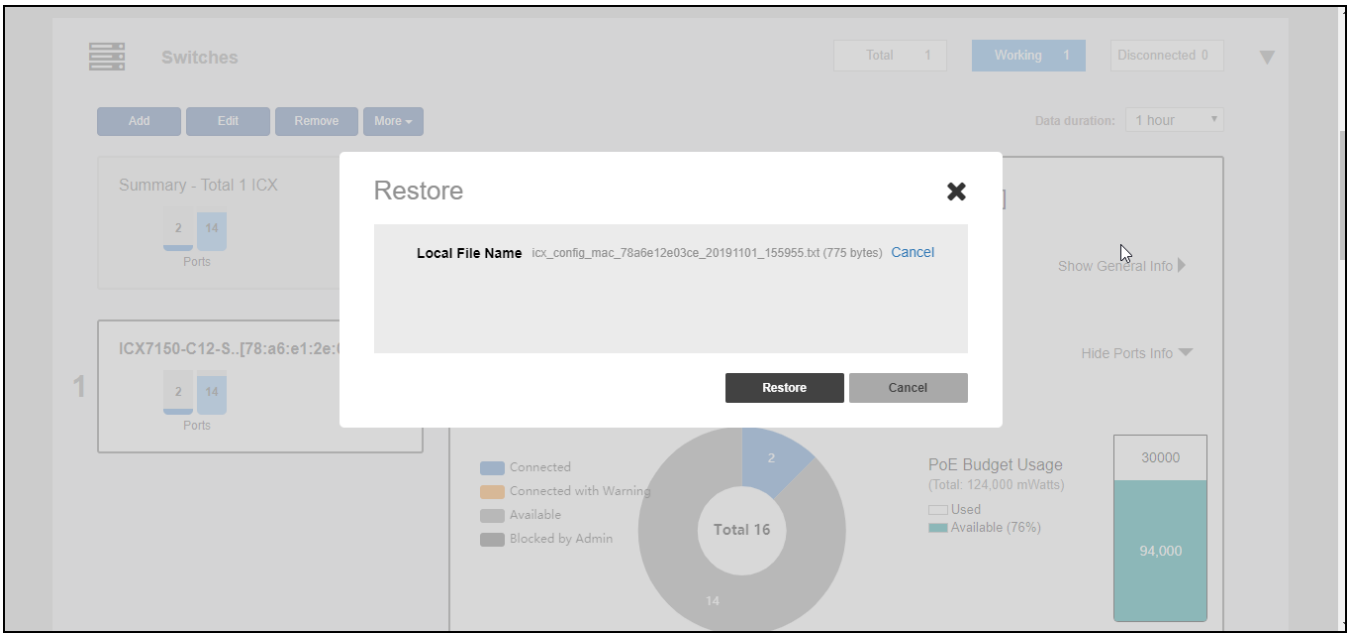
5. To restore configuration settings from a previously saved backup file, click **More > Restore**.

FIGURE 246 Restore Switch Configuration



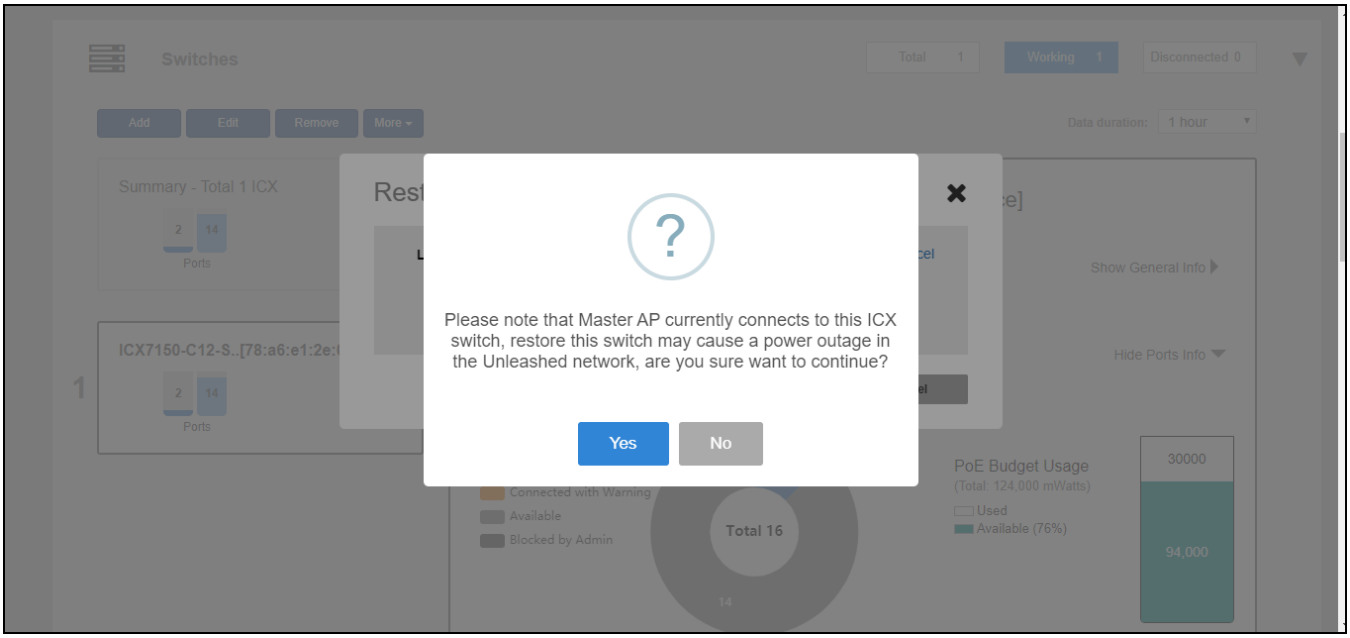
6. In the *Restore* dialog, click **Choose File** and select a valid backup file.
7. Click **Restore**.

FIGURE 247 Restore Configuration from Backup File



8. A warning message appears notifying you that the restore process will cause a power outage to the Unleashed network. Click **Yes** to confirm.

FIGURE 248 Switch Restore Warning

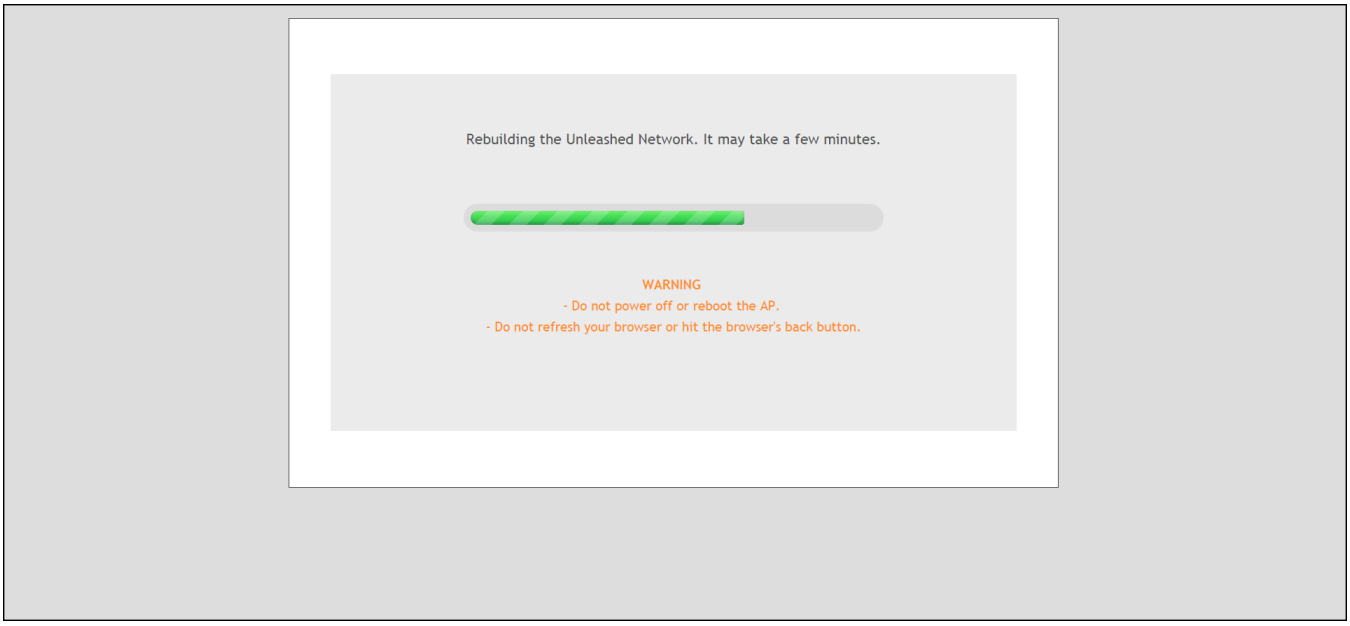


9. The *Switch restore in process* screen appears, notifying you that the restore process may take 10 minutes or more.

FIGURE 249 Switch Restore in Process

10. The *Rebuilding the Unleashed Network* screen appears, displaying a progress bar. Do not power off or reboot the AP, or refresh your browser or click the browser's back button.

    FIGURE 250 Rebuilding Unleashed Network



11. When the process is finished, the restored switch appears in the connected device list.

Upgrading ICX Switch Firmware

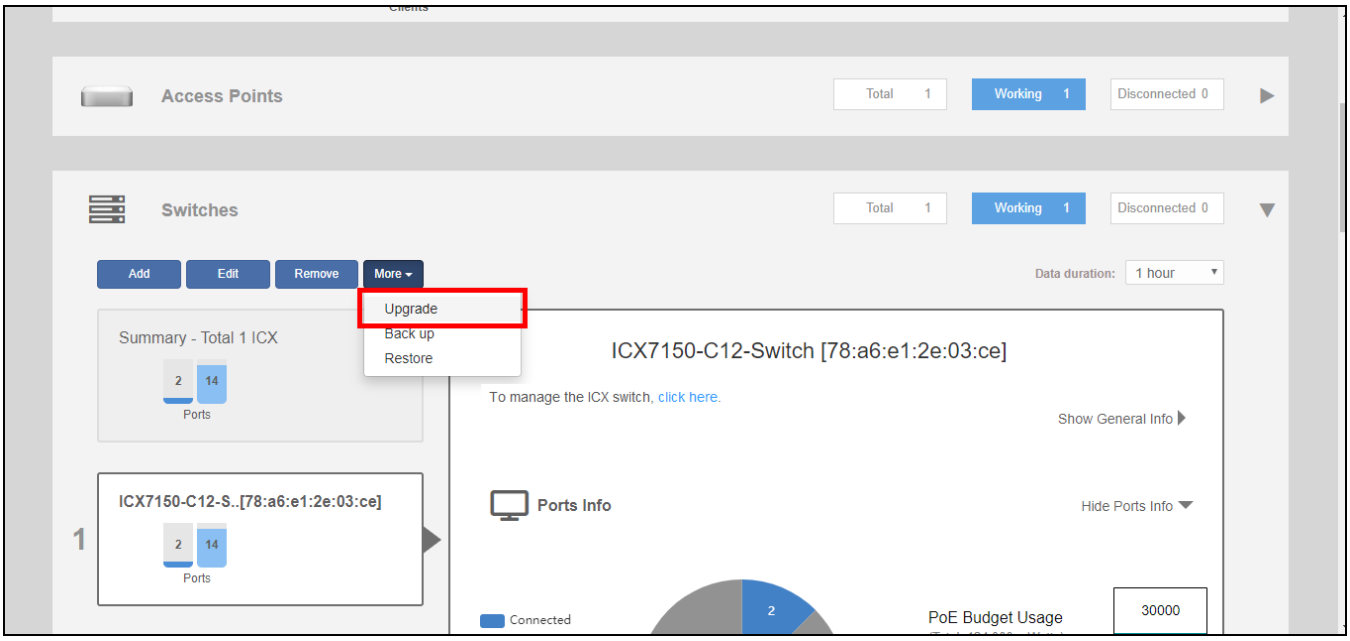
Unleashed management requires FastIron firmware version 08.0.90 or later.

To upgrade the firmware of an ICX switch, use the following procedure:

1. Expand the *Switches* dashboard component and select a connected switch from the connected device list on the left.

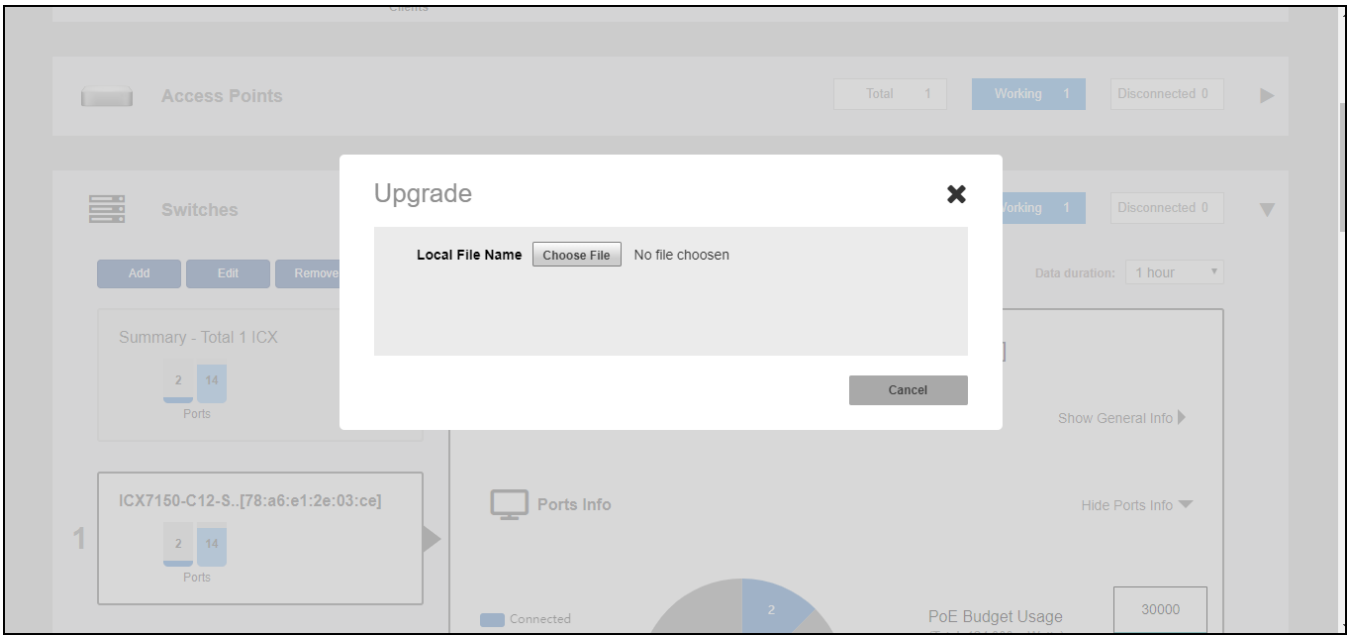
2. Click **More > Upgrade**.

FIGURE 251 Upgrading an ICX switch



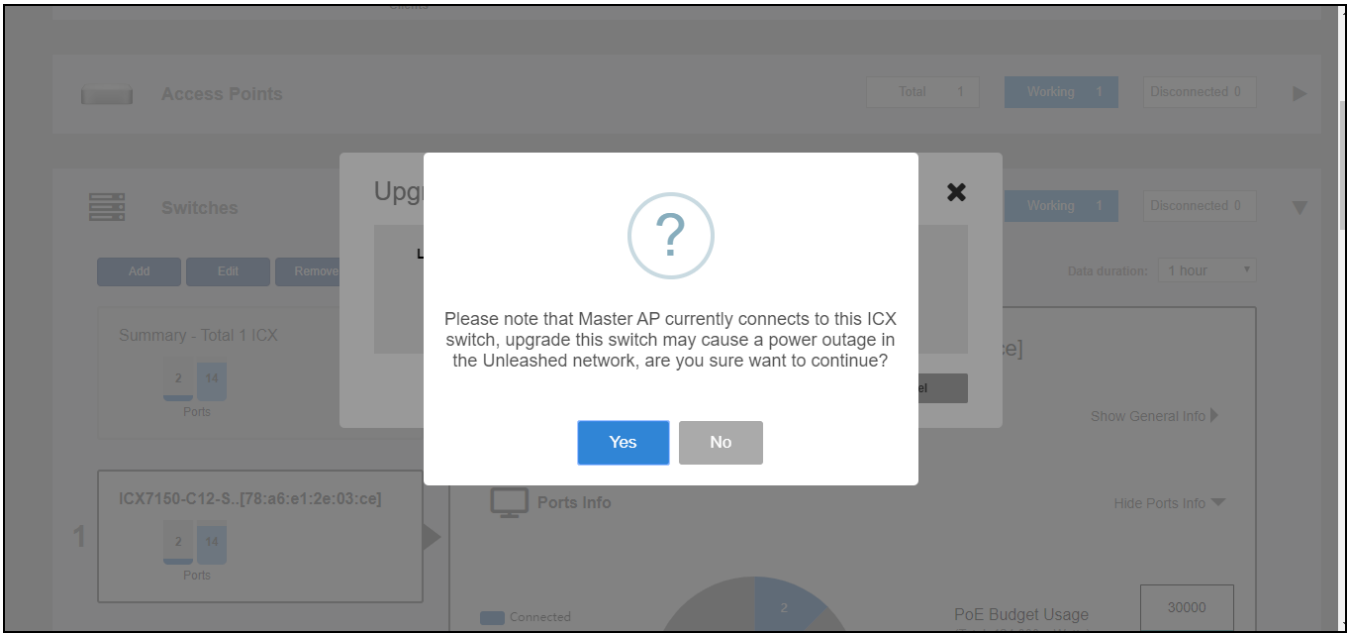
3. In the *Upgrade* dialog, click **Choose File** and select a valid FastIron image file.

FIGURE 252 Choose upgrade image file



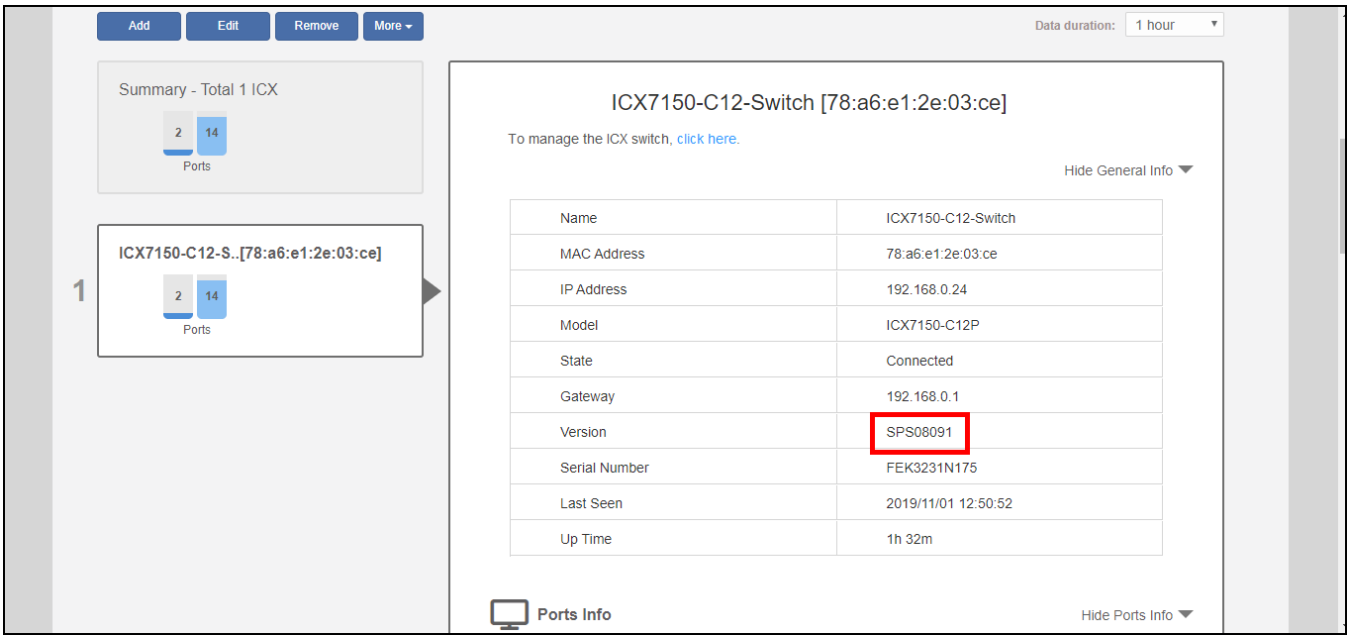
4. Click **Upgrade**. A warning message appears notifying you that the upgrade will cause a power outage to your Unleashed APs. Click **Yes** to continue.

FIGURE 253 Upgrade warning message



5. When the upgrade is complete, Unleashed reboots and displays the switch in the connected device list.
6. Verify the new firmware version from the **Show General Info** display.

FIGURE 254 Verify switch version



Working with Clients

- Client Management Overview....351
- Viewing the Clients List....351
- Renaming a Client....353
- Deleting a Client....355
- Permanently Blocking a Client Device....355
- Marking a Client as a Favorite....356
- Running a SpeedFlex Performance Test on a Wireless Client....357
- Client Connection Troubleshooting....361
- Marking a Client as a Legacy Device....363
- Adding User Accounts to the Internal User Database....363
- Authenticating Clients Using an External Database....364

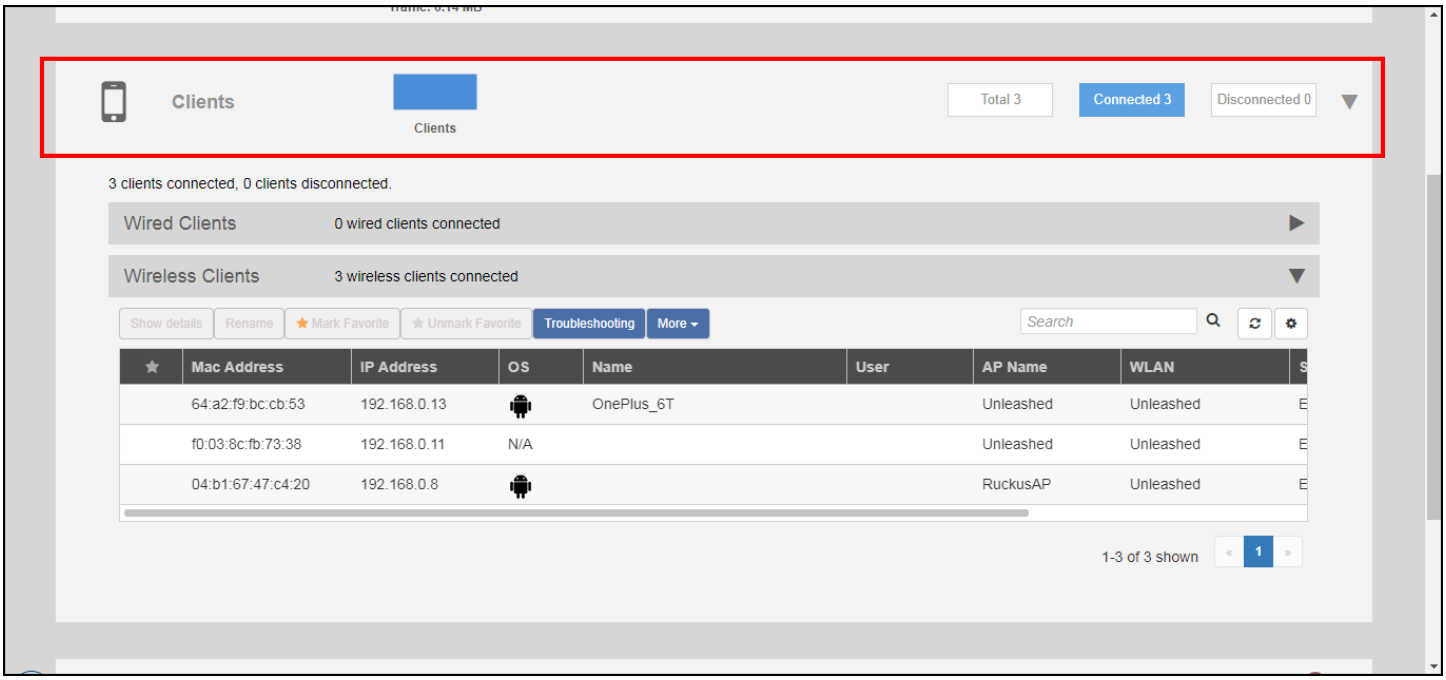
Client Management Overview

The Unleashed Admin Interface provides tools for monitoring and managing wireless clients, including blocking and deleting client devices, viewing an overview of client traffic, and drilling down into details about a specific client's connection status and traffic statistics.

Viewing the Clients List

To view a list of currently connected wireless clients, expand the **Clients** section on the **Dashboard**.

FIGURE 255 Viewing the currently connected Clients list



The clients list displays the number of connected and blocked clients, along with a table that lists the details on the client such as its MAC address, IP address, OS, Hostname, User, connected AP, WLAN, and Signal level indicator.

To view additional details about a specific client, select the client from the list and click **Show Details**.

FIGURE 256 Click Show Details to view client details

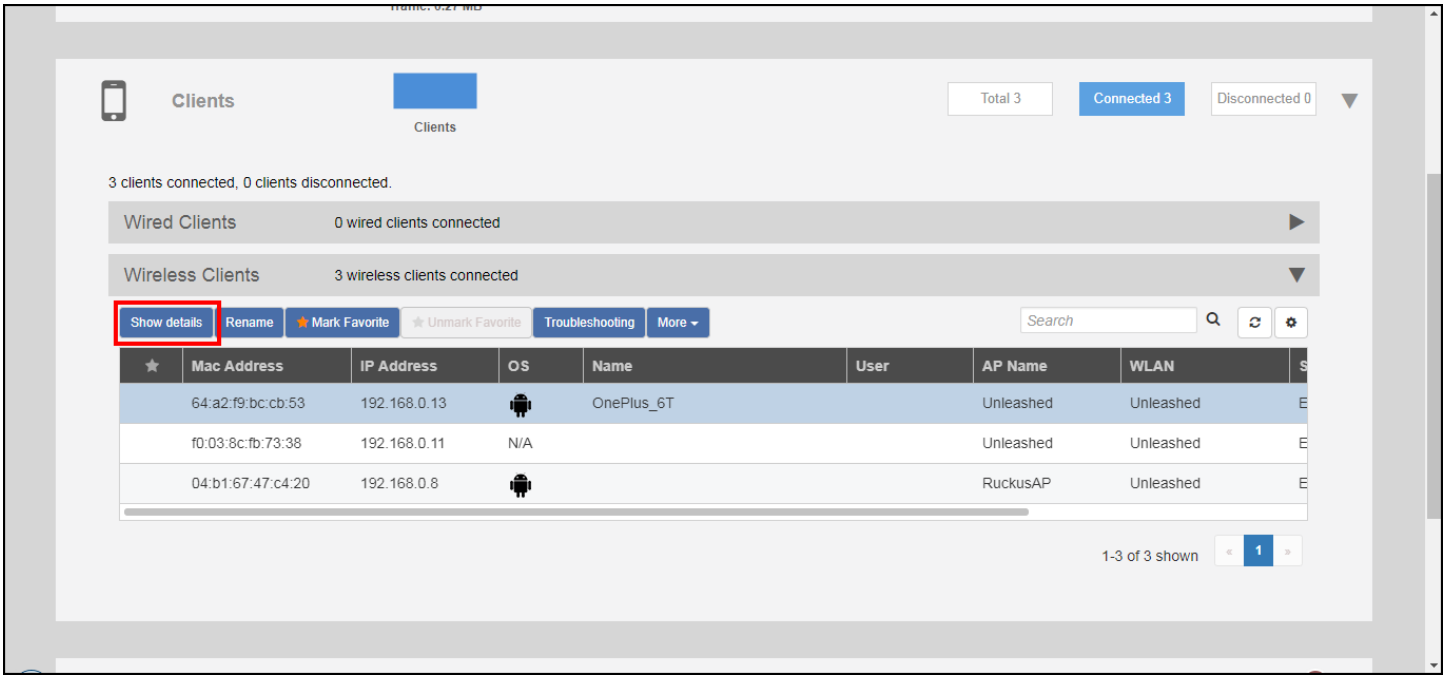
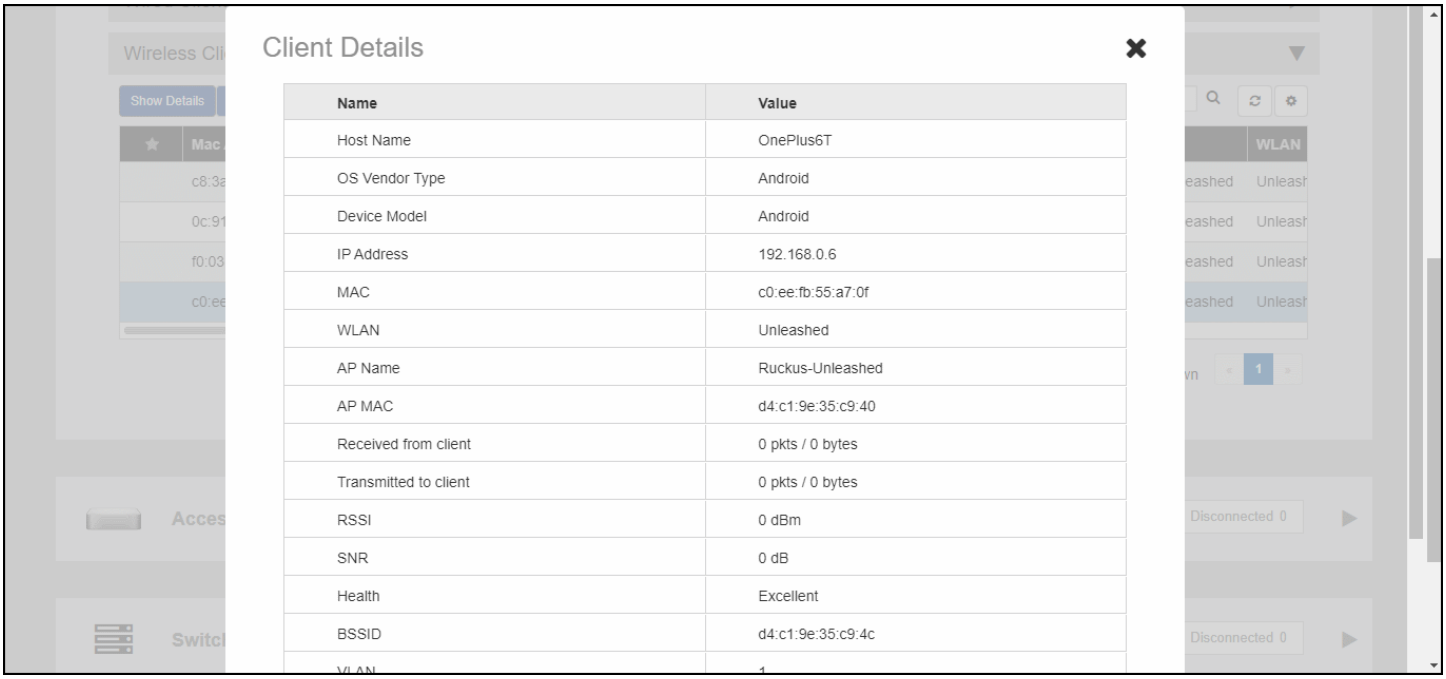


FIGURE 257 Viewing details on a specific client



Renaming a Client

Unleashed collects client host names from the client's operating system and displays them in client lists, tables and charts on the web interface. However, the host names provided by the OS are often not very useful in identifying clients on the network.

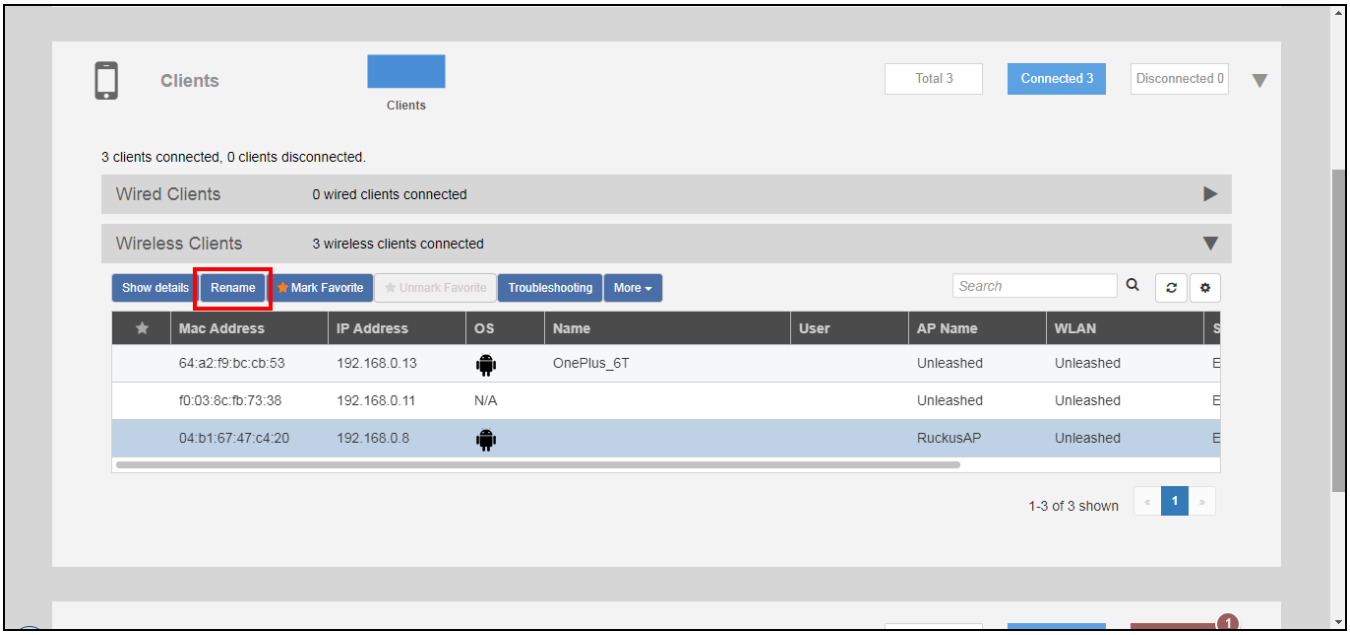
Entering a custom host name manually via the web interface is one way to address this issue.

Any renamed clients will be displayed using the new name whenever they are online. The maximum number of marked clients is 520. When this max is reached, Unleashed will delete the oldest renamed offline stations, 10 stations at a time, and trigger an alarm event to indicate the renamed stations have been deleted.

To rename a connected wireless client:

1. Open the **Clients** component, and select the client you want to rename from the list.
2. Click **Rename**.

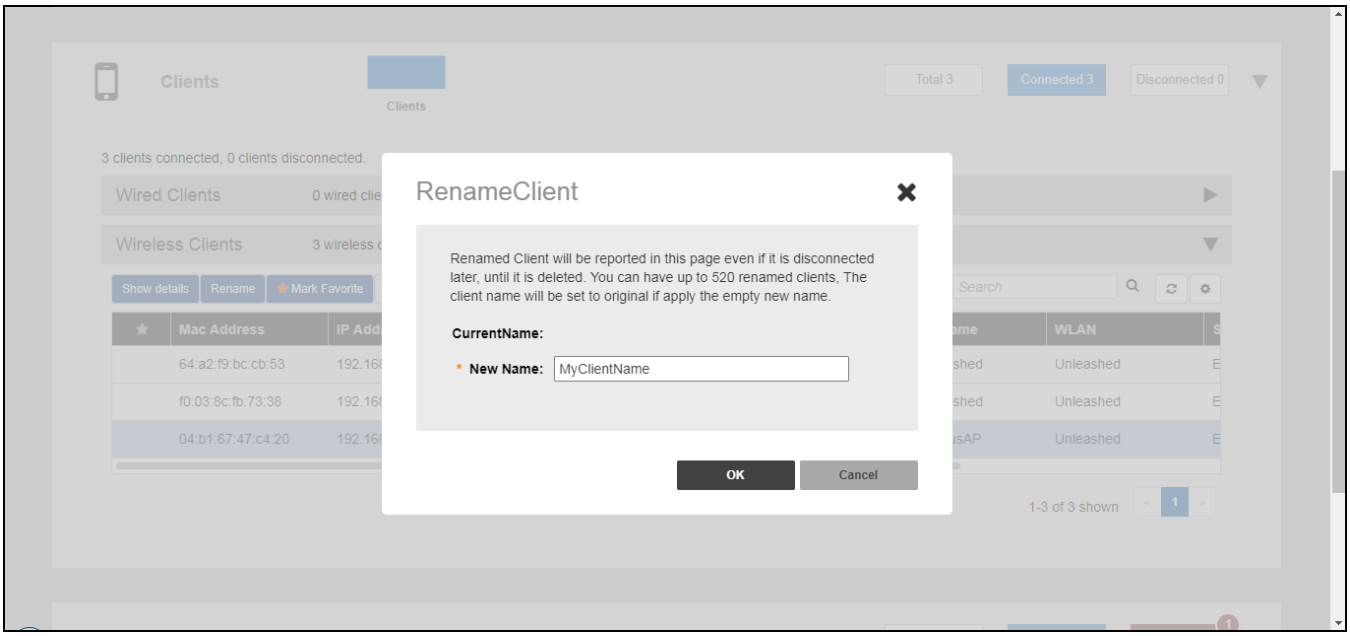
FIGURE 258 Rename a client



The *Rename Client* dialog appears.

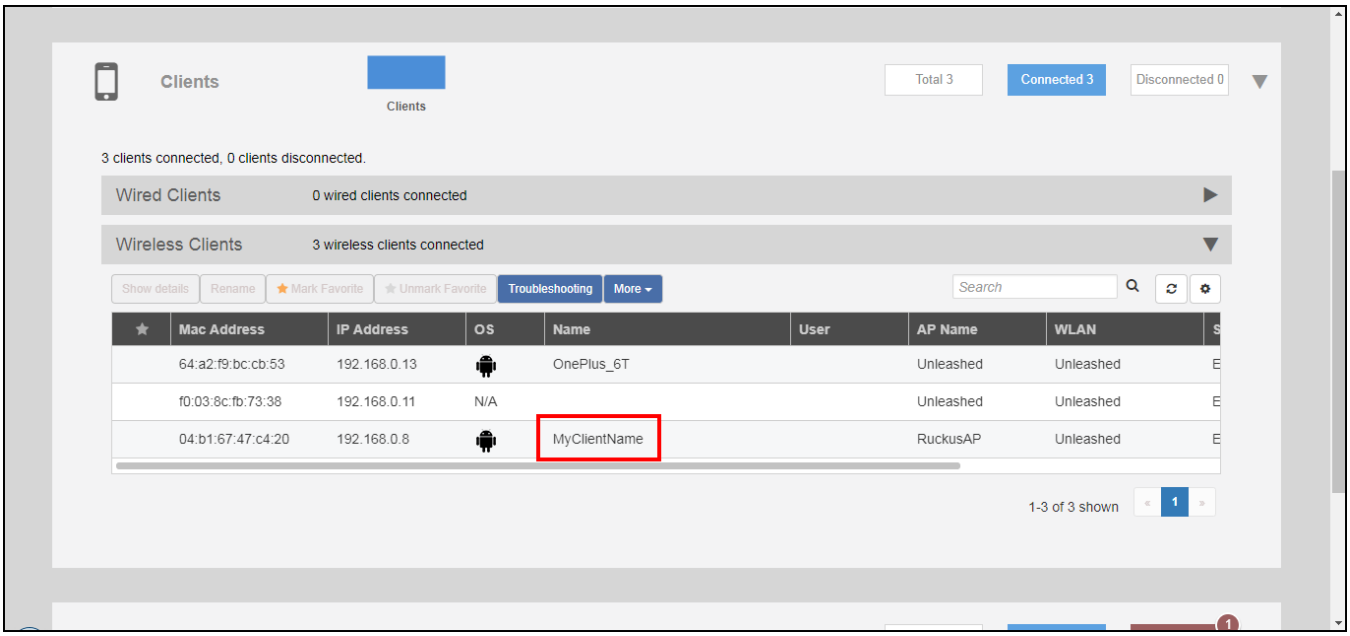
3. Enter the **New Name**, and click **OK**.

FIGURE 259 Enter new client name



4. The new client name now appears in clients lists in the *Host Name* column.

FIGURE 260 New name appears in Host Name

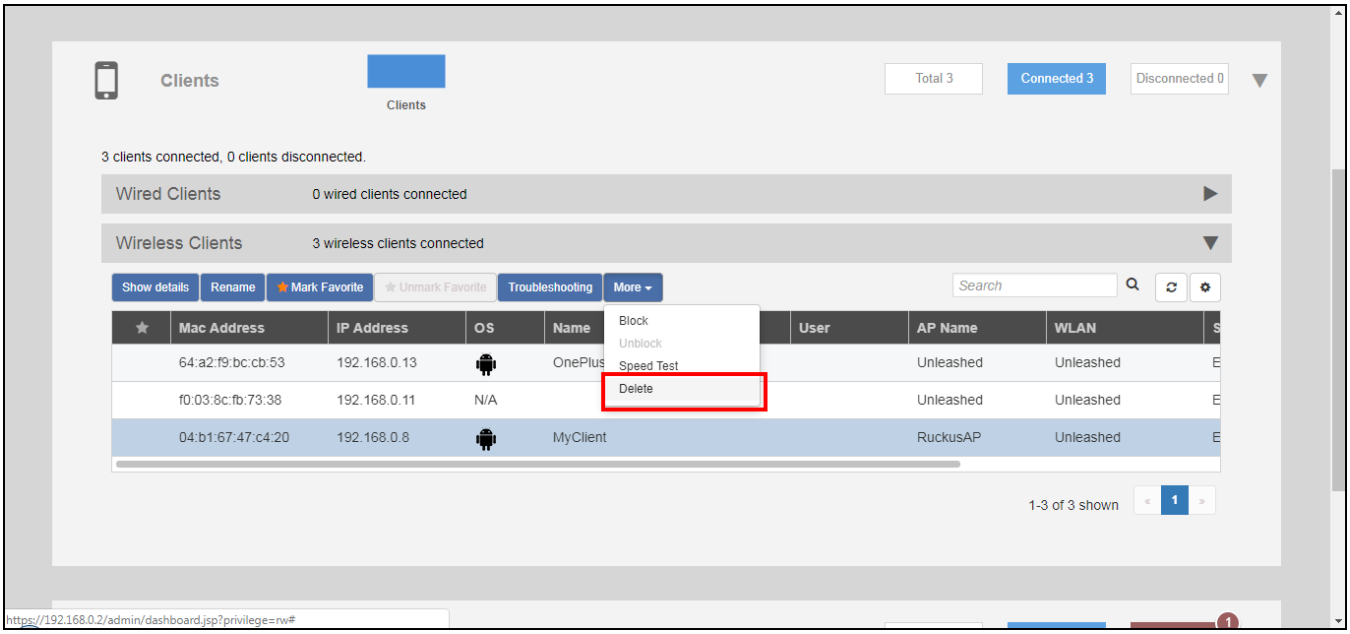


Deleting a Client

Follow these steps to temporarily disconnect a client device from your WLAN. (The user can simply reconnect manually, if they prefer.) This is helpful as a troubleshooting tip for problematic network connections.

1. Expand the **Clients** component on the Dashboard.
2. Select a client from the list, and click **Delete**.

FIGURE 261 Click the Delete button to temporarily delete a client. The client will be able to reconnect.



The entry is deleted from the Active Clients list, and the listed device is disconnected from your WLAN.

The user can reconnect at any time, which, if this proves to be a problem, may prompt you to consider Permanently Blocking a Client Device on page 355.

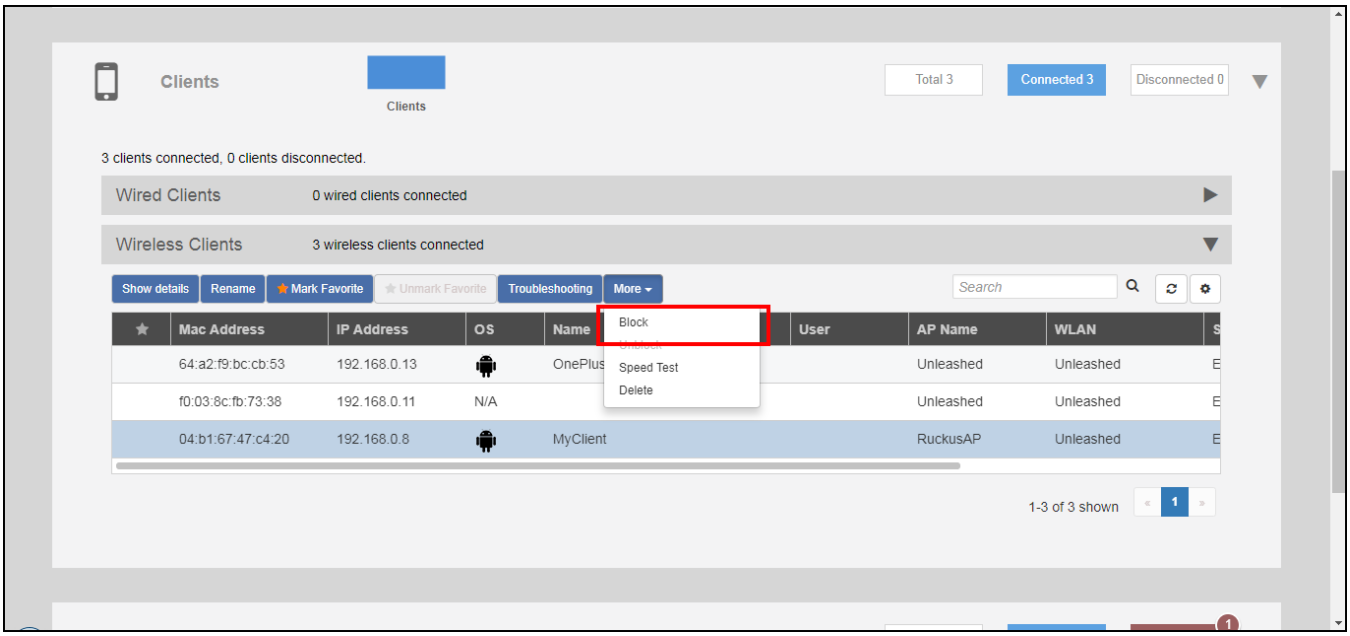
Permanently Blocking a Client Device

Complete the following steps to permanently block a client device from WLAN connections.

1. Expand the **Clients** component on the dashboard.
2. In the **Status** column of the clients list, identify any unauthorized users.

3. Select an AP from the list, and click the **Block** button from the **More** pull-down menu to move this client to the blocked clients list.

FIGURE 262 Blocking a Client Permanently



The status of the client is changed to **Blocked**, preventing the listed device from using your RUCKUS WLANs.

Marking a Client as a Favorite

Designating a client as a "favorite" client provides a way to monitor the client's behavior, triggering a report when the client goes online or offline.

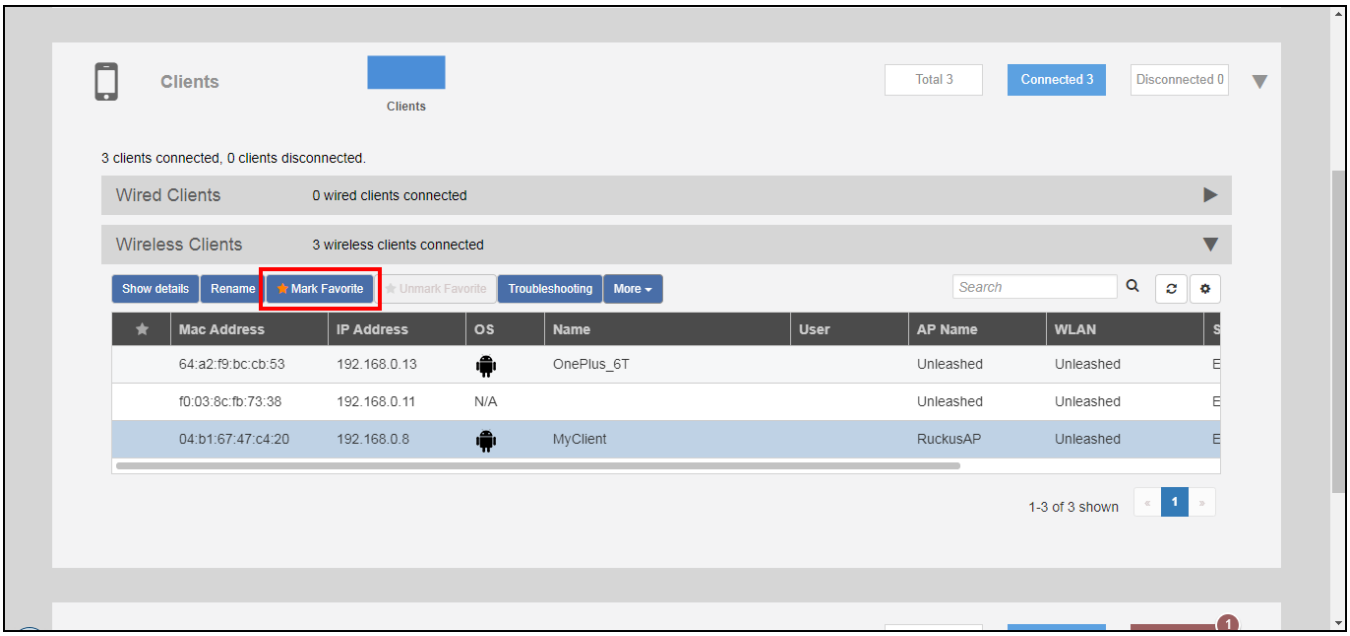
NOTE
Unleashed supports a maximum of 20 favorite clients.

To mark a client as a favorite, use the following procedure:

1. Expand the **Clients** component on the Unleashed Dashboard.

2. Select a client from the list, and click **Mark Favorite**.

FIGURE 263 Mark Favorite



An alarm event will be generated each time this client goes online or offline.

Running a SpeedFlex Performance Test on a Wireless Client

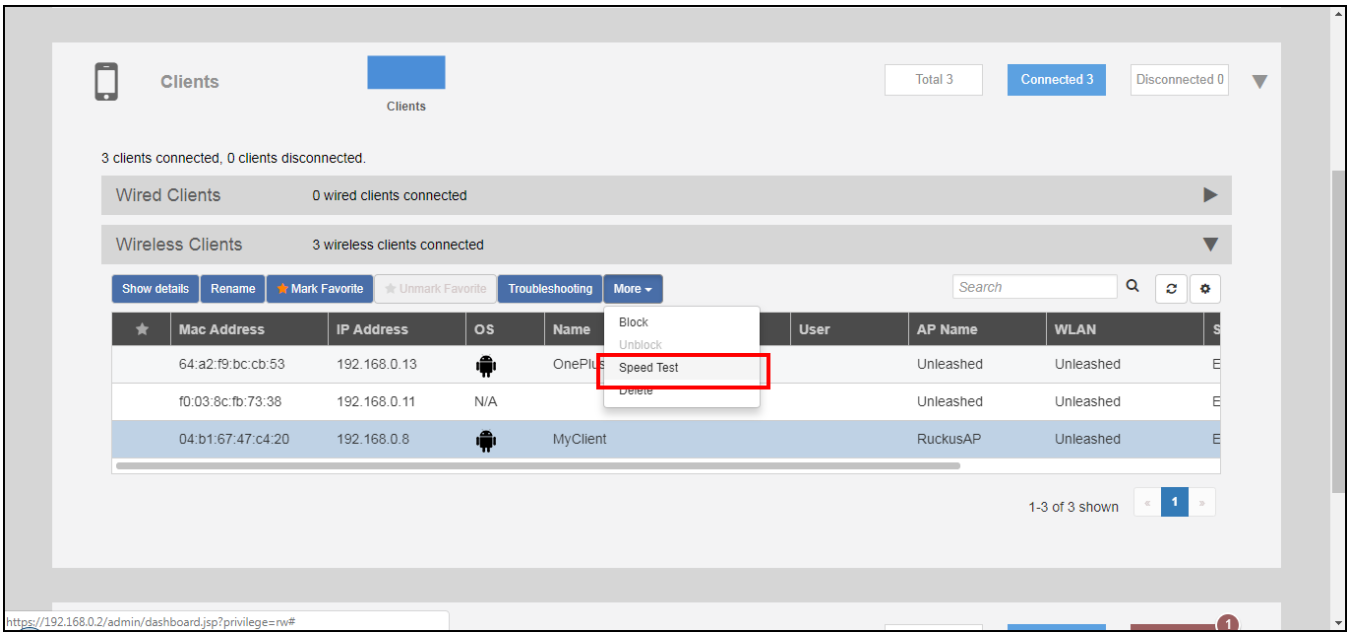
You can test the wireless throughput to a client using the SpeedFlex tool.

To do so, you will need to install and run the SpeedFlex application on the client device.

1. Expand the **Clients** menu.

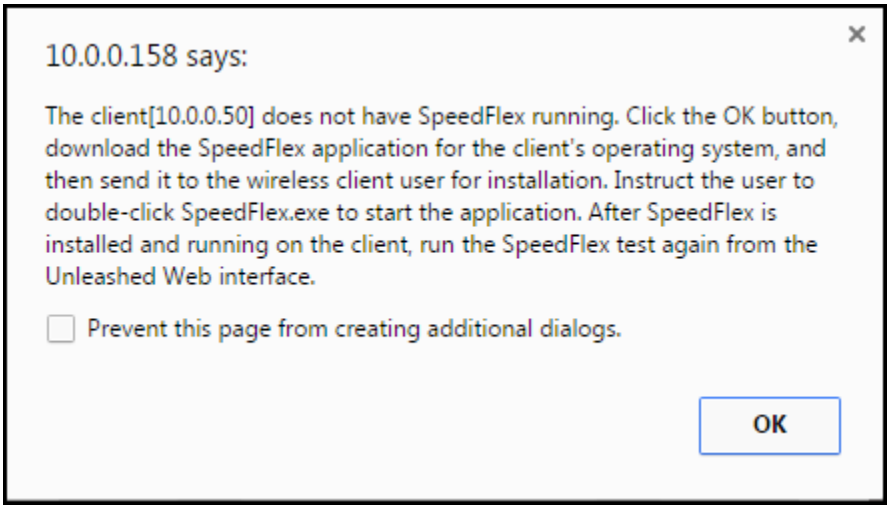
2. Select a client device from the list and click **Speed Test** from the **More** pull-down menu.

FIGURE 264 Select a client and click Speed Test



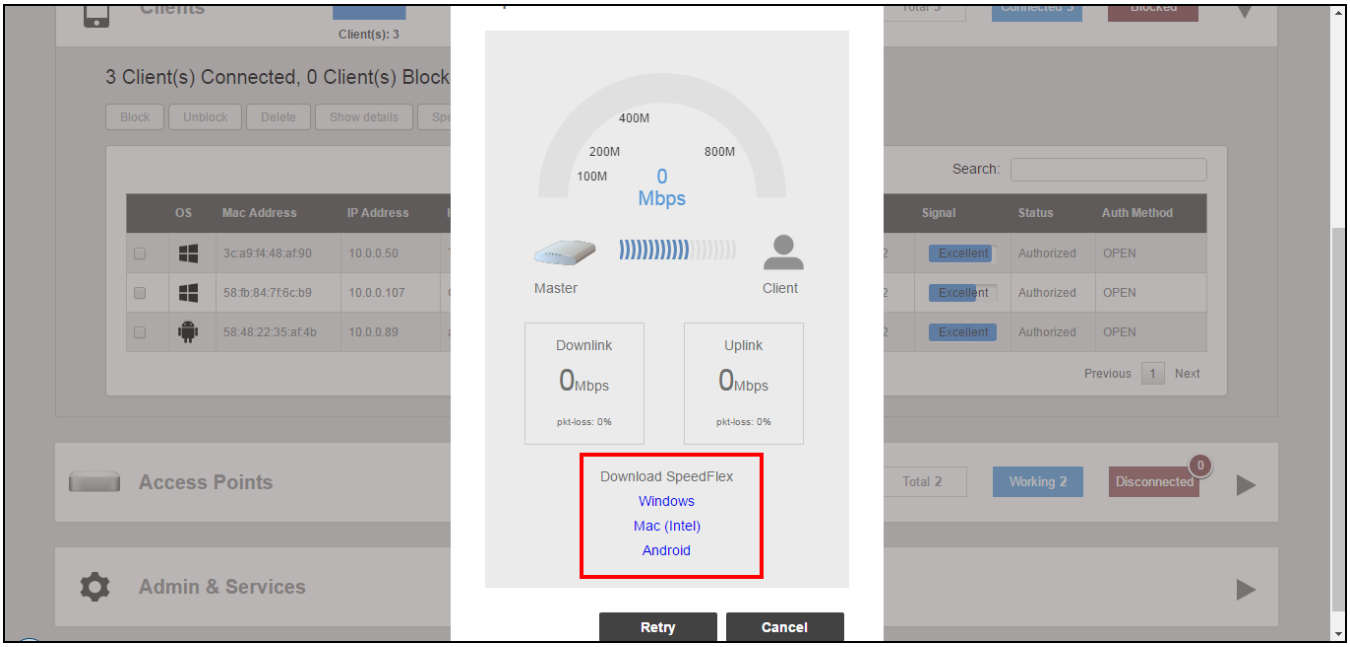
3. A Speed Test dialog appears. Click **Start** to begin.
4. If the SpeedFlex application is not already running on the client, follow the instructions to install and run the application on your client device.

FIGURE 265 The client does not have SpeedFlex running



5. Download the SpeedFlex application for your Operating System. Choices are:
   - Windows
   - Mac (Intel)
   - Android

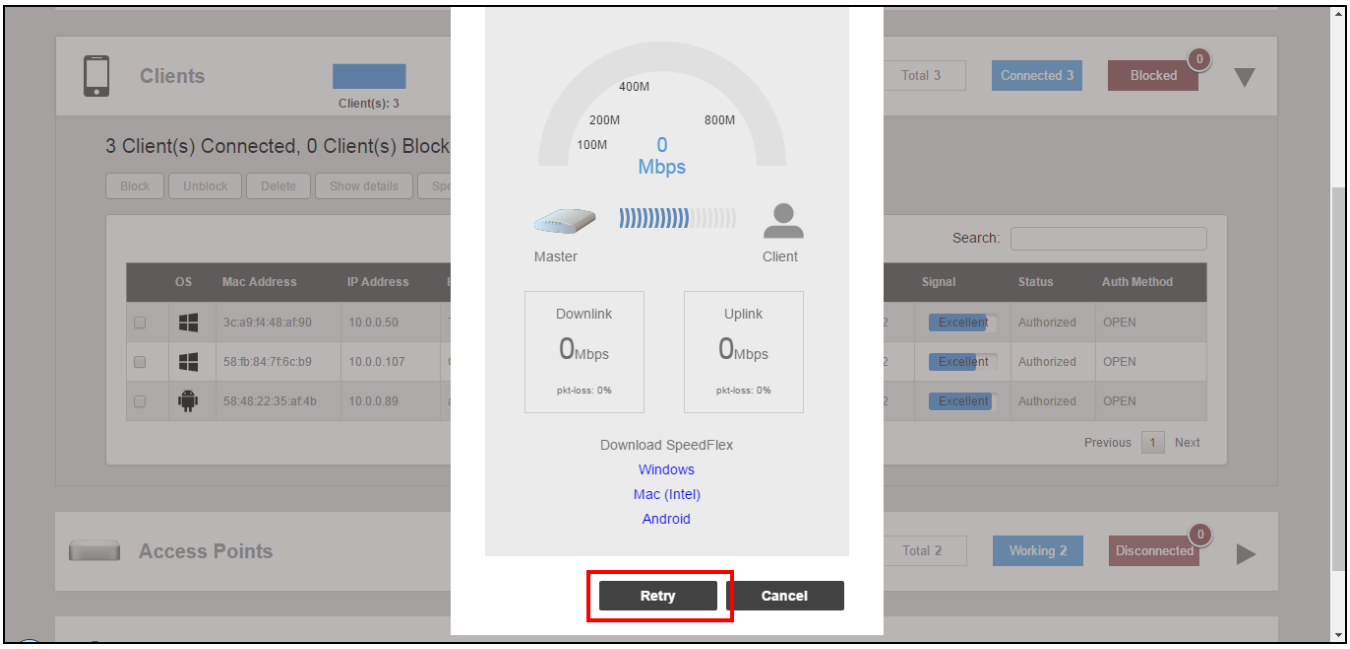
FIGURE 266 Download SpeedFlex



6. Install and run the application.

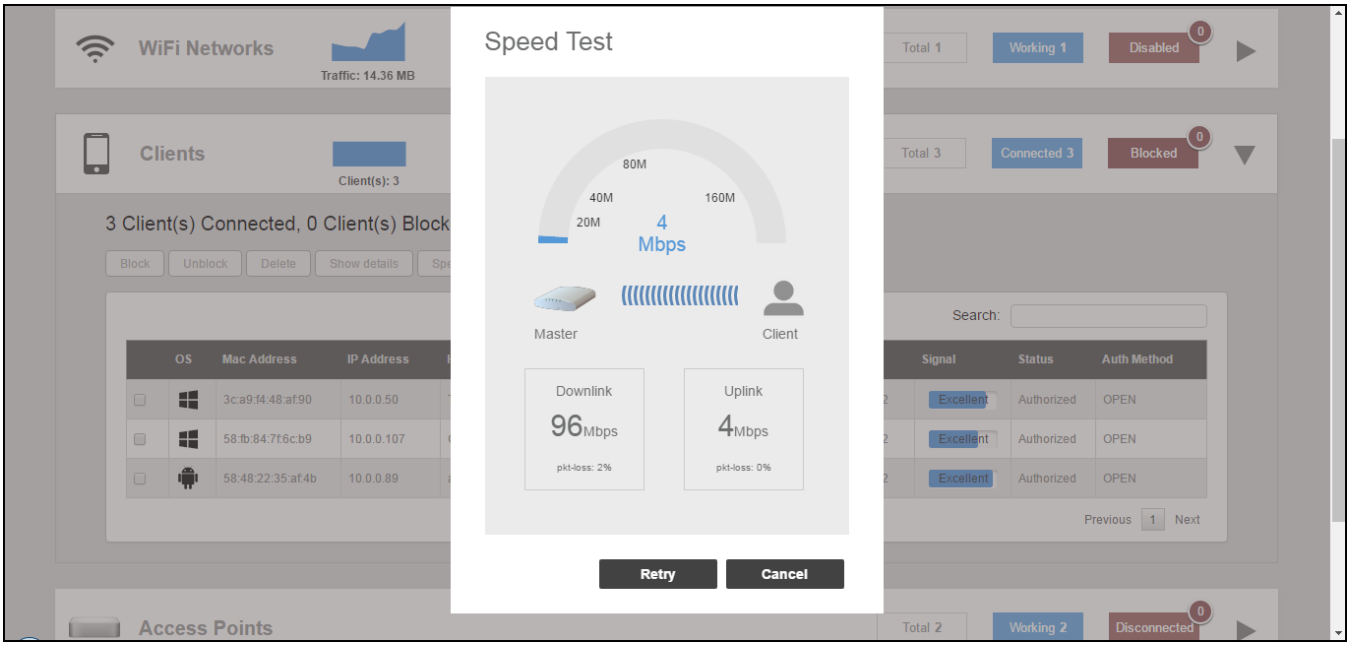
7. With the application running, click **Retry**.

FIGURE 267 Click Retry



8. When the test is complete, the average Downlink and Uplink speed results are displayed along with packet loss percentages.

FIGURE 268 SpeedFlex results



Client Connection Troubleshooting

The client connectivity trace feature is designed to help customers diagnose wireless client connection issues to determine why a client fails to connect to the wireless network.

To perform a client connectivity trace:

1. Open the **Clients** section, and select the problematic client from the list.

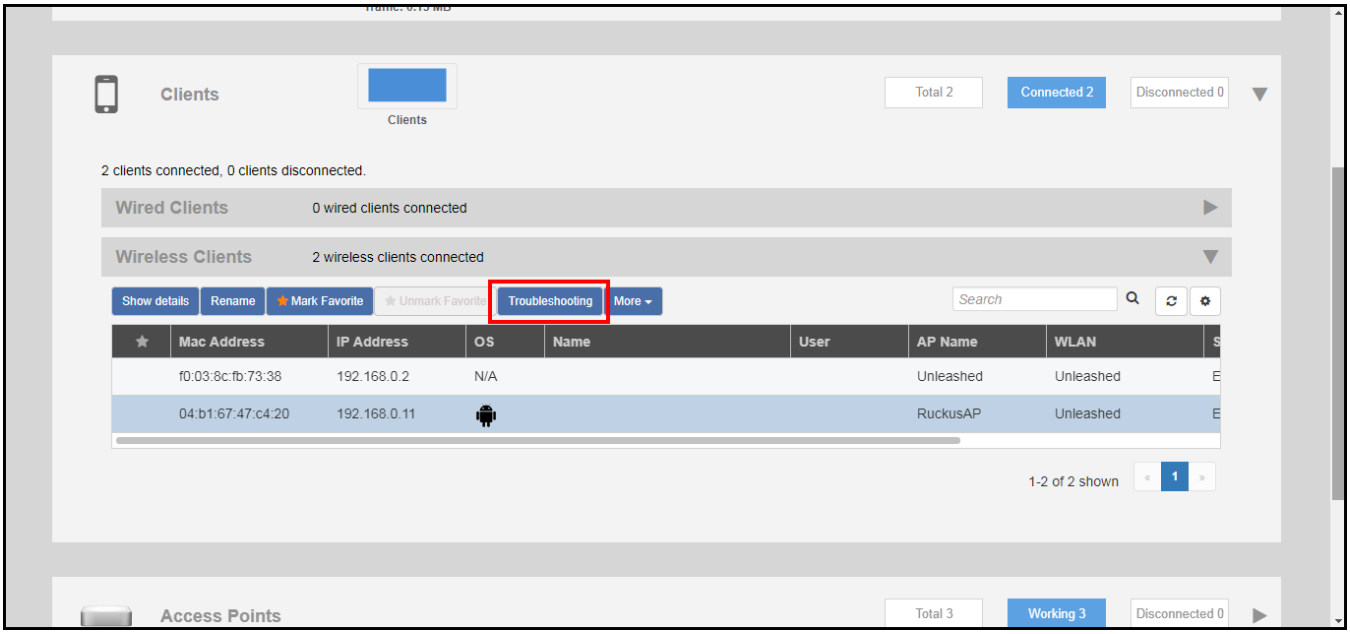
   NOTE
   Alternatively, go to **Admin & Services > Administration > Diagnostics > Client Troubleshooting**, and locate the **Client Connection Logs** section.

   NOTE
   As of release 200.8, client connection traces can be performed on clients connected to the following WLAN types:

   - WPA2
   - Web Auth
   - Hotspot
   - Guest Access

2. Click **Troubleshooting**.

   FIGURE 269 Click Troubleshooting to perform client connectivity trace



   The *Troubleshooting* screen appears.

3. In *Connectivity Trace*, click the **Start** button to begin. The association trace begins. The page refreshes to display detailed results.

FIGURE 270 Click Start to begin connectivity trace

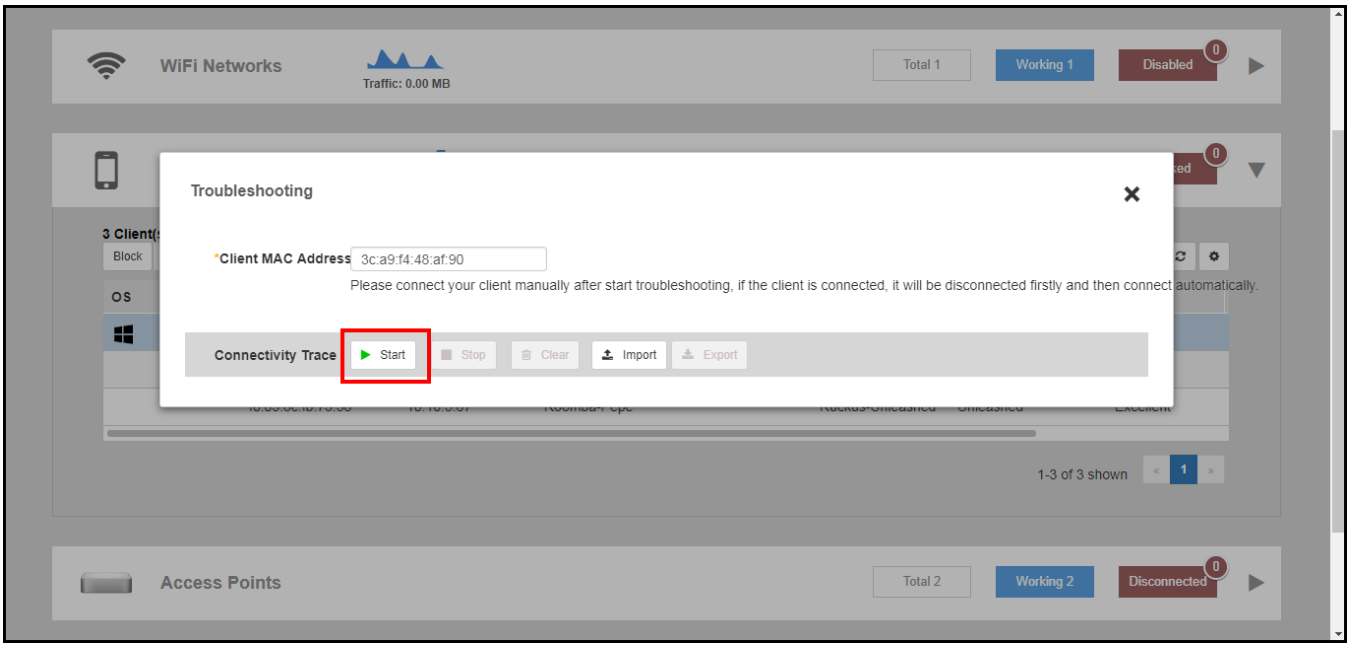
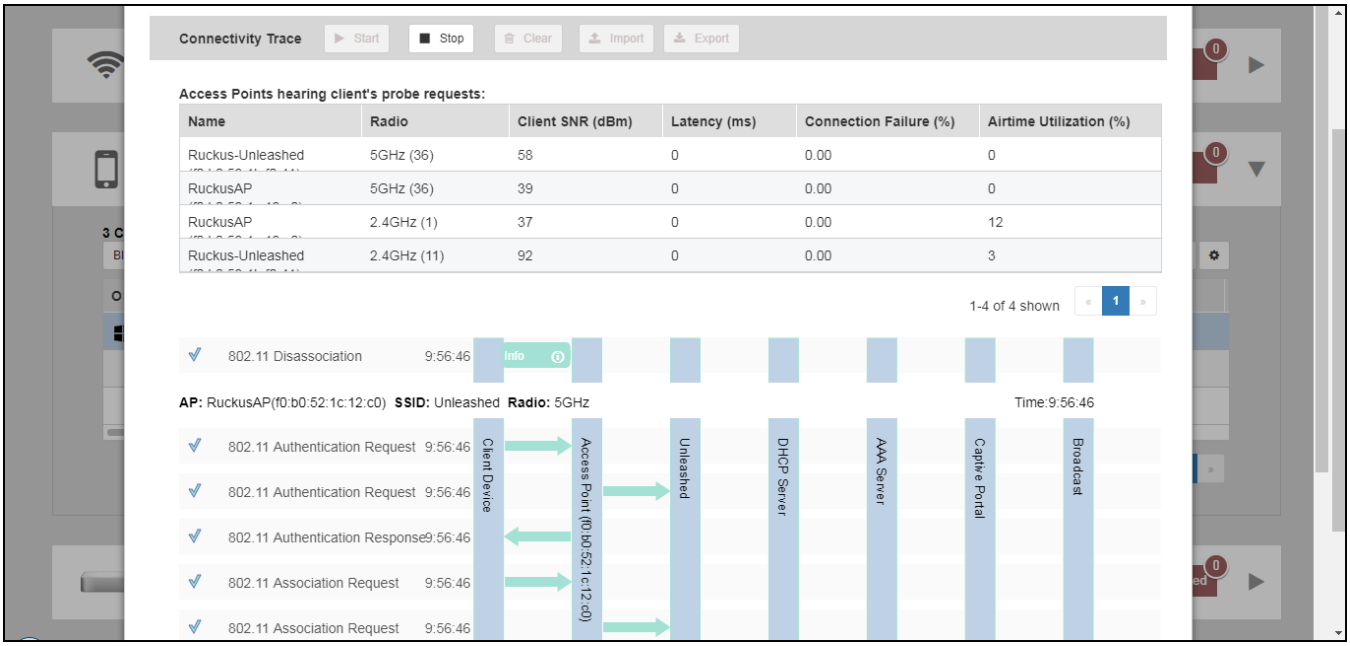


FIGURE 271 Connectivity trace in progress



4. Examine the results to isolate the problematic step in the process.
5. If needed, you can download the client connectivity data to a file, which can later be imported for analysis. Click **Export** to download the data file and save it to your local computer. Click **Import** to import a previously exported file back into Unleashed.

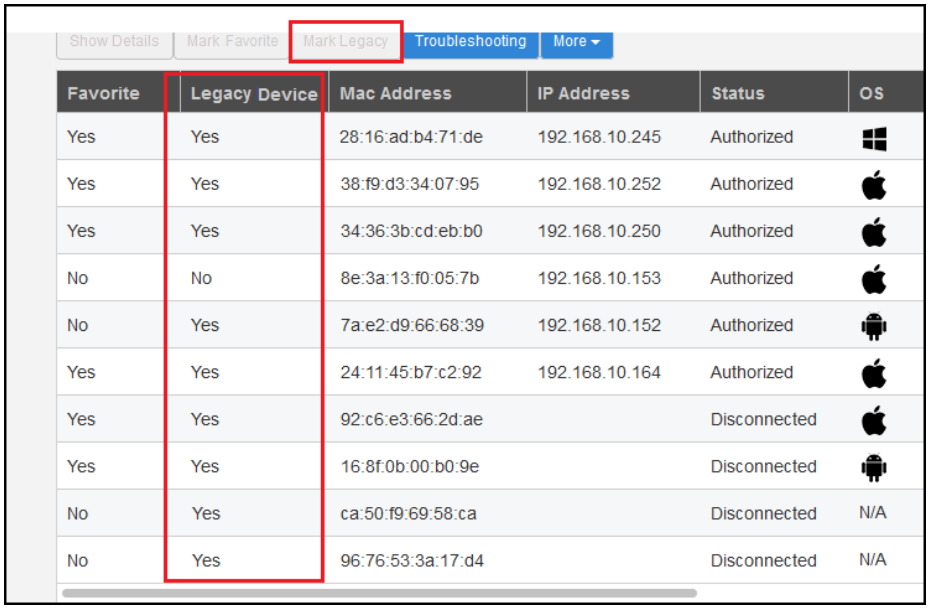
Marking a Client as a Legacy Device

Designating a wireless client as a legacy device provides a way to change a password, but allows original connected wireless devices to continue using the previous password. On a large-scale deployment, marking a wireless client as a legacy device is effective because the customer is not required to change the passwords on all the connected wireless devices.

Complete the following steps to mark a wireless client as a legacy device.

1. From the Unleashed dashboard, expand the **Clients** component.
2. Under **Wireless Clients**, select a client from the list and click **Mark Legacy**.

   FIGURE 272 Marking a Client as a Legacy Device



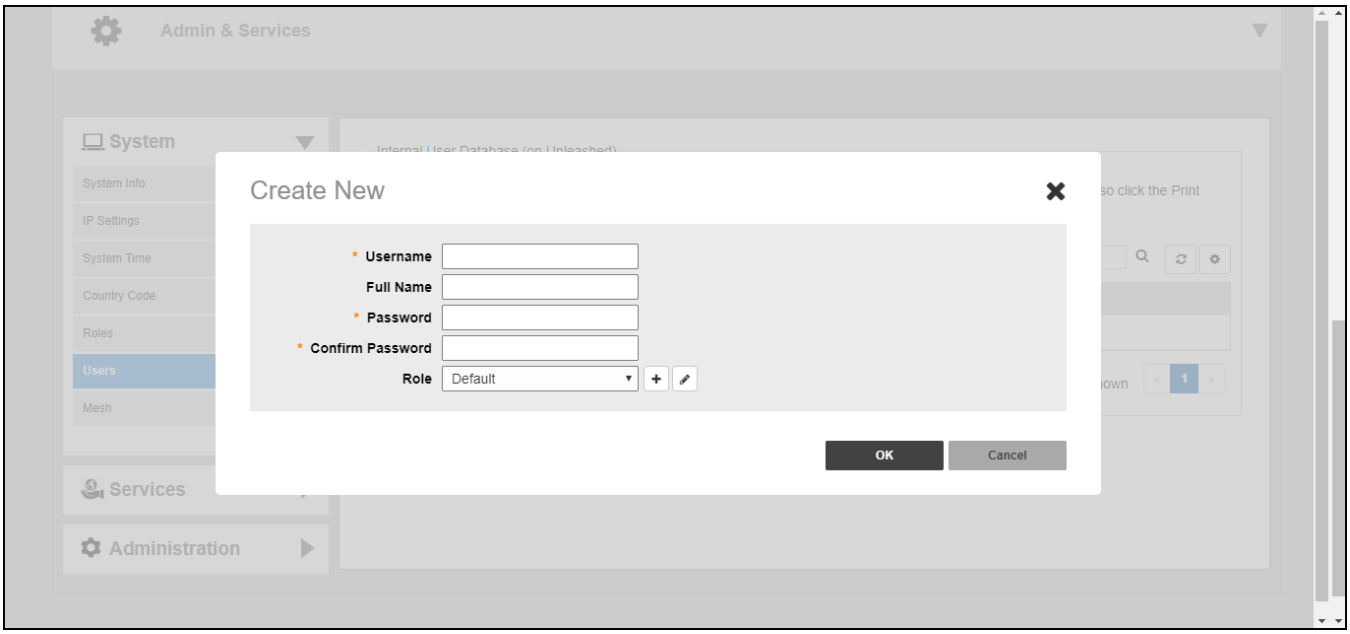
   The devices marked as legacy devices are allowed to connect to the WLAN with the previous password. For more information, refer to "Creating a New WLAN".
3. (Optional) Select a client and click **More** > **Unmark Legacy** to unmark the wireless client.

Adding User Accounts to the Internal User Database

1. Go to **Admin & Services > System > Users** and click **Create New**.
2. Enter a **User Name**, optional **Full Name**, **Password**, **Confirm Password**, and select a **Role** for this user.

3. Click **OK** to create the new user.

FIGURE 273 Creating a new User on the Internal User Database



Authenticating Clients Using an External Database

In addition to the Internal User Database, Unleashed also supports authenticating clients using an external authentication server.

To enable this feature, you must first create an "AAA Server" entry, and then apply the AAA server to one or more WLANs with external authentication enabled. Unleashed supports the following types of external authentication servers:

- Microsoft Active Directory
- RADIUS

For more information on configuring AAA servers, see AAA Servers on page 410.

Configuring Admin & Services Settings

- Admin & Services Overview..... 365
- System Settings.....365
- Services..... 409
- Administration Settings..... 461

Admin & Services Overview

The **Admin & Services** settings provide tools for use in managing many of the "under the hood" features of your Unleashed deployment.

These options allow you to configure system settings such as system name and IP address, configure services such as Application Recognition and Control, Guest Access and Hotspot services, and perform administration functions such as changing the admin user name and password, performing an upgrade and performing diagnostics.

The Admin & Services component is divided into the following sub-components:

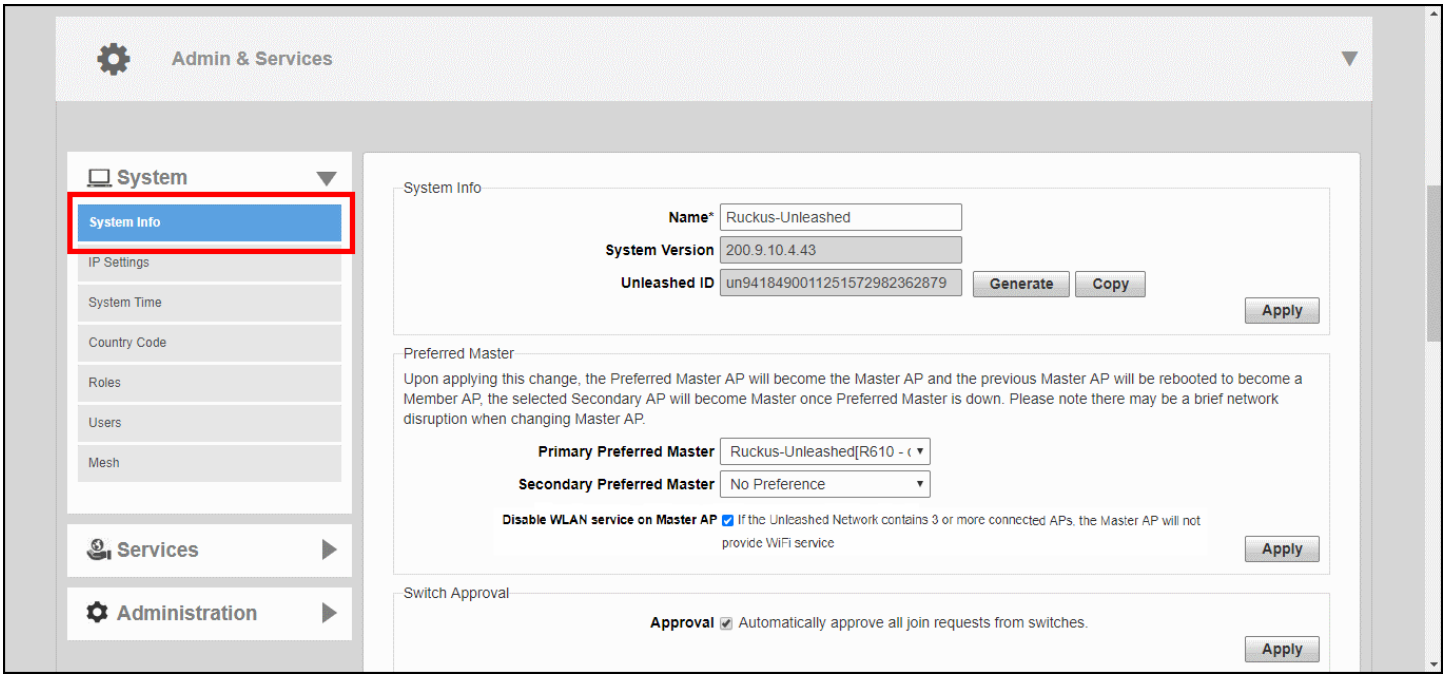
- System Settings on page 365
- Services on page 409
- Administration Settings on page 461

System Settings

System settings include options for changing the system name, preferred Master AP, IP address, time zone, country code, users, user roles and mesh settings.

To configure system settings, click **Admin & Services > System**. The menu expands to display additional options under the **System** tab.

FIGURE 274 Click Admin & Services, and expand the System tab to configure system settings



System Info Settings

System Info settings include options for configuring system name, preferred Master, automatic switch approval, email and SMS server settings.

Changing the System Name

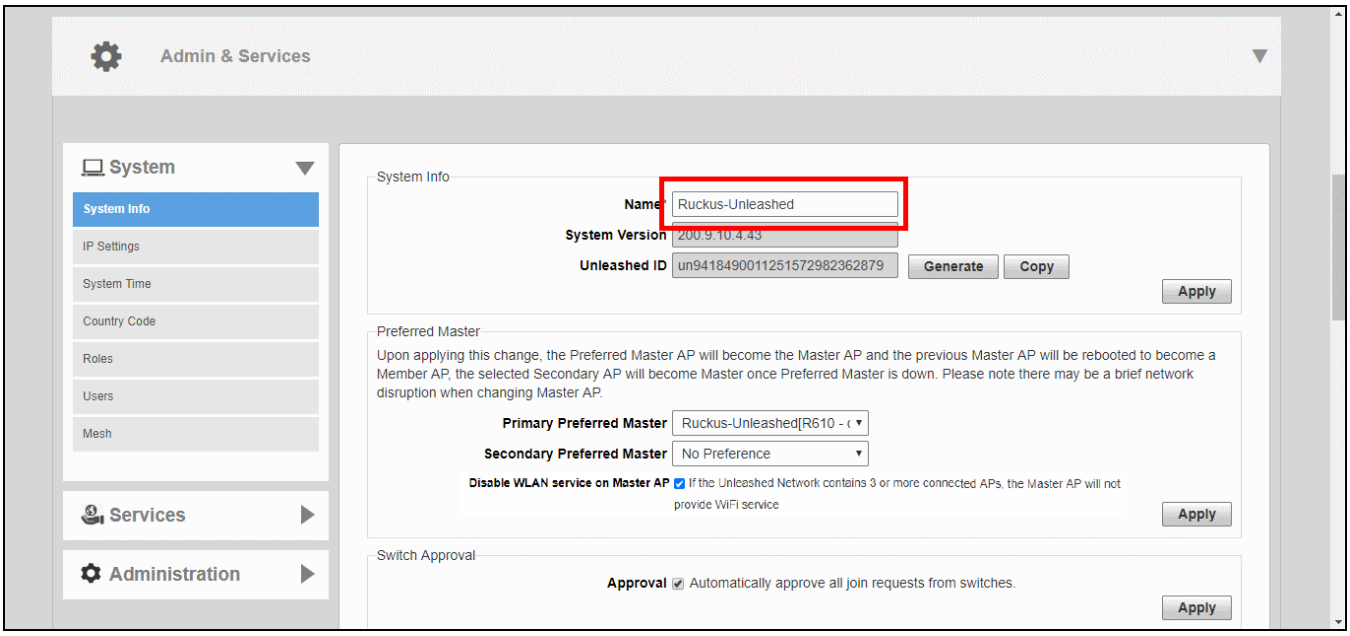
The **System Info** page displays the current system firmware version and provides an option to reconfigure the system name.

To change the system name:

1. Go to **Admin & Services > System > System Info**.
2. In **System Name**, delete the text, and then type a new name. The name should be between 1 and 32 characters in length, using letters, numbers, underscores (_) and hyphens (-). Do not use spaces or other special characters. Do not start with a hyphen (-) or underscore (_). System names are case sensitive.

3. Click **Apply** to save your settings. The change goes into effect immediately.

FIGURE 275 The System Info page displays the firmware version and system name



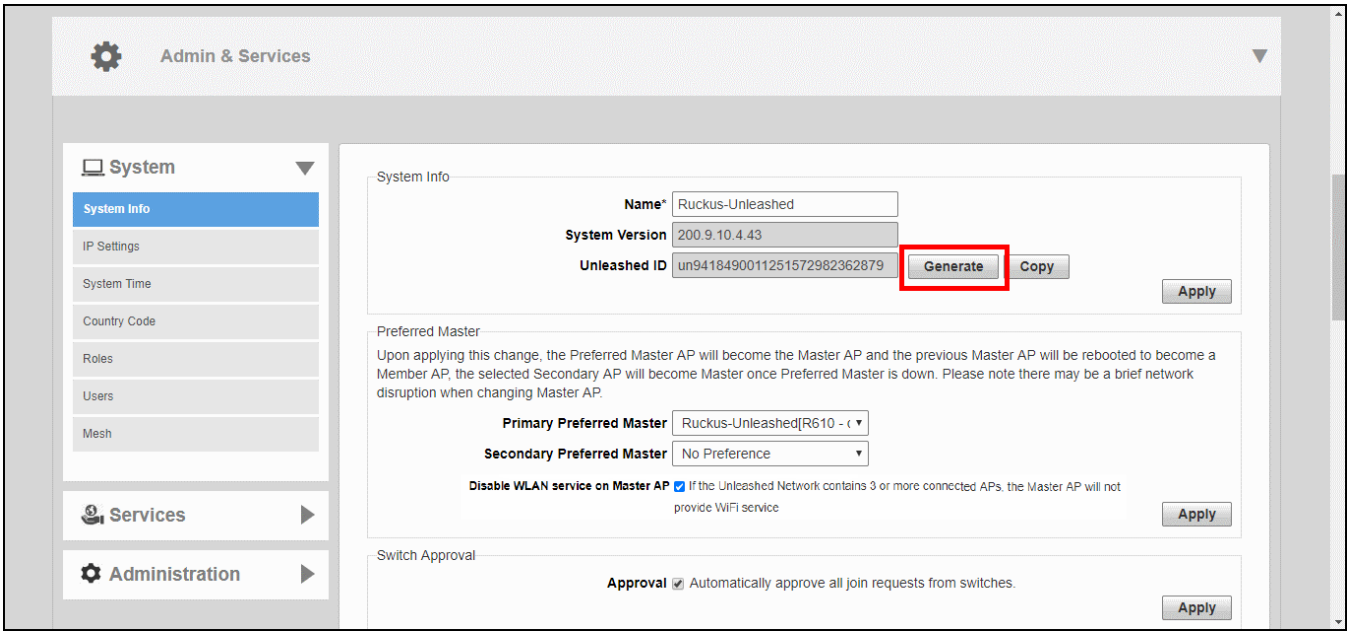
Generating an Unleashed ID

The Unleashed ID uniquely identifies each Unleashed network for use in remote management via either the Unleashed Mobile App or the Unleashed Multi-Site Manager.

1. Go to *Admin & Services* > *System* > *System Info*.
2. Click the *Generate* button next to Unleashed ID.

3. A new ID number appears in the Unleashed ID field. You can now use this number for remote management of this Unleashed network using the Unleashed Mobile App or Unleashed Multi-Site Manager.

FIGURE 276 Generating a new Unleashed ID for use in remote management



Designating a Preferred Master AP

The **Preferred Master** settings allow an administrator to manually designate the primary and secondary preferred Master APs.

By default, there is no preference as to which AP should become the Master AP. The first AP that is deployed automatically becomes the Master AP. If the Master AP goes offline for any reason, any other Ethernet-connected member AP can take over the role of the Master AP.

By using the **Preferred Master** option, the administrator can designate the APs that will have a priority as the Master AP.

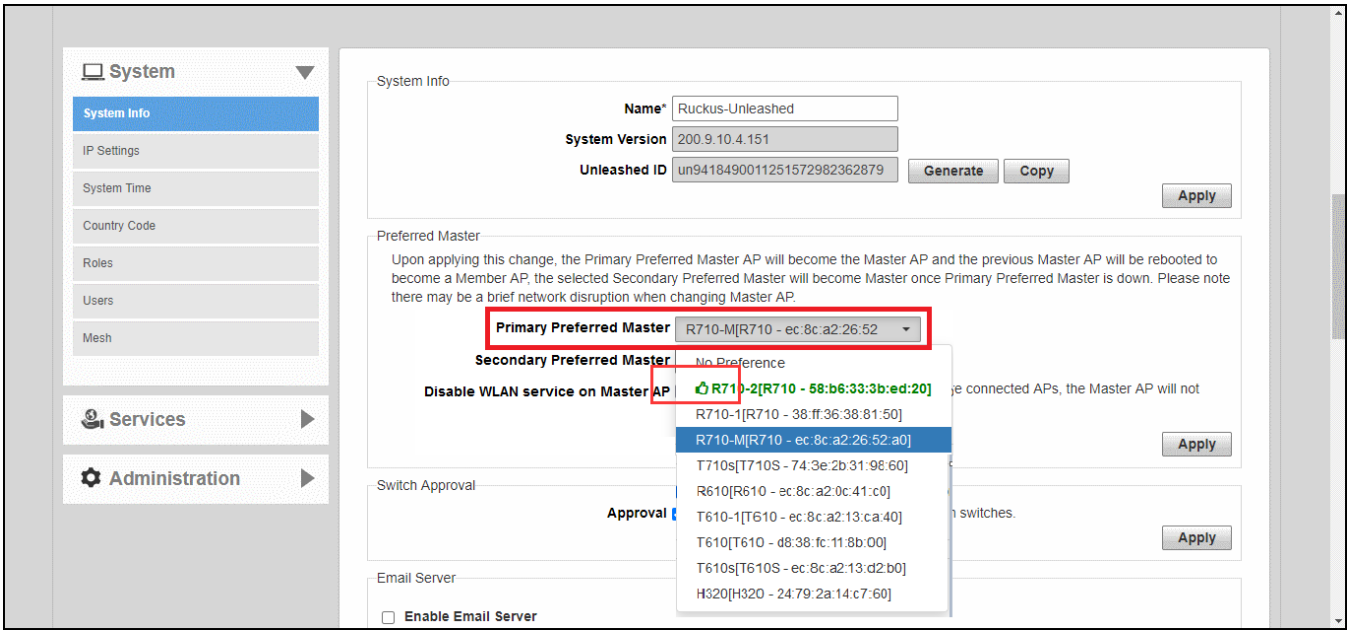
Complete the following steps to configure the primary and the secondary preferred Master APs.

1. Go to **Admin & Services** > **System** > **System Info**.

2. Under **Preferred Master**, from the **Primary Preferred Master** list, select a primary preferred Master AP.

   The **Primary Preferred Master** list displays the best Master AP at the top of the list. The recommended best Master AP is displayed in green and is indicated by a ("thumbs up" symbol), as shown in the following figure and you can choose this AP as the primary preferred Master.

   FIGURE 277 Designating APs as the Preferred Masters



3. From the **Secondary Preferred Master** list, select a secondary preferred Master AP.

   When the primary preferred Master AP is offline, the secondary preferred Master AP assumes the role of the Master AP. When the primary preferred Master AP returns online, it rejoins the Unleashed network and resumes the role of the Master AP again.

Disabling WLAN Service on the Master AP

Because the Master AP has to perform a number of tasks at once, it may be useful in some scenarios to reduce the compute load on the Master AP by disabling its WLAN service and allow the Master to focus on controller functions.

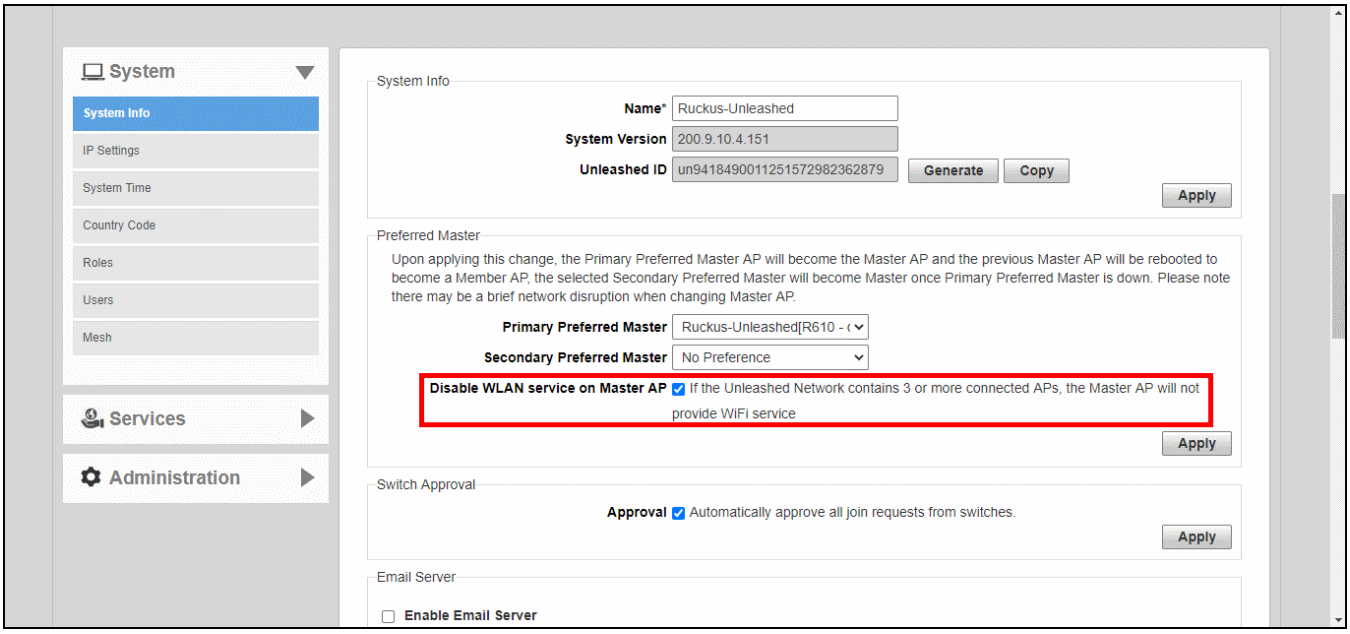
To disable WLAN service on the Master AP to allow it to focus on controller functions:

1. Go to *Admin & Services* > *System* > *System Info*.
2. In the *Preferred Master* section, deselect the **Enable WLAN service on Master AP** option.

3. Click **Apply** to save your changes.

NOTE
This feature will only take effect when the Unleashed network contains at least three other connected APs to provide WLAN service.

FIGURE 278 Disabling Master AP WLAN service



Configuring Global Access Point Policies

The **Access Point Policies** settings allow you to define how new APs are detected and approved for use in WLAN coverage, as well as policies on Dedicated Master discovery and communicating with the Dedicated Master.

Complete the following steps to review and revise the general AP policies.

1. Go to **Admin & Services** > **System** > **System Info**.

2. Review the current settings under **Access Point Policies**. You can change the following settings:
   - **Approval**: This option is enabled by default, which means that all join requests from any RUCKUS AP will be approved automatically. If you want to manually review and approve the joining of new APs to the WLAN, clear the **Approval** check box.
   - **Dedicated Master Discovery Policy**: If you have multiple Dedicated Masters on the network and want specific APs to join a specific Dedicated Master, you can limit Dedicated Master discovery. Ensure that Dedicated Master setup is completed.

     Select one of the following options:

     - **Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored)**: Add the Option 43 setting under DHCP server in the Linux DHCP server.

       ```
       #Ruckus Option 43 configuration as below:
       option space ruckus_info;
       option ruckus_info.zdiplist code 3 = text;
       vendor-option-space ruckus_info;
       option ruckus_info.zdiplist "10.223.26.121";
       ```

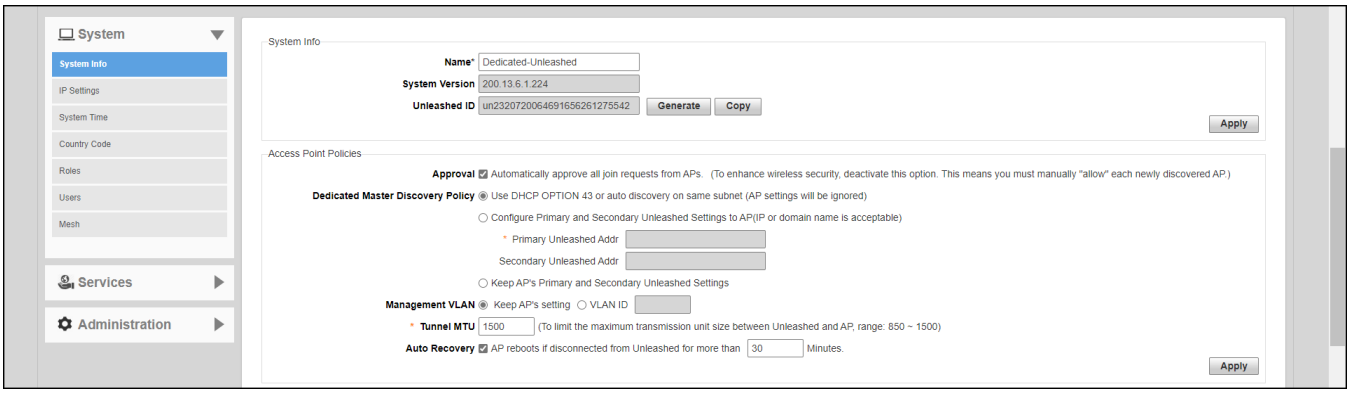
     - **Configure Primary and Secondary Unleashed Settings to AP**: Enter the IP addresses (or FQDNs) of the primary and secondary Dedicated Master units to which you want APs to join. APs will first attempt to join the primary Dedicated Master. If they cannot find or are unable to join the primary Dedicated Master, they will attempt to join the secondary Dedicated Master. If still unsuccessful, APs will stop attempting for a brief period of time, and then they will restart the joining process. They will repeat this process until they successfully join either the primary or secondary Dedicated Master.

       NOTE
       If you have two Dedicated Masters, RUCKUS recommends using Smart Redundancy. For information on Smart Redundancy configuration, refer to Smart Redundancy Configuration on page 176.

   - **Management VLAN**: You can enable the Dedicated Master management VLAN if you want to separate management traffic from regular network traffic. The following options are available:
     - **Keep AP's setting**: Select this option if you want to preserve the Management VLAN settings as configured on the AP. Note that the Management VLAN on the AP is disabled by default.
     - **VLAN ID**: Select this option and enter a valid VLAN ID to segment management traffic into the specified VLAN. Valid VLAN IDs are from 1 through 4094.
   - **Tunnel MTU**: Use this field to set the Maximum Transmission Unit for tunnel packets between a Dedicated Master and the APs. The MTU is the size of the largest protocol data unit (in bytes) that can be passed. Supported MTU values range from 850 through 1500 (the default is 1500).
   - **Auto Recovery**: Set an AP auto-recovery time in minutes, after which APs will reboot in attempt to reconnect to Dedicated Master. Default is 30 minutes.

3. Click **Apply** to save and apply your settings.

FIGURE 279 Configuring Global AP Policies

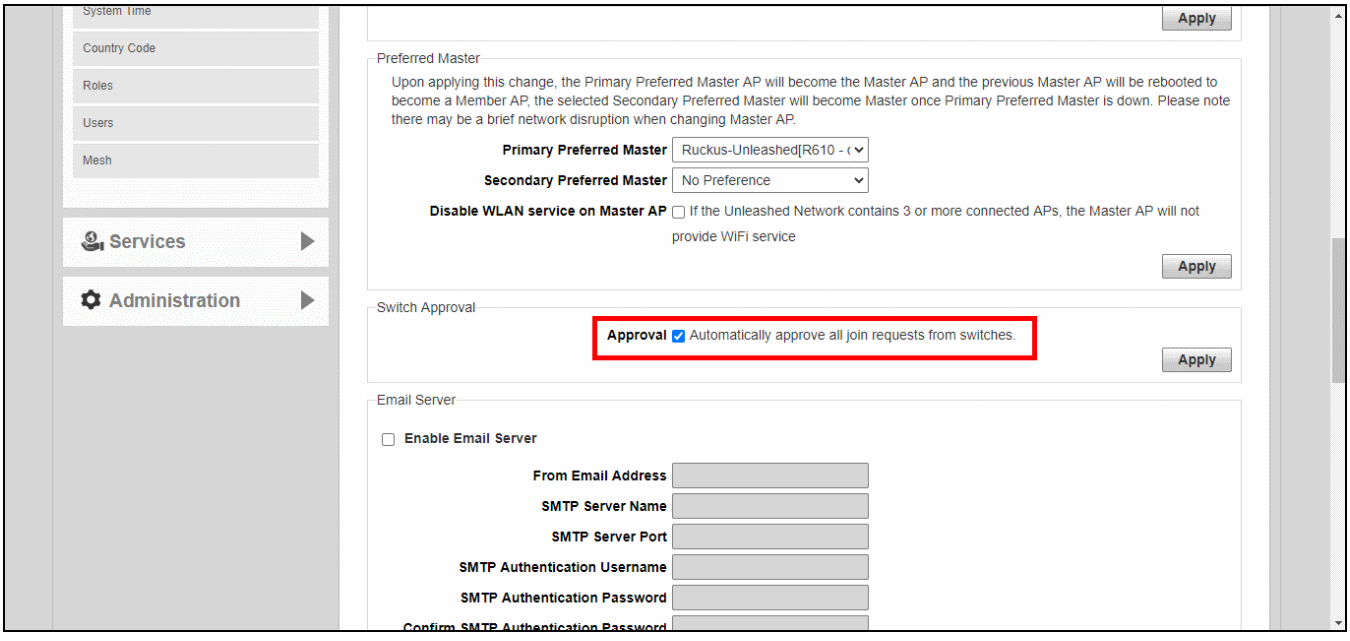


Enabling Automatic Switch Approval

To enable automatic approval of RUCKUS ICX switches, use the following procedure:

1. Go to *Admin & Services* > *System* > *System Info*, and locate the *Switch Approval* section.
2. Enable the **Approval** option.
3. Click **Apply** to save your changes.

FIGURE 280 Enable automatic approval of ICX switches



Configuring Email Server Settings

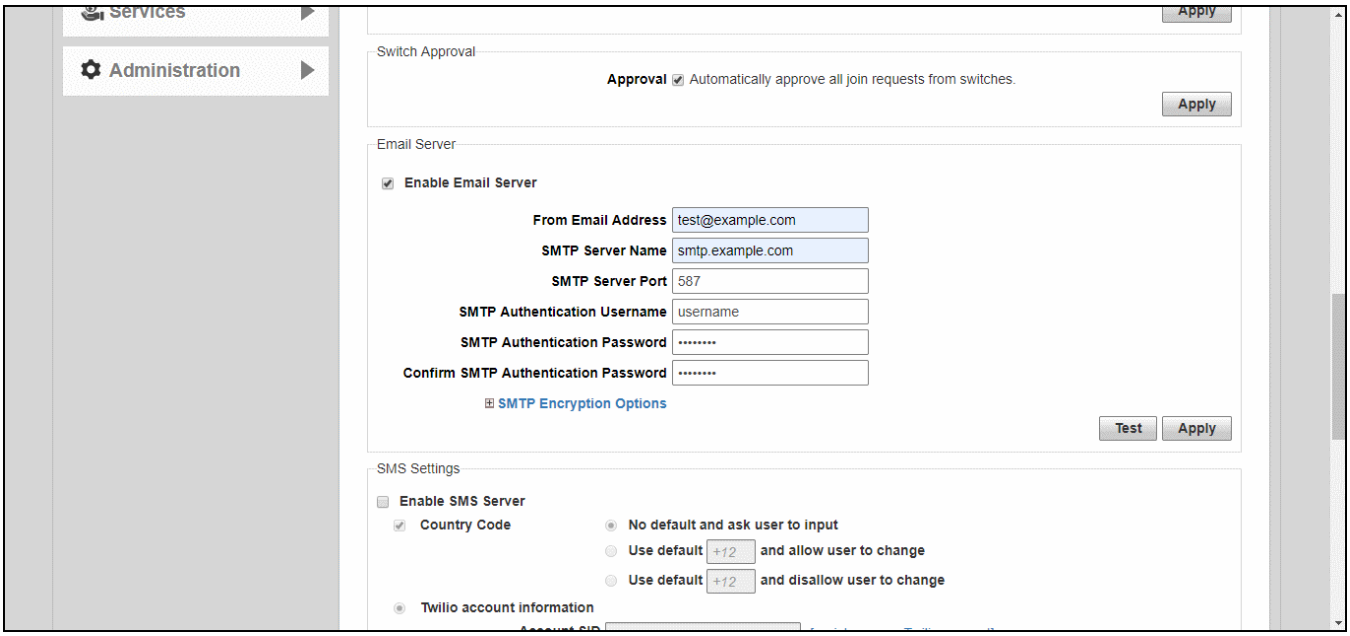
In order for Unleashed to send guest pass codes to guest users via email, it needs to have an email server configured.

To configure email server SMTP settings:

1. Go to **Admin & Services > System > System Info**.
2. In the **Email Server** section, enable the **Enable Email Server** check box, and then enter the following:
   - **From email address**: Type the email address from which Unleashed will send email messages.
   - **SMTP Server name**: Type the full name of the server provided by your ISP or mail administrator. Often, the SMTP server name is in the format smtp.company.com.
   - **SMTP Server port**: Type the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is 465 or 587. The default SMTP port value is 587.
   - **SMTP Authentication username**: Type the user name provided by your ISP or mail administrator. This might be just the part of your email address before the @ symbol, or it might be your complete email address. If you are using a free email service (such as Hotmail or Gmail), you typically have to type your complete email address.
   - **SMTP Authentication password**: Type the password that is associated with the user name above.
   - **Confirm SMTP Authentication password**: Retype the password you typed above to confirm.
   - **SMTP Encryption Options**: If your mail server uses TLS encryption, click the SMTP Encryption Options link, and then select the TLS check box. Additionally, select the STARTTLS check box that appears after you select the TLS check box. Check with your ISP or mail administrator for the correct encryption settings that you need to set.
3. To verify that Unleashed can send email messages using the SMTP settings you configured, click the **Test** button.
   - If Unleashed is able to send the test message, the message `Success!` appears at the bottom of the Email Notification page.
   - If Unleashed is unable to send the test message, the message `Failed!` appears at the bottom of the Email Notification page. Go back to the previous step, and then verify that the SMTP settings are correct.

4. Click **Apply**. The email server settings you configured become active immediately.

FIGURE 281 Email Server settings



Configuring SMS Server Settings

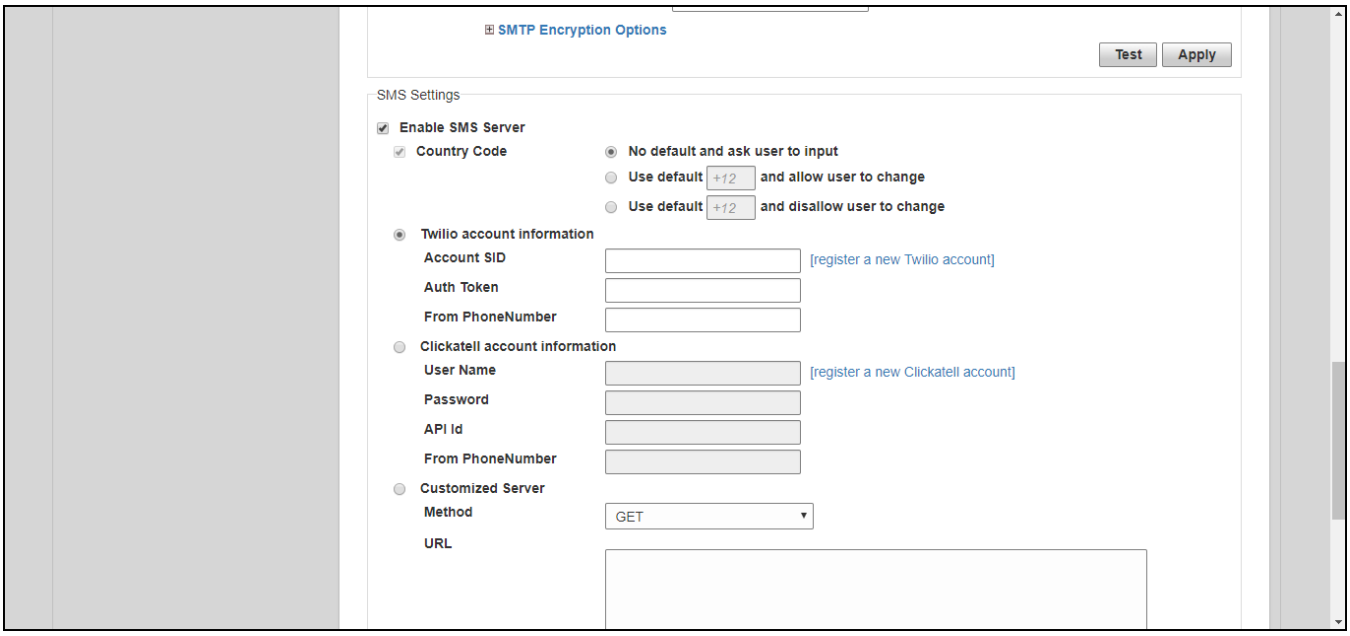
In order for Unleashed to send guest pass codes to guest users via SMS, it needs to have an SMS server configured.

To configure SMS server settings:

1. Go to **Admin & Services > System > System Info**.
2. In the **SMS Settings** section, enable the **Enable SMS Server** check box.
3. In **Country Code**, select one of the following options:
   - **CountryCode**: This option is only available with "Customized Server" SMS server type (for Twilio and Clickatell, the country code is mandatory and cannot be unchecked). When unchecked, the guest registration page does not support country code input.
   - **No default and ask user to input**: The guest registration page does not provide a default country code and the guest user is asked to input one.
   - **Use default and allow user to change**: The guest registration page provides a default country code and allows the guest user to change it.
   - **Use default and disallow user to change**: The guest registration page provides a default country code and the guest user is not allowed to change it.
4. Select **Twilio**, **Clickatell**, or **Customized Server**, depending on your SMS service provider.
5. Enter your **Account SID**, **Auth Token** and **From Phone Number** (Twilio) or your **User Name**, **Password** and **API ID** (Clickatell), or **Method** (Get or Post) and the URL for a custom SMS service provider.
6. Click the **Test** button to test your settings.

7. Once confirmed, click **Apply** to save your changes.

FIGURE 282 Configuring SMS settings



IP Settings

The *IP Settings* page provides options for configuring the Unleashed Master AP's IP address, IP address mode, management IP interface and DHCP options.

Configuring Device IP Address Settings

If you want to update the IP address and DNS server settings of your Master AP, complete the following steps.

NOTE
As soon as the IP address has been changed (applied), you will be disconnected from your web interface connection to the Master AP. You can log in to the web interface again by using the new IP address in your web browser.

Complete the following steps to change the IP address settings:

1. Go to **Admin & Services > System > IP Settings**.
2. Review the **IP Settings** options.

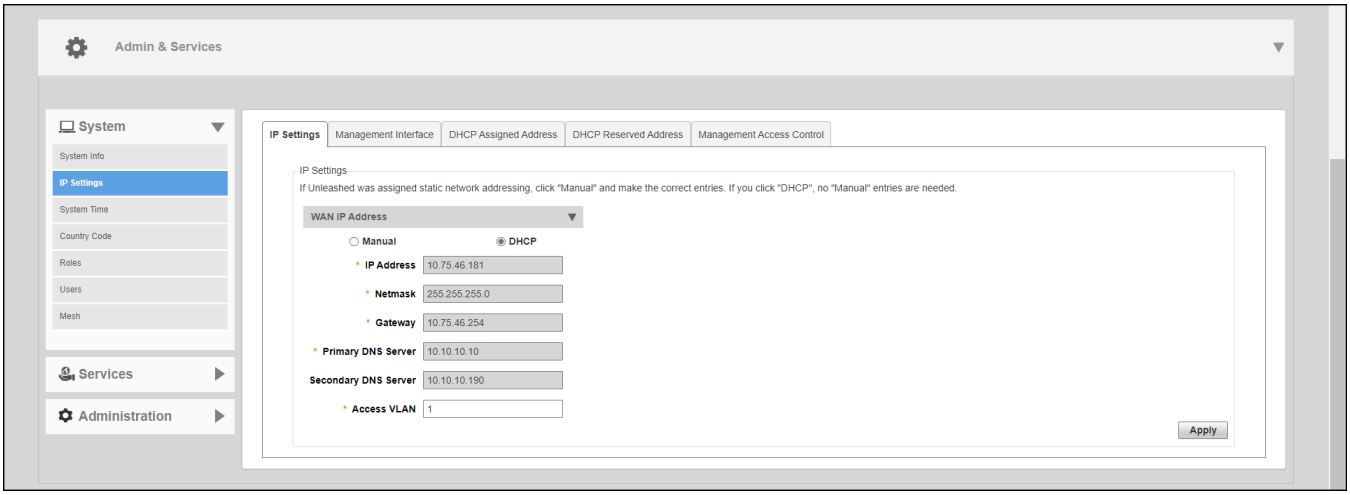
NOTE
Upon enabling Gateway mode, all devices will reboot immediately. Refer to Gateway Mode on page 376.

3. Under **WAN IP Address**, select one of the following options:
   - **Manual**: If you select **Manual**, enter the correct information in the active fields (**IP Address**, **Netmask**, **Gateway**, **Primary DNS Server**, **Access VLAN** are required).
   - **DHCP**: If you select **DHCP**, enter the access VLAN ID.

     NOTE
     The default value of the access VLAN ID is 1.

4. Click **Apply** to save your settings. You will lose connection to the Master AP.
5. To log in again to the web interface, use the newly assigned IP address in your web browser or use the Universal Plug and Play (UPnP) application to rediscover the Master AP.

FIGURE 283 Configuring Device IP Address Settings



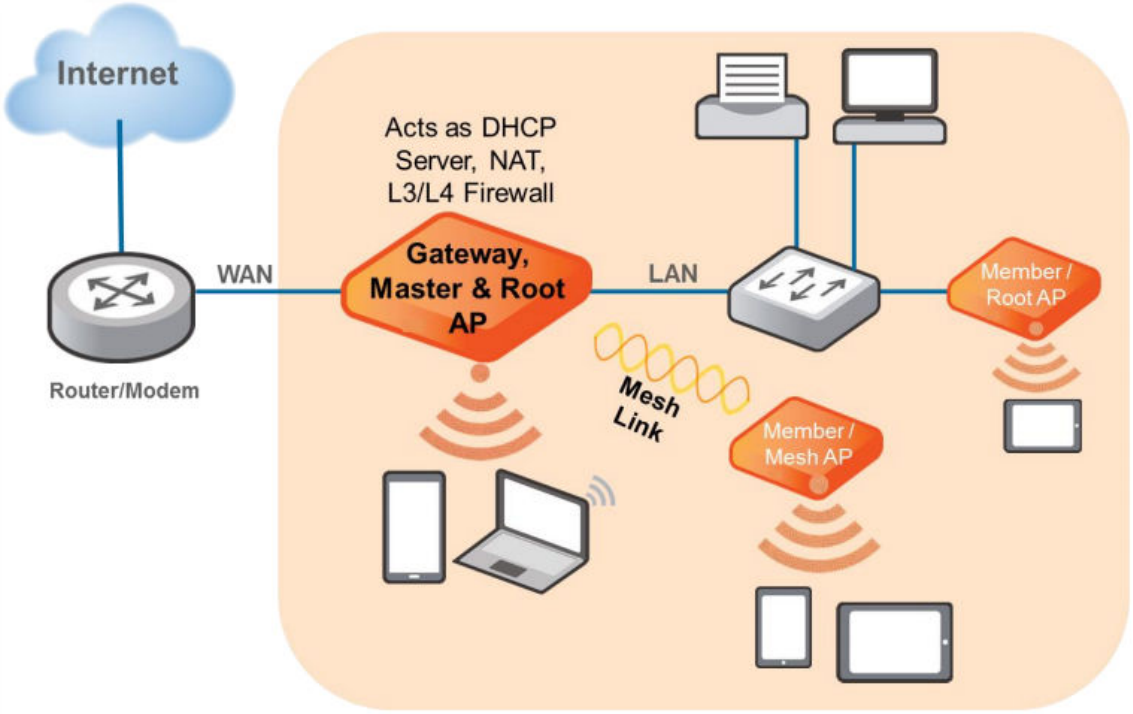
Gateway Mode

Gateway mode provides a solution for small and midsize business (SMB) customers who want to provide private IP addresses for clients and do not have an existing gateway router, or who connect to their Internet service provider (ISP) over PPPoE. Enabling Gateway mode provides Network Address Translation (NAT) and DHCP functionality to assign private IP addresses to member APs and clients.

Only the H350 AP and the H550 AP support dual WAN ports, where one Ethernet port is configured as the active WAN port and the other Ethernet port is configured as the standby WAN port for the RUCKUS Unleashed gateway. At any given point, only one Ethernet port acts as the active WAN port. The traffic moves through the active WAN port. If the active WAN port fails, the traffic is automatically switched to the standby WAN port until the active WAN port recovers.

NOTE
If Gateway mode is enabled, the maximum number of APs in a RUCKUS Unleashed network is 25, even if the Master AP can otherwise support more APs.

FIGURE 284 Gateway Mode Topology



Gateway functionality can be restored with minimum user intervention when a Gateway Master AP is out of service. If the Gateway Master AP goes down, simply replace it with one of the member APs and connect the uplink Ethernet cable to the WAN port, and the member AP will become the new gateway.

If the gateway recovery mechanism does not work, you can still access the web interface of the new Master AP to configure it manually.

Configuring Gateway Mode

The Master AP can be configured to serve as a gateway router.

Complete the following steps to configure the Master AP as a gateway:

1. Go to **Admin & Services** > **System** > **IP Settings**.

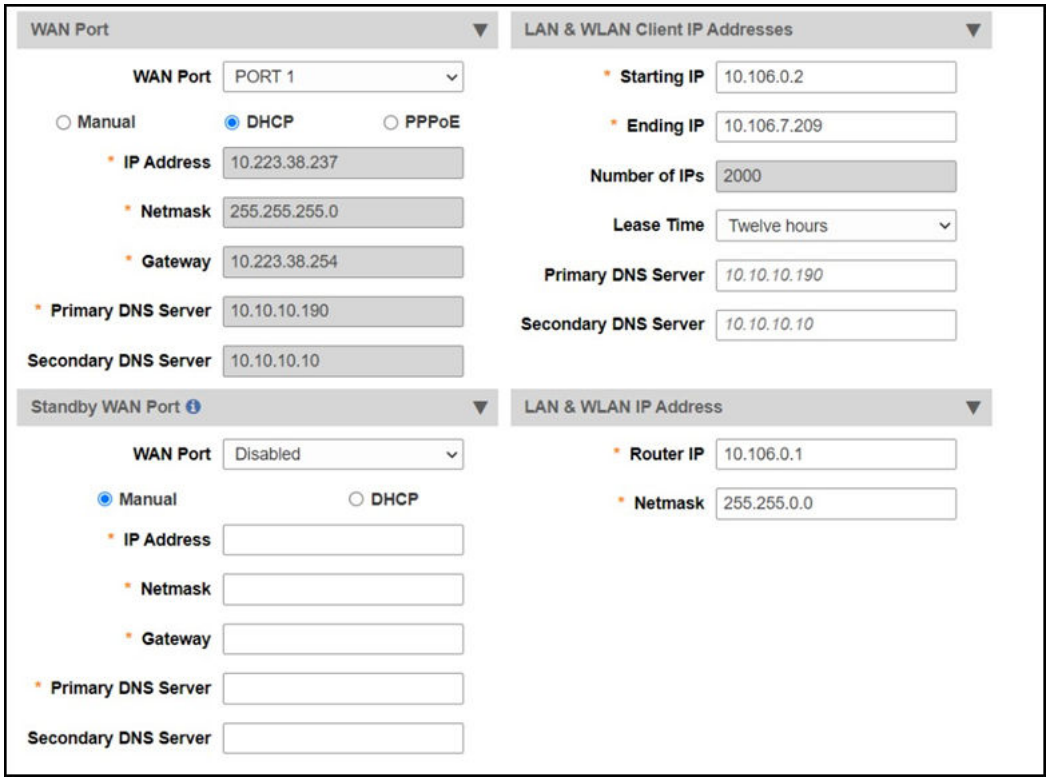
2. Under **IP Settings**, enable the **Gateway Mode** option and configure the WAN and LAN IP address settings.

   NOTE
   Alternatively, in the factory default state, you can connect to the Master AP and perform the initial setup as described in step 2b - Setup Using a Web Browser. On the second wizard screen (**Management IP**) select **Enabled** in **Gateway Mode**. Refer to Advanced Install on page 140 for more information.

FIGURE 285 Enabling Gateway Mode

3. Designate which port will be the WAN (uplink) port. The Gateway AP must have at least two Ethernet ports. Under **WAN Selection**, use the AP diagram to identify which port is LAN1 and LAN2 on the AP, and select the relevant port from the **WAN Port** list.

   FIGURE 286 Configuring WAN, Standby WAN, and LAN & WLAN IP Addresses



4. Configure how the WAN (uplink) port obtains its IP address:
   - **DHCP (Dynamic)**: When **DHCP (Dynamic)** is selected, the WAN port is assigned an IP address automatically.
   - **Manual (Static)**: When **Manual (Static)** is selected, enter an IP address, netmask, gateway address, and primary DNS server addresses in the required fields, and (optionally) enter the secondary DNS server address.
   - **PPPoE**: When PPPoE is selected, enter the PPPoE username and PPPoE password in the fields provided.
5. Configure local subnet settings for the LAN port:
   - **LAN & WLAN Client IP Addresses**
     - **Starting IP** and **Ending IP**: Enter the first and last IP addresses that will be issued in this scope.
     - **Number of IPs**: Enter the total number of addresses in this scope.
     - **Lease Time**: Select a duration for IP address lease time from the list.
     - **Primary DNS Server** and **Secondary DNS Server**: Enter the primary and secondary DNS server addresses.
   - **LAN & WLAN IP Address**
     - **Router IP**: Enter the IP address for the LAN port.
     - **Netmask**: Enter the netmask.

6. Designate which port will be the standby WAN (uplink) port and configure how the standby WAN port obtains its IP address:
   - **DHCP (Dynamic)**: When **DHCP (Dynamic)** is selected, the WAN port is assigned an IP address automatically.
   - **Manual (Static)**: When **Manual (Static)** is selected, enter an IP address, netmask, gateway address, and primary DNS server address in the required fields, and (optionally) enter the secondary DNS server address.

     NOTE
     A standby WAN port is applicable only for the H350 AP and H550 AP.

7. Click **Apply**. Once setup is complete, the Gateway AP will begin providing DHCP and NAT service for clients, and clients will be assigned IP addresses from the DHCP scope that you configured.

Gateway Mode Limitations and Considerations

There are several important limitations and factors to consider when enabling gateway mode.

- All Unleashed AP models with multiple Ethernet ports support gateway mode. If your network's WAN bandwidth is higher than 100 Mbps, RUCKUS recommends using 802.11ac Wave 2 or later APs (such as R510, R610, R710, R720) to enjoy the fastest internet access experience.
- The Master AP acts as the gateway for both wired and wireless clients.
- The gateway AP provides IP addresses and performs NAT (routing) functions in addition to serving as the Unleashed Master AP, and servicing wireless clients. For this reason, it is preferable to use an AP with higher CPU/memory resources, especially 802.11ac Wave 2 or later APs (e.g., R510, R610, R710, R720) as the Gateway AP, if possible.
- If gateway mode is enabled, the maximum number of APs in an Unleashed network is 25, even if the Master AP could otherwise support more.
- No VLAN support in gateway mode.
- Bonjour Gateway is not supported in gateway mode (no VLANs).
- When Mesh is enabled in gateway mode, and when the WAN IP address is obtained via PPPoE, the Master AP cannot be part of a Mesh tree. However, Mesh can still be enabled and any member AP can be a Root AP or Mesh AP.
- The WAN and LAN IP addresses must be in different IP subnets, and the address ranges may not overlap.
- If gateway mode is enabled, redundancy is disabled. This means that if the Master (gateway) AP goes offline for any reason, a member AP will not be able to take over and become the new Master.

Configuring M510 as Unleashed Master in Gateway Mode

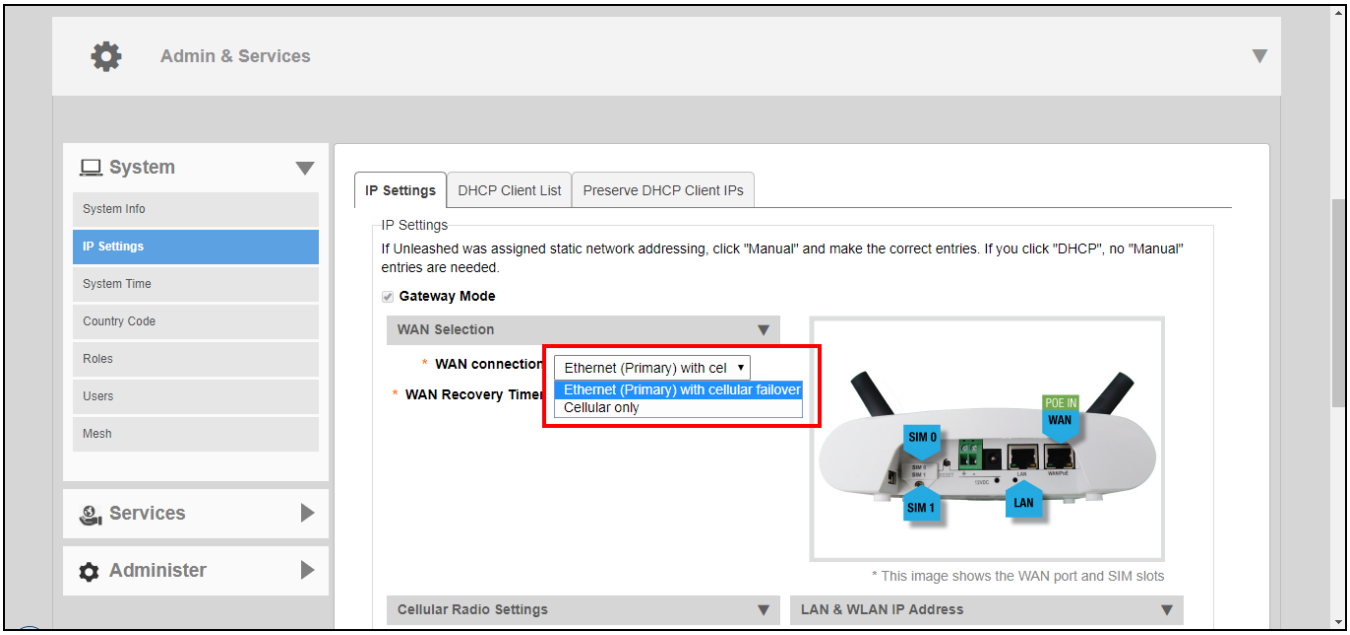
The Unleashed M510 provides additional options for configuring the LTE uplink mode.

To configure the M510 LTE WAN connection settings:

1. Go to **Admin & Services > System > IP Settings**.

2. IN *WAN connection*, select one of the following options:
   - **Ethernet (Primary) with cellular failover**: M510 in Gateway Mode with the Ethernet port as the WAN port and the LTE connection as the backup WAN port, only one of which can be active at any time. If the Ethernet connection goes down, the LTE connection becomes active to provide a backup internet uplink.
   - **Cellular only**: M510 configured as Master AP in Gateway Mode with an LTE connection as the uplink WAN port.

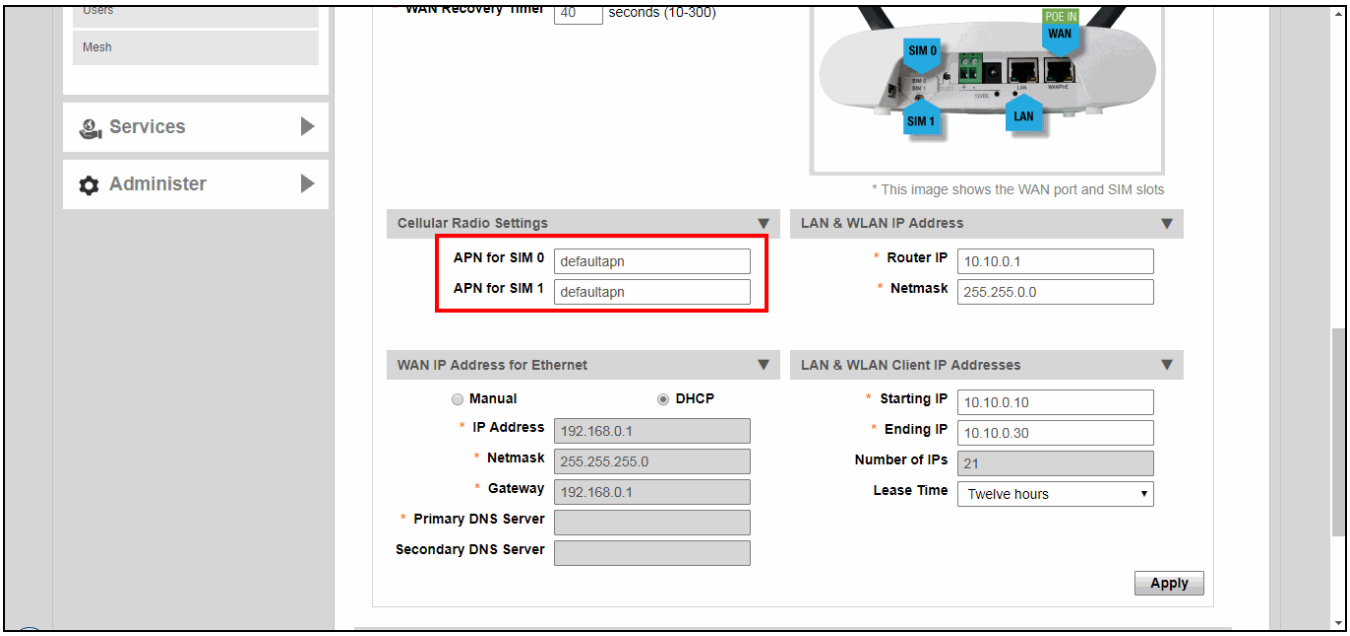
FIGURE 287 Select WAN uplink connection mode



3. In **WAN Recovery Timer**, enter a value in seconds after which failover to LTE uplink will occur.
4. In **Cellular Radio Settings**, enter the Access Point Name for each SIM card. The APN identifies the mobile network operator and the data network that the client intends to connect to.
5. If the *Ethernet (Primary) with cellular failover* option is selected, configure the **WAN IP Address for Ethernet** settings:
   - **Manual**: Enter IP address, Netmask, Gateway and DNS addresses according to your network configuration.
   - **DHCP**: Automatically assign WAN IP address from a DHCP server on the network.

6. Configure internal WLAN and LAN IP address settings as described in *Configuring Device IP Address Settings*.

FIGURE 288 M510 Cellular Radio Settings



DHCP Server

RUCKUS Unleashed provides a built-in DHCP server that you can enable to assign IP addresses to devices that are connected to the RUCKUS Unleashed network. The internal DHCP server will only assign addresses to devices that are on its own subnet and part of the same VLAN.

NOTE
Before you can enable the built-in DHCP server, the Master AP must be assigned a manual (static) IP address. If you configured RUCKUS Unleashed to obtain its IP address from another DHCP server on the network, the options for the built-in DHCP server will not be visible on the *IP Settings* page.

Complete the following steps to configure the built-in DHCP server:

1. Go to **Admin & Services > System > IP Settings**.
2. Under **WAN IP Address**, select **Manual** and enter the static IP settings (IP address, netmask, gateway and DNS settings).
3. In *LAN and WLAN Client IP Addresses*, enable the **DHCP Server** check box.
4. **Starting IP**: Enter the first IP address that the built-in DHCP server will allocate to DHCP clients. The starting IP address must be on the same subnet as the IP address assigned to the Master AP. If the value that you entered is invalid, an error message appears and prompts you to let RUCKUS Unleashed automatically correct the value. Click **OK** to automatically correct the entry.
5. **Ending IP**: Enter the last IP address in the range that you want to allocate to requesting clients. The built-in DHCP server can allocate up to 512 IP addresses including the one assigned to the Master AP. The default value is 200.
6. **Lease Time**: Select a time period for which IP addresses will be allocated to DHCP clients. Options range from six hours to two weeks (the default is one week).

7. Enter the primary and secondary DNS server addresses.

   NOTE
   In the gateway mode, the user can customize the DNS server setting for wireless clients. If the DNS server setting is ignored, the WAN interface DNS server setting is used.

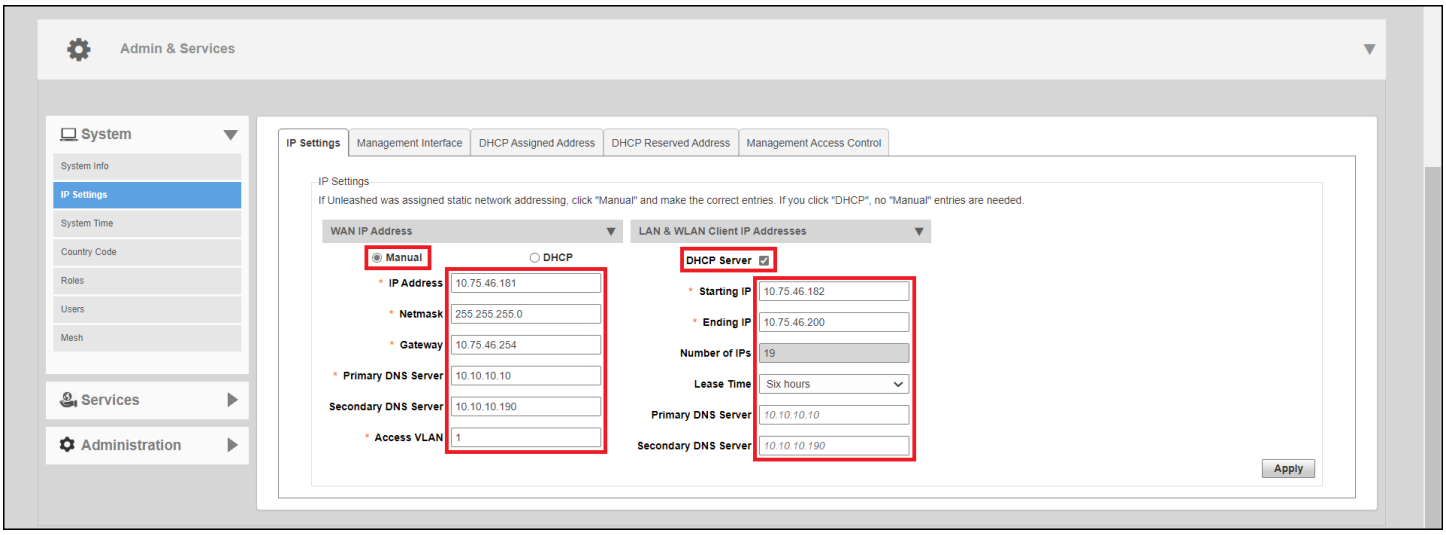
8. Click **Apply**.

   NOTE
   If you entered an invalid value in any of the text boxes, an error message appears and prompts you to let RUCKUS Unleashed automatically correct the value. Click **OK** to automatically correct the value.

   NOTE
   RUCKUS recommends that you only enable the built-in DHCP server if there are no other DHCP servers on the network. If you enable the built-in DCHP server, RUCKUS also recommends enabling rogue DHCP server detection. For more information, refer to Rogue DHCP Server Detection on page 451.

   NOTE
   Make sure the DHCP address pool is routable to the internet and non-overlapping with other devices. Because RUCKUS Unleashed in non-gateway mode does not support Network Address Translation (NAT), this is important to avoid IP address conflicts. For example, if your router uses the 192.168.0.x subnet, you must use any subnet *other* than 192.168.0.x for your RUCKUS Unleashed DHCP subnet.

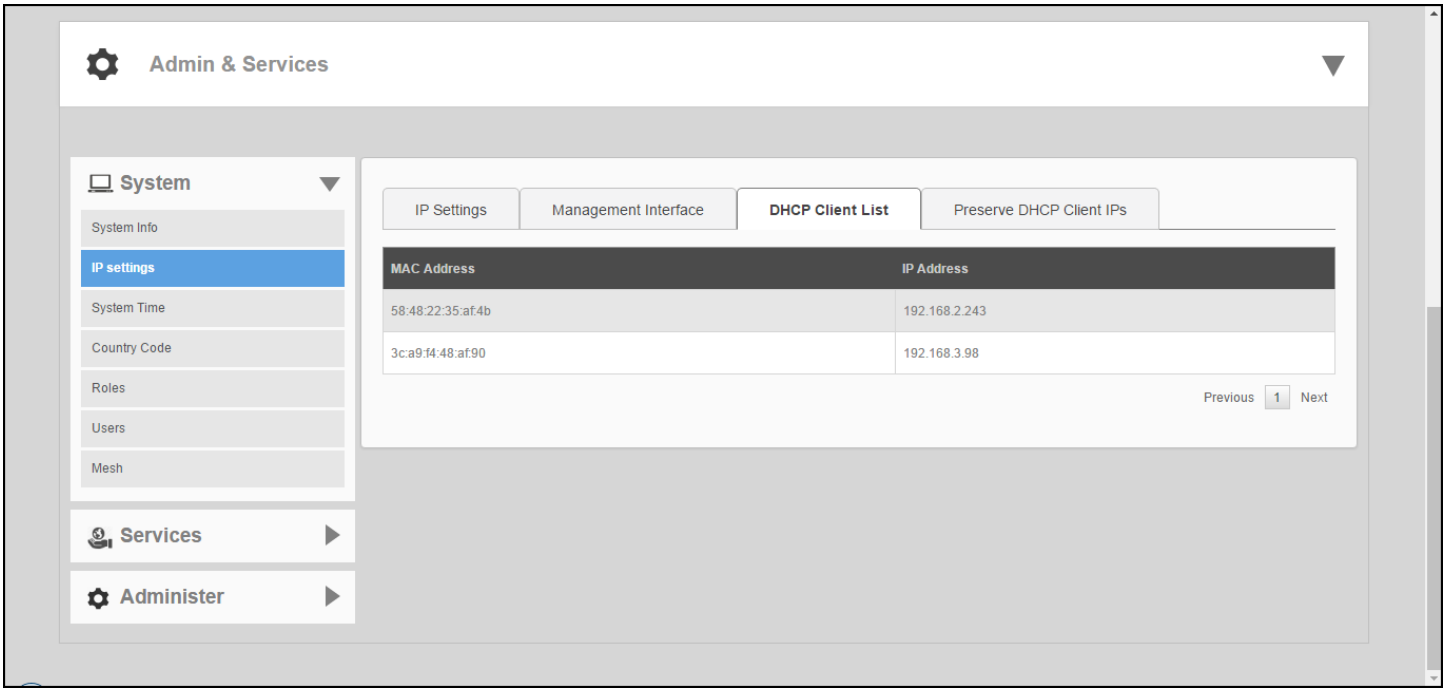
FIGURE 289 DHCP Server Configuration



DHCP Client List

The **Admin & Services > System > IP Settings > DHCP Client List** page displays a list of IP addresses assigned to clients by the Unleashed Master AP.

FIGURE 290 DHCP Client List



Reserve DHCP Client IPs

Use this page to create a list of reserved IP addresses bound to specific MAC addresses.

To create an entry, click **Create New**, and enter the client's **MAC Address**, the **IP Address** you want to reserve, and optionally a **Description** of the device.

A maximum of 128 reserved IP address entries can be created.

FIGURE 291 Create New Reserved IP Address

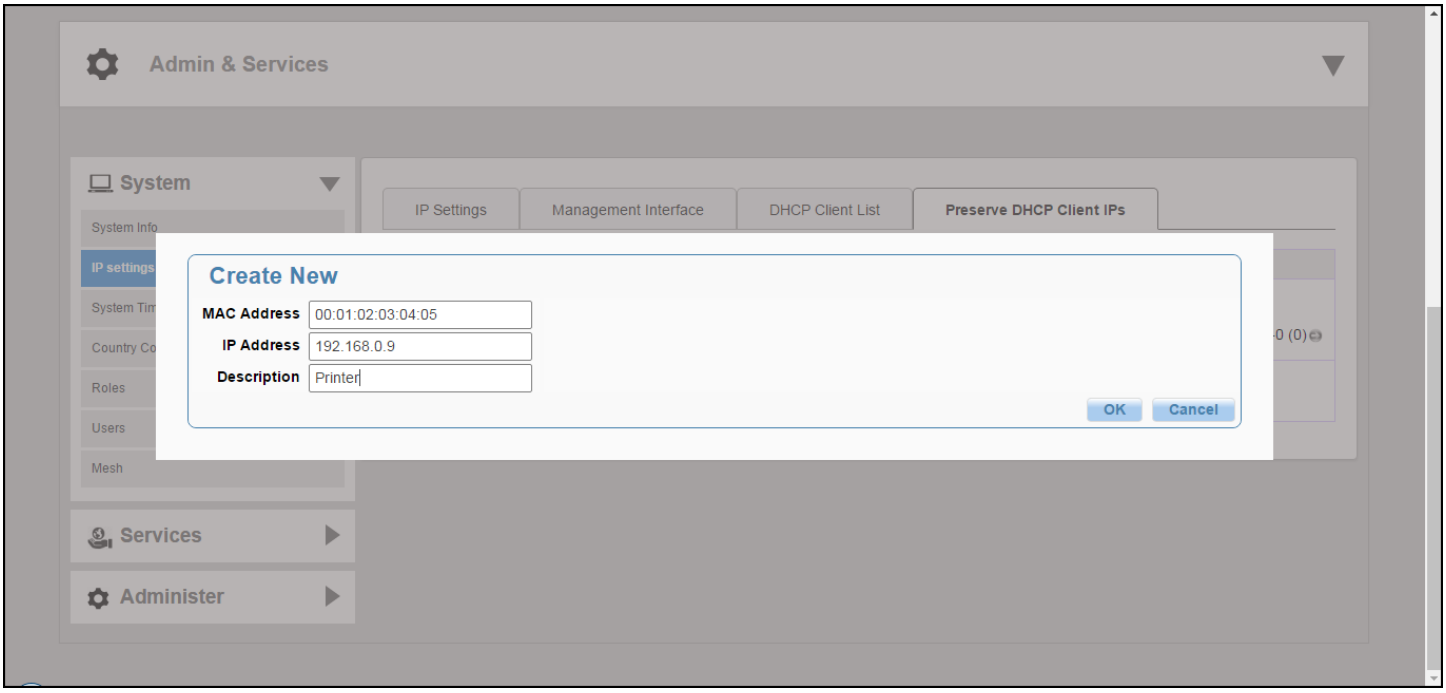
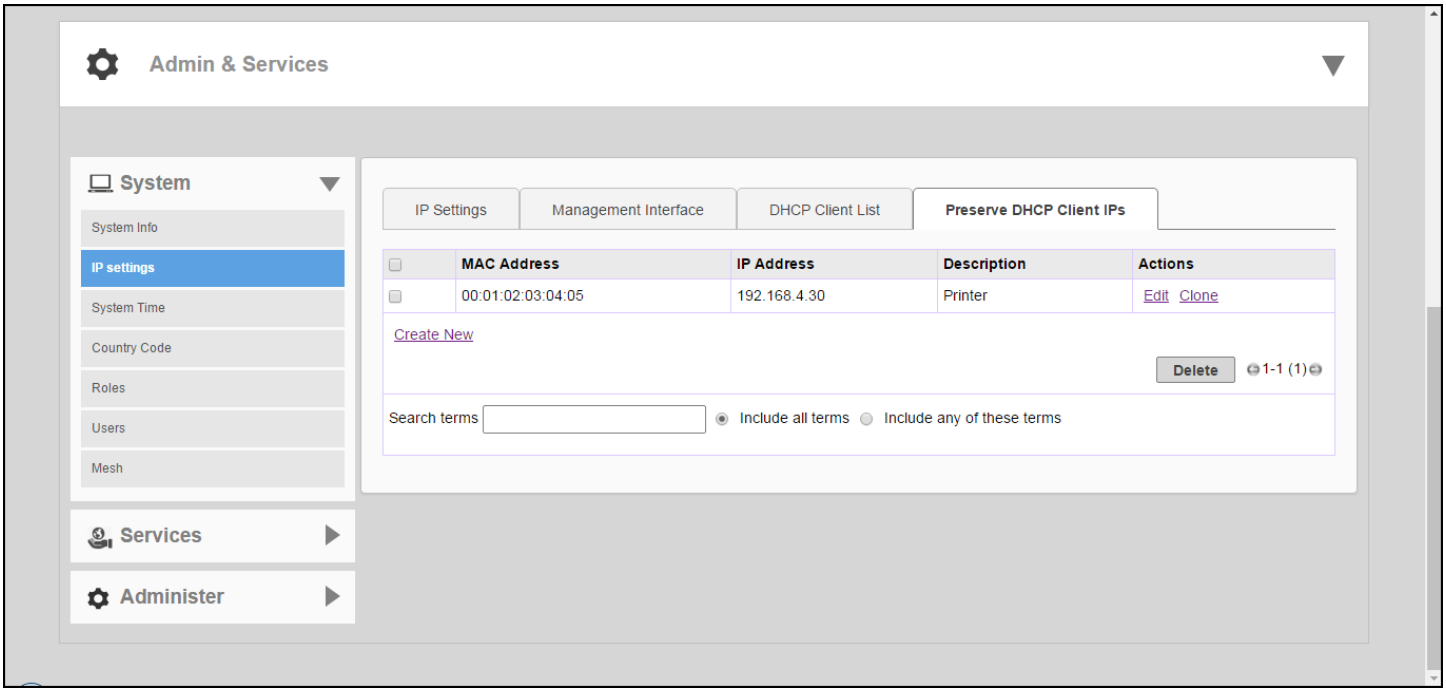


FIGURE 292 Reserved IP Addresses



Configuring a Management Interface

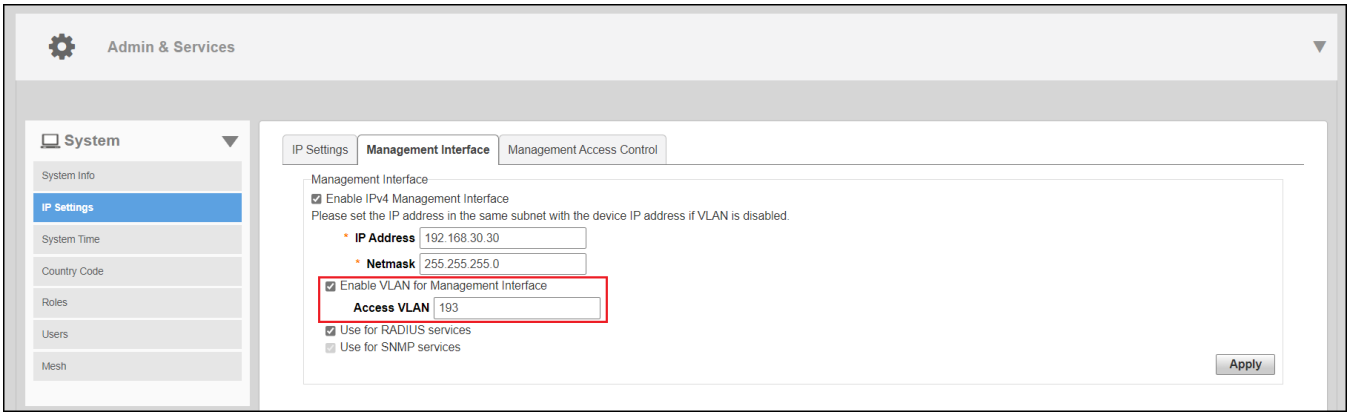
The Management IP address can be configured to allow an administrator to manage the Unleashed network from a single IP address, regardless of which Unleashed AP is currently the Unleashed Master AP.

The Management IP can be reached from anywhere on the network as long as it is routable by way of the default Gateway configured in **Device IP Settings**. Then, you only have to remember one IP address.

Complete the following steps to configure a Management Interface:

1. Go to **Admin & Services** > **System** > **Device IP Settings**, and click the **Management Interface** tab.
2. Select the check box next to **Enable IPv4 Management Interface**.
3. Enter an **IP Address** and **Netmask**.
4. (Optional) Select **Enable VLAN for Management Interface** and enter **Access VLAN**.
5. (Optional) Enable the check box next to **Use for RADIUS services** to use this IP address for communication with a RADIUS authentication/accounting server. If enabled, the Master AP will send RADIUS packets through this management interface, and the RADIUS server only needs to record one IP address for the Unleashed network. Otherwise, it will record the addresses of all APs.
6. The **Use for SNMP** services check box is automatically enabled when a Management Interface is enabled, and this address will be used for SNMP communications, if enabled.

FIGURE 293 Management Interface



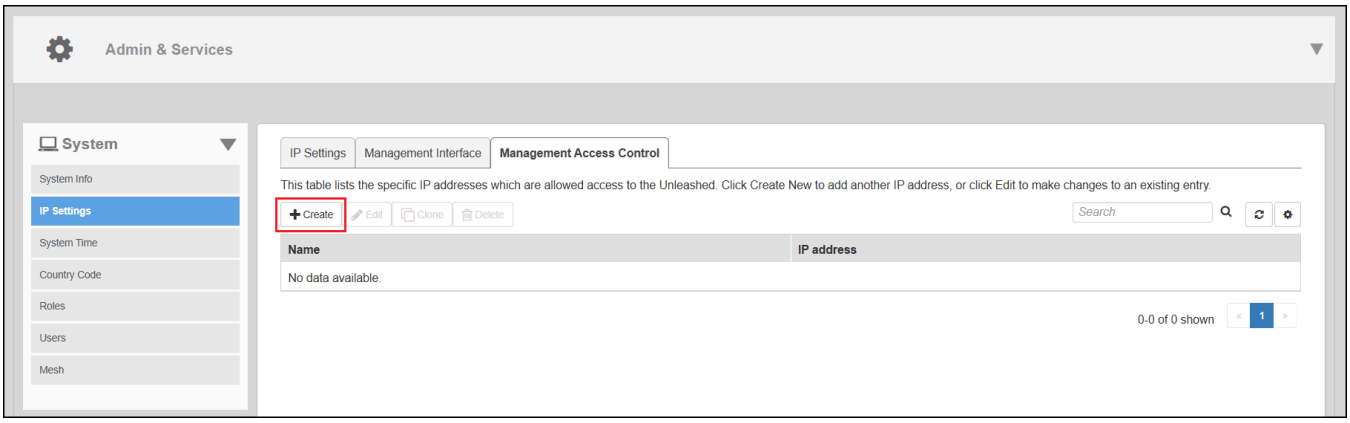
Configuring a Management Access Control

Management Access Control can be used to control access to the management interface of RUCKUS Unleashed.

When you create a management access control rule, all IP addresses and subnets other than those listed specifically listed are blocked from accessing the RUCKUS Unleashed web interface. Access can be restricted by subnet, single IP address, and IP address range.

1. Go to **Admin & Services** > **IP Settings** > **Management Access Control**.

   FIGURE 294 Management Access Control Tab



2. Click **Create**.

3. In the **Create New** dialog box, enter the following information:
   a) In the **Name** field, enter the user name that you want to allow access to the RUCKUS Unleashed web interface.
   b) For **Restriction**, select one of the options:
      - **Single**
      - **Range**
      - **Subnet**
   c) In the **IP Address** field, enter a single IP address, a range of IP addresses, or a subnet based on your **Restriction** option.

FIGURE 295 Creating a New Management Access Control

4. Click **OK**.

Configuring the System Time

Many RUCKUS Unleashed features require that the Master AP maintains the proper system time.

Maintaining the proper time relies on periodically retrieving the time from a Network Time Protocol (NTP) server on the internet. By default, the RUCKUS Unleashed network automatically updates its system time using the Network Time Protocol (NTP), which periodically polls an NTP server and synchronizes its time with the NTP server.

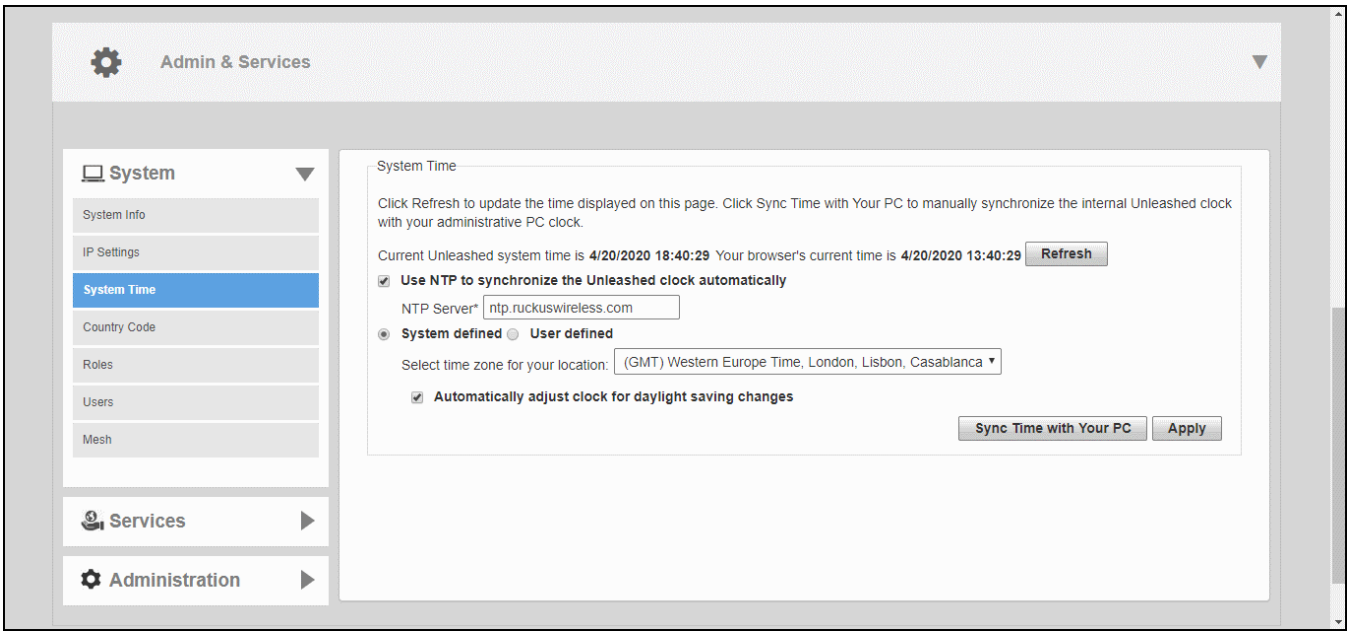
You can also sync time with your PC to manually synchronize the internal clock with the clock of your administration PC.

Complete the following steps to configure the system time:

1. From the dashboard, go to **Admin & Services > System > System Time**.
2. Click **Refresh** to update the display (a static snapshot) from the internal clock.

3. Enable the **Use NTP to synchronize the Unleashed clock automatically** option.

FIGURE 296 Configuring the System Time



4. Configure the **NTP Server**: The default NTP server is maintained by RUCKUS, and is located at *ntp.ruckuswireless.com*. If you would like to use a different NTP server, enter the DNS name or IP address from which Unleashed will sync its clock.
5. Select **System defined** or **User defined** for the time zone. By default, the system-defined time zones are listed in the **Select time zone for your location** list. For information on the user-defined time zone option, refer to Configuring a User-Defined Time Zone on page 389.
6. From the **Select time zone for your location** list, select your time zone. Setting the proper time zone ensures that time stamps on log files are in the proper time zone.
7. Click **Sync Time with Your PC** to update the internal clock with the current time settings from your administration PC if needed.
8. Click **Apply** to save the results of any re-synchronization or NTP server settings changes.

Configuring a User-Defined Time Zone

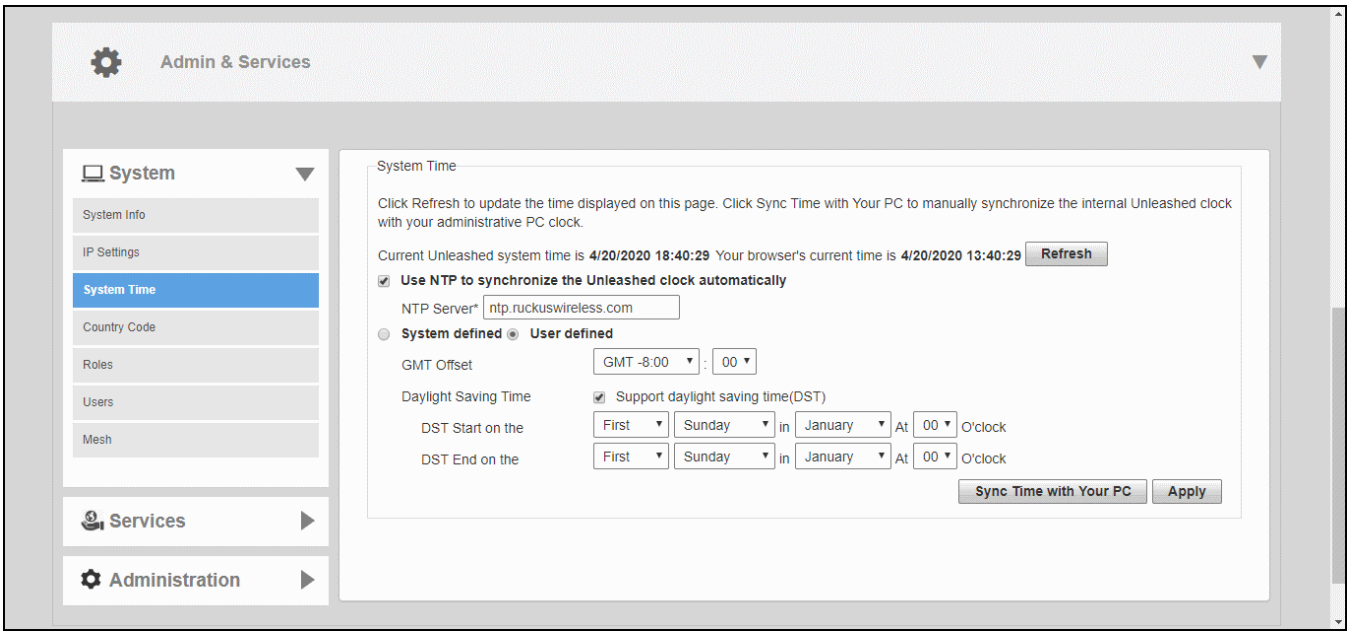
The user-defined time zone option allows the admin to customize the time zone and daylight savings time start and end times.

To configure a user-defined time zone:

1. Go to *Admin & Services* > *System* > *System Time*.
2. Enable **Use NTP to synchronize the Unleashed clock automatically**, and select **User Defined**.
3. Select **GMT Offset** (hours and minutes) away from GMT.
4. Optionally, enable **Daylight Saving Time (DST)**, and enter the DST Start and DST End dates.

5. Click **Apply** to save your changes.

FIGURE 297 Configuring a user-defined time zone



Setting the Country Code

Different countries and regions maintain different rules that govern which channels can be used for wireless communications. Setting the country code to the proper regulatory region ensures that your RUCKUS Unleashed network does not violate local and national regulatory restrictions.

Setting the country code for the Master AP will also set the country code for all member APs under its control.

NOTE
Changes to the country code are applied to all Access Points in the RUCKUS Unleashed network.

NOTE
RUCKUS Unleashed APs sold in the United States are fixed to US country code, and cannot be changed.

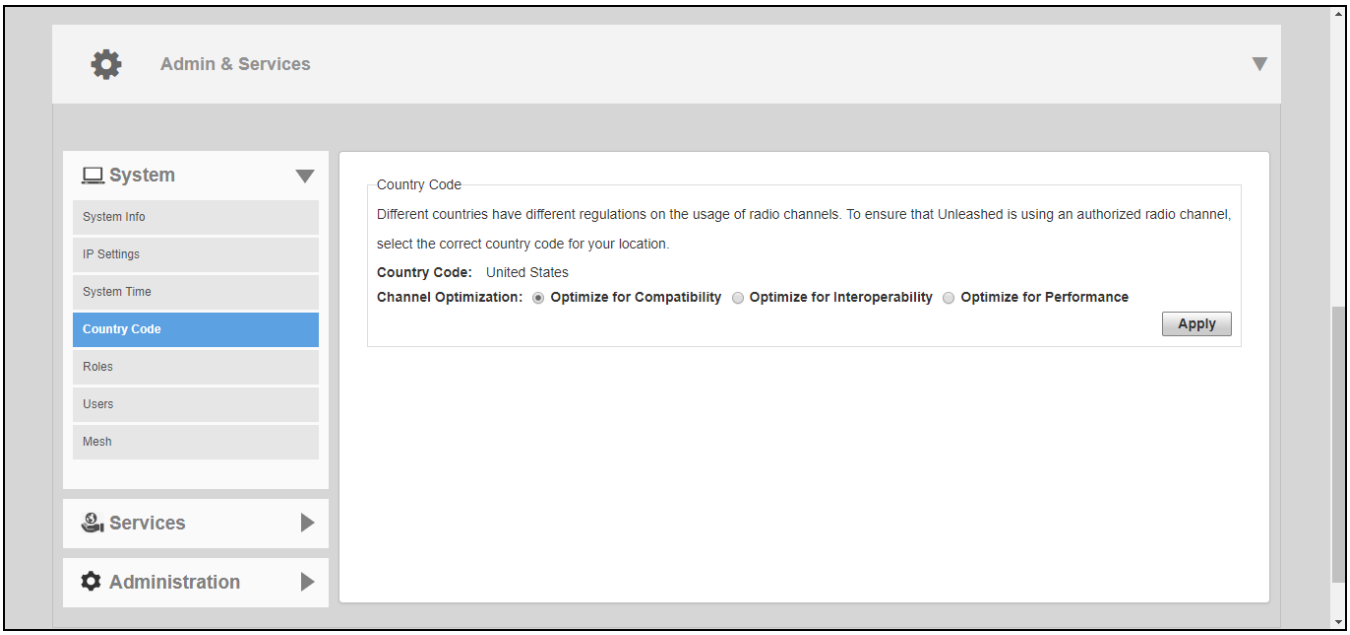
Complete the following steps to set the country code to the proper location:

1. From the dashboard, go to **Admin & Services > System > Country Code**.
2. Choose your location from the **Country Code** drop-down menu.
3. In **Channel Optimization**, select one of the following options:
   - **Optimize for Compatibility**: Allows the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 165 (non-DFS channels).
   - **Optimize for Interoperability**: Allows all non-DFS channels plus channels 52, 56, 58, 60.
   - **Optimize for Performance**: Allows all DFS/non-DFS channels, including 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

NOTE
Note that these settings only affect RUCKUS APs that support the extended DFS channel list.

4. Click **Apply** to save your settings.

FIGURE 298 Setting the Country Code



Channel Optimization

If your Country Code is set to "United States," an additional configuration option, **Channel Optimization**, is shown. This feature allows you to choose whether additional DFS (Dynamic Frequency Selection) channels in the 5 GHz band should be available for use by your APs.

Note that these settings only affect RUCKUS APs that support the extended DFS channel list. Channel Optimization settings are described in the following table.

The 5 GHz channels available for AP use are the following:

- **Optimize for Compatibility**: 36, 40, 44, 48, 149, 153, 157, 161, 165 (non-DFS channels).
- **Optimize for Interoperability**: non-DFS channels plus channels 52, 56, 58, 60.
- **Optimize for Performance**: all DFS + non-DFS channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 149, 153, 157, 161.

TABLE 35 Channel Optimization settings for US Country Code

Setting	Description	Use this setting when
Optimize for Compatibility	DFS-capable Unleashed APs are limited to the same channels as all other APs (non-DFS channels only).	You have a mixture of APs that support DFS channels and other RUCKUS APs that do not support DFS channels in a Smart Mesh configuration.
Optimize for Interoperability	Unleashed APs are limited to non-DFS channels, plus four DFS channels supported by Centrino systems (may not be compatible with other wireless NICs).	You have only DFS-capable APs in your network, or Smart Mesh is not enabled, and you are confident that all wireless clients support DFS channels.
Optimize for Performance	Unleashed APs can use all available DFS and non-DFS channels, without regard for compatibility or interoperability	You have only DFS-capable APs in your network, you are not concerned with DFS compatibility of client devices, and you want to make the maximum use of all possible available channels.

Channel Mode

The Channel Mode option allows you to configure outdoor APs to use channels regulated as indoor-only.

Some countries restrict certain 5 GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15 GHz to 5.25 GHz band to indoor use. When an Unleashed outdoor AP is set to a country code where these restrictions apply, the AP can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment such as a warehouse, the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the web interface by configuring the **Channel Mode** and checking **Allow indoor channels**. If you have an indoor AP functioning as a Root AP with outdoor APs functioning as Mesh APs, the mesh backhaul link must initially use a non-indoor-only channel. Your outdoor Mesh APs may fail to join if the mesh backhaul link is using a restricted indoor-only channel.

Configuring User Roles

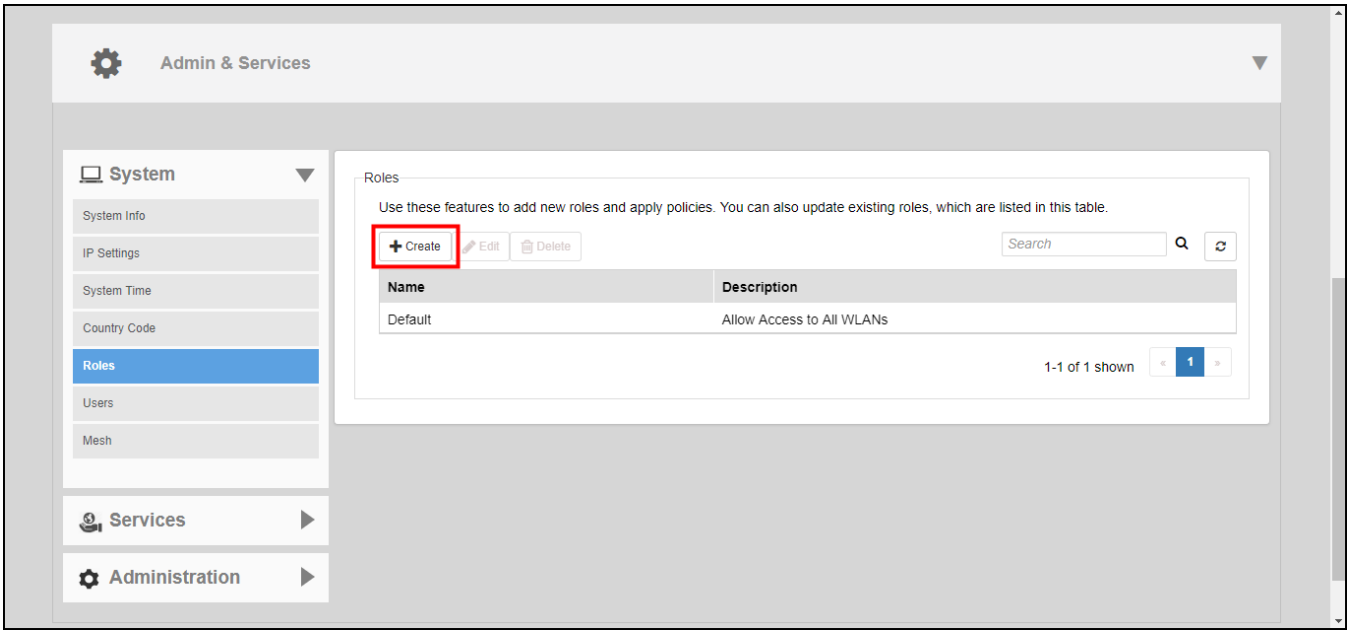
Unleashed provides a "Default" role that is automatically applied to all new user accounts.

This role links all users to the internal WLAN and permits access to all WLANs by default. As an alternative, you can create additional roles that you can assign to selected wireless network users, to limit their access to certain WLANs, to allow them to log in with non-standard client devices, or to grant permission to generate guest passes. (You can then edit the "default" role to disable the guest pass generation option.)

To create a new user Role:

1. Go to **Admin & Services > System > Roles**. The **Roles** page appears, displaying a Default role in the **Roles** table.
2. Click **Create** .

FIGURE 299 Roles



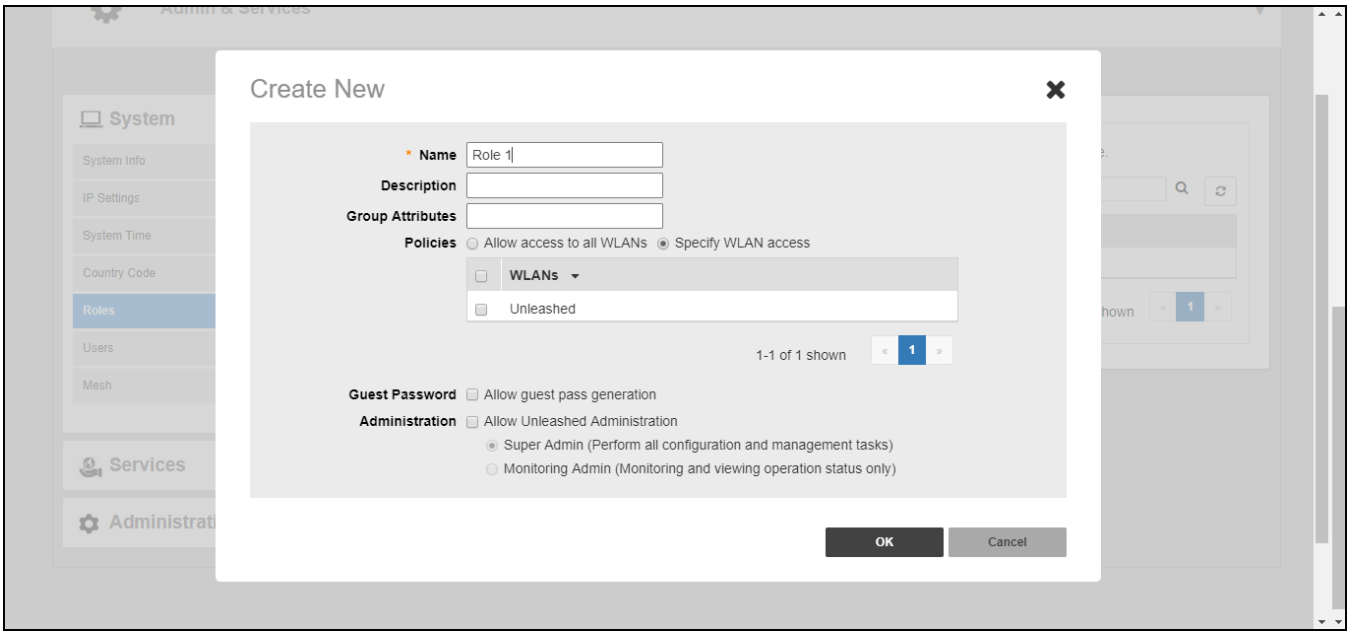
3. Enter a **Name** and a short **Description** for this role.

4. Choose the options for this role from the following:
   - **Group Attributes**: Fill in this field only if you are creating a user role based on Group attributes extracted from an Active Directory server. Enter the User Group name here. Active Directory/LDAP users with the same group attributes are automatically mapped to this user role.
   - **Allow All WLANs**: You have two options: (1) Allow Access to all WLANs, or (2) Specify WLAN Access. If you select the second option, you must specify the WLANs by clicking the check box next to each one.
   - **Guest Pass**: If you want users with this role to have the permission to generate guest passes, enable this option.

     NOTE
     When creating a guest pass generator role, you must ensure that this role is given access to the guest WLAN/s. If you create a role and allow guest pass generation, but do not allow the role access the relevant WLANs, members of the "Guest Pass Generator" Role will be unable to generate guest passes for the guest WLAN.

   - **Administration**: Enable this option to allow this user role admin privileges. Admin privileges are divided into two levels:
     - **Super Admin**: Allows users to perform all configuration and management tasks.
     - **Monitoring Admin**: Allows monitoring and viewing of operating status only.
5. When you finish, click **OK** to save your settings. This role is ready for assignment to authorized users.
6. If you want to create additional roles with different policies, repeat this procedure.

FIGURE 300 Creating a new user Role



Adding New Users to the Local Database

Once the wireless network is set up, you can choose to authenticate wireless users using an external authentication server (Active Directory or RADIUS server), or to authenticate users by referring to accounts that are stored in the system's internal user database.

This section describes the procedures for managing users using the internal user database. For authentication using an external AAA server, see AAA Servers on page 410.

To use the internal user database as the default authentication source and to create new user accounts in the internal database:

1. Go to **Admin & Services > System > Users**.
2. In the **Internal User Database** table, click **Create New**.
3. When the **Create New** form appears, fill in the text fields with the appropriate entries:
   - **User Name**: Enter a name for this user. User names must be 1-32 characters in length, using letters, numbers, underscores (_) and periods (.). User names are case-sensitive and may not begin with a number.
   - **Full Name**: Enter the assigned user's first and last name. The user name can be up to 64 characters, including special characters and spaces.
   - **Password**: Enter a unique password for this user, 4-32 characters in length, using a combination of letters, numbers and special characters including characters from (!) (char 33) to (~) (char 126). Passwords are case-sensitive.
   - **Confirm Password**: Re-enter the same password for this user.
4. If you have created roles that enable non-standard client logins or that gather staff members into workgroups, select the appropriate role for this user from the **Roles** drop-down menu. For more information on roles and their application, see Configuring User Roles on page 392.
5. Click **OK** to save your settings. Be sure to communicate the user name and password to the appropriate end user.

FIGURE 301 The Users Page

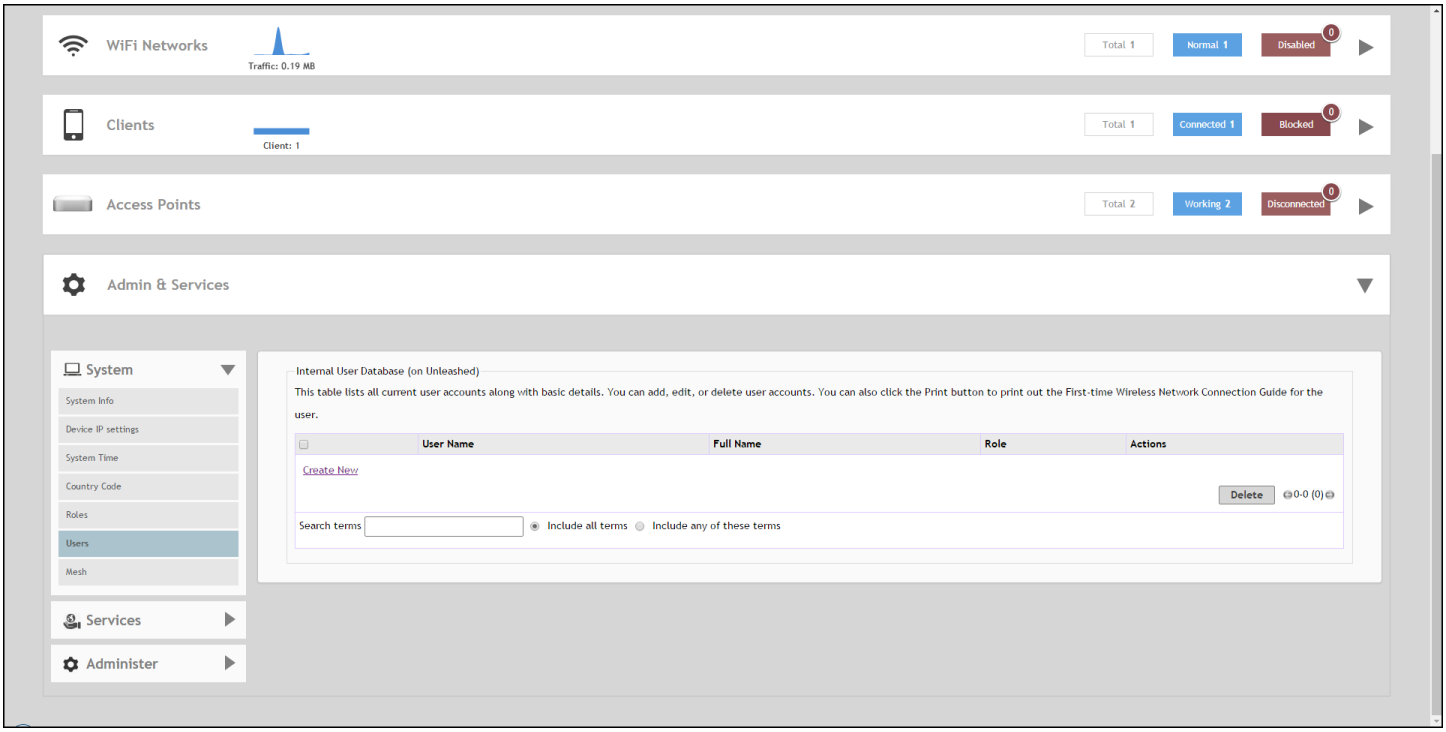
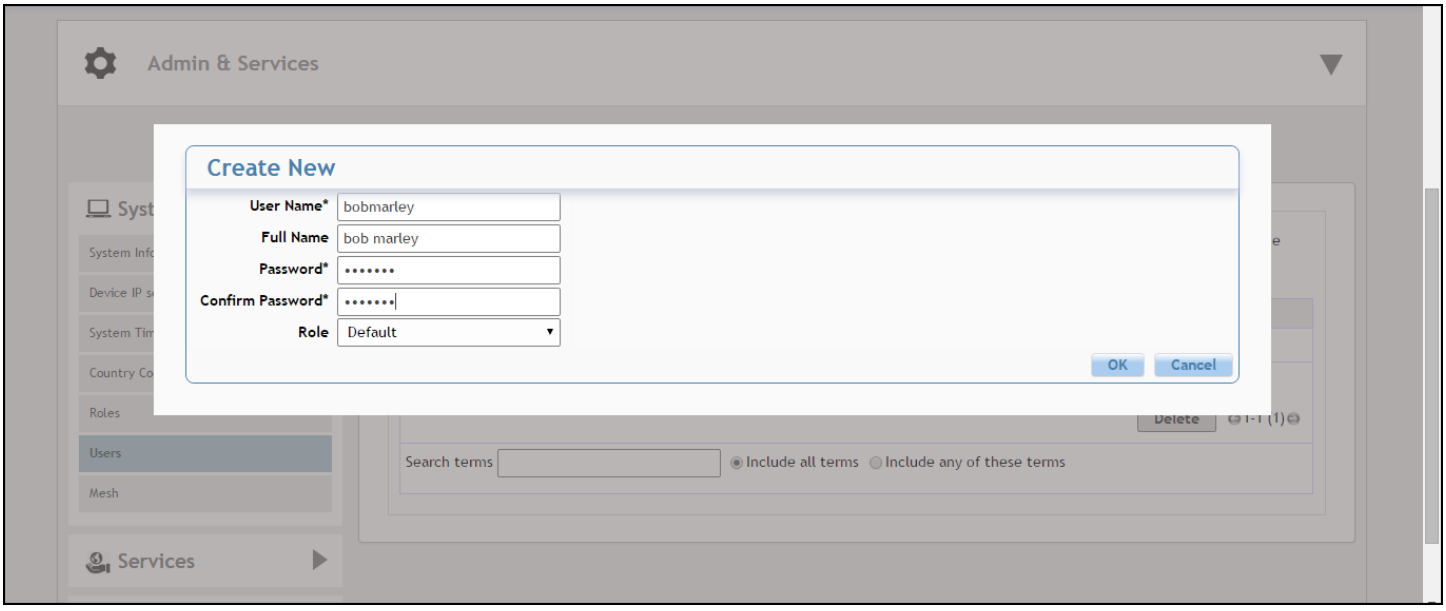


FIGURE 302 Creating a New User on the Internal Database



Changing an Existing User Account

1. Go to **Admin & Services > System > Users**.

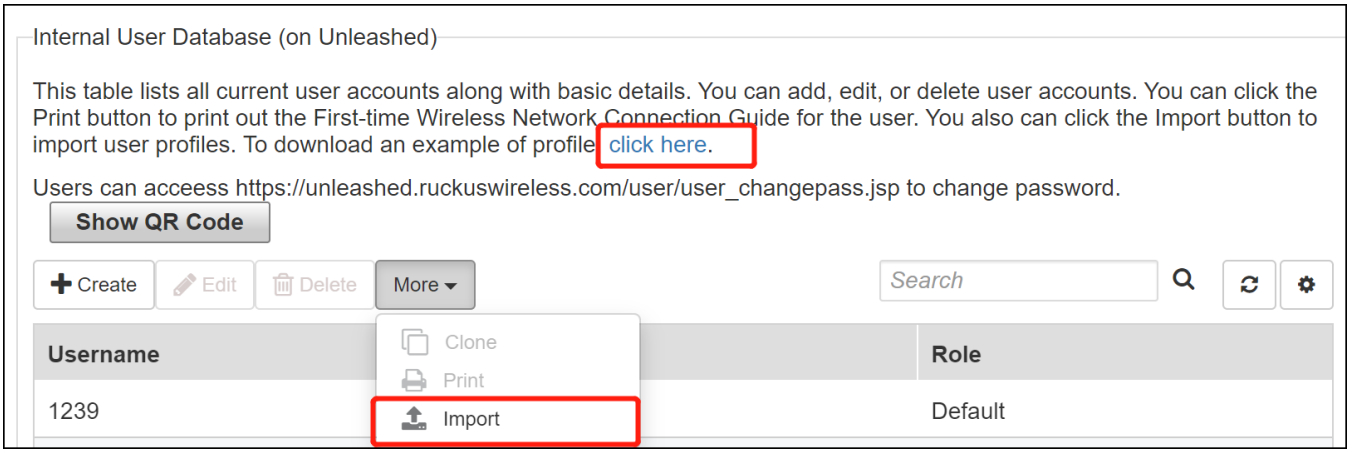
2. When the **Users** features appear, locate the specific user account in the **Internal User Database** table, and then click **Edit**.
3. When the **Editing [user name]** form appears, make the needed changes.
4. If a role must be replaced, select a new **Role** for this user. (For more information, see Configuring User Roles on page 392.)
5. Click **OK** to save your changes. Be sure to communicate the relevant changes to the appropriate end user.

Importing Users into the Local Database using CSV File

1. From the dashboard, select **Admin & Services** > **System** > **Users**.
2. Under **Internal User Database**, click **More** > **Import** to import user profiles.

   You can download a sample user profile using the link in **To download a example of profile, click here**.

FIGURE 303 Importing Users into the Local Database



3. In the **Import User List** window, either drag-and-drop a file within the dotted area or click to upload the file.

FIGURE 304 Importing User List

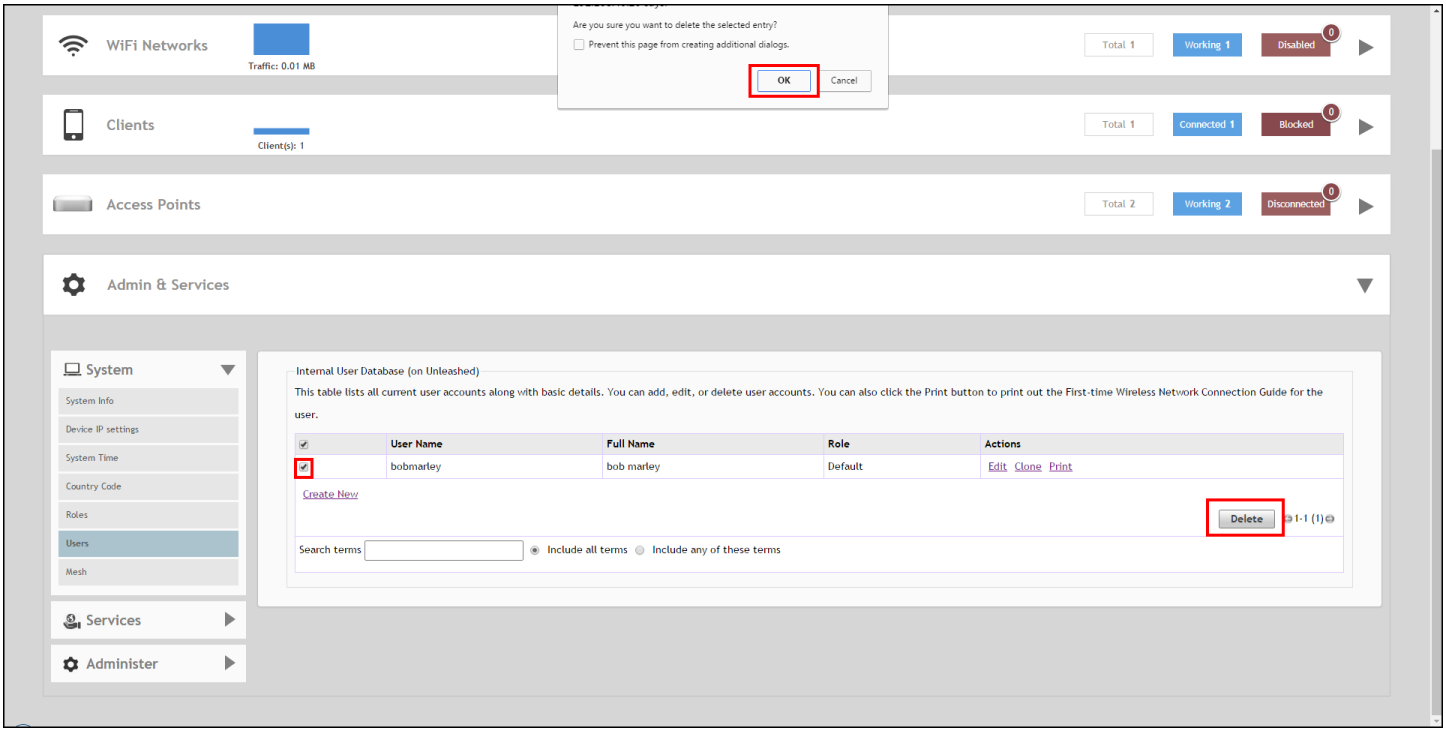
Limitations and Considerations for CSV Import

- A CSV file can contain a maximum of 2048 accounts at one time. A maximum of 2048 accounts are stored in the local database.
- A CSV file must use the following format: UserName,FullName,Password,RoleName.
  - Password can contain only between 4 through 32 characters, and cannot contain "< >" (angle brackets).
  - RoleName must be between 1 through 32 characters and cannot contain "< >" (angle brackets).
  - UserName must be from 1 through 32 characters in length and can consist only of alphanumeric characters, underscore (_), and period (.), and Chinese characters.
  - FullName is not necessary.

Deleting a User Record

1. Go to **Admin & Services > System > Users**.
2. Review the **Internal User Database** table.
3. To delete one or more records, click the check boxes next to those account records, and click the **Delete** button.
4. When the confirmation dialog box appears, click **OK** to save your settings. The records are removed from the internal user database.

FIGURE 305 Deleting a user from the internal database



Changing User Password

Users can change their account passwords without the aid of the administrator. Syslog maintains a record of the users who have changed their passwords, which reduces the workload of the administrator.

1. Go to https://unleashed.ruckuswireless.com/user/user_changepass.jsp or scan the QR code to reset the password.

2. In the **Change your password** dialog box, enter the following information:
   a) For **Username**, enter your username.

      The username must be from 1 through 32 characters in length and can consist only of alphanumeric characters, underscore (_), period (.), and Chinese characters.

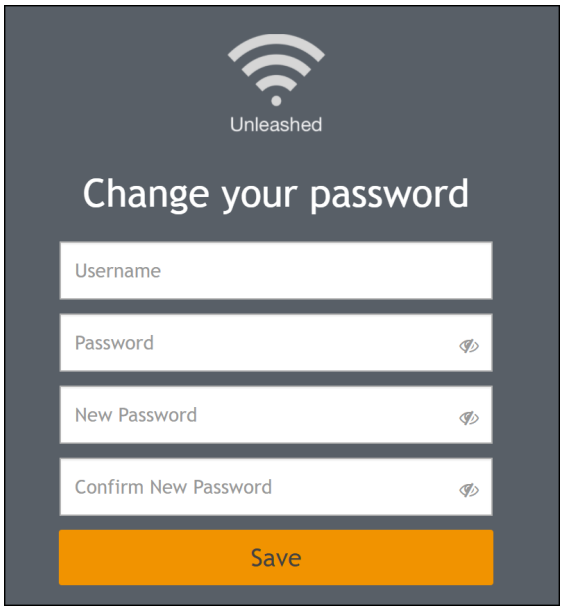
   b) For **Password**, enter your current password.

      The password must be from 4 through 32 characters in length. The usage of a pair of special characters "< >" (angle brackets) is limited, but you can use the characters separately.

   c) For **New Password**, enter your new password.

   d) For **Confirm New Password**, enter your new password again.

   FIGURE 306 Changing the Password for a Local Database User



3. Click **Save** to save the changes.

   NOTE
   If the authentication failed three times within five minutes, the login is disabled for three minutes.

Mesh Networking

Overview of Smart Mesh Networking

A Smart Mesh network is a peer-to-peer, multi-hop wireless network wherein participant nodes cooperate to route packets.

In a RUCKUS Smart Mesh network, the routing nodes (that is, the access points forming the network), or "mesh nodes," form the network's backbone. Clients connect to the mesh nodes and use the backbone to communicate with one another, and, if permitted, with nodes on the internet. The mesh network enables clients to reach other systems by creating a path that "hops" between nodes.

Smart Mesh networking offers many advantages:

- Smart Mesh networks are self-healing: If any one of the nodes fails, the nodes note the blockage and re-route data.
- Smart Mesh networks are self-organizing: When a new node appears, it becomes assimilated into the mesh network.

In the RUCKUS Smart Mesh network, all traffic going through the mesh links is encrypted. A passphrase is shared between mesh nodes to securely pass traffic. When deployed as a mesh network, member APs communicate with the Master AP either through a wired Ethernet connection (Root APs) or through the wireless connection using the 5 GHz radio (Mesh APs).

Smart Mesh Networking Terms

Before you begin deploying your Smart Mesh network, RUCKUS recommends getting familiar with the following terms that are used in this document to describe wireless mesh networks.

TABLE 36 Mesh Networking Terms

Term	Definition
Mesh Node	A RUCKUS Unleashed AP with mesh capability enabled.
Root AP (RAP)	A mesh node that communicates with the Master AP through its Ethernet (wired) interface. The Master AP itself must also be a Root AP.
Mesh AP (MAP)	A mesh node that communicates with the Master AP through its wireless interface by way of a Root AP.
Ethernet-Linked Mesh AP (eMAP)	An eMAP is a mesh node that is connected to its uplink AP through a wired Ethernet cable, rather than wirelessly. eMAP nodes are used to bridge wireless LAN segments together.
Mesh Tree	Each Mesh AP can have exactly one uplink to a Root AP or another Mesh AP, and each Root AP or Mesh AP can have multiple Mesh APs connected to it, resulting in a tree-like topology. A single Master AP can manage more than one mesh tree. There is no limit on the number of mesh trees per RUCKUS Unleashed Master AP. For example, a RUCKUS Unleashed network can consist of 1 mesh tree of 6 APs, 2 mesh trees of 3 APs each, or 3 mesh trees of 2 APs each.
Hop	The number of wireless mesh links a data packet takes from one Mesh AP to the Root AP. For example, if the Root AP is the uplink of Mesh AP 1, then Mesh AP 1 is one hop away from the Root AP. In the same scenario, if Mesh AP 1 is the uplink of Mesh AP 2, then Mesh AP 2 is two hops away from the Root AP. A maximum of 8 hops is supported.

Refer to Supported Mesh Topologies on page 400 for more information.

Supported Mesh Topologies

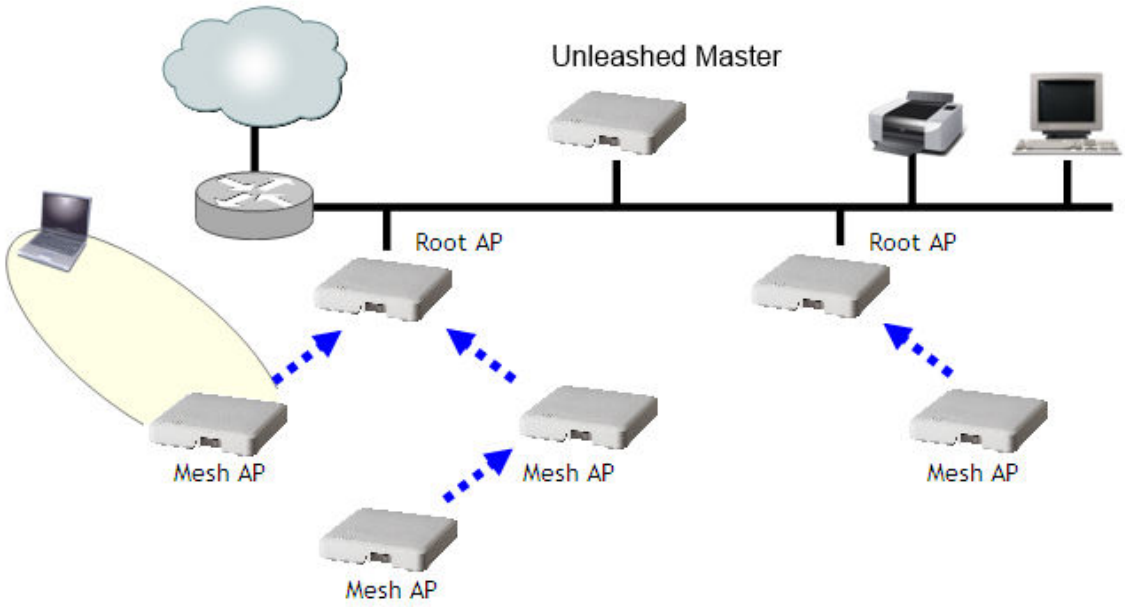
Smart Mesh networks can be deployed in three types of topologies:

- Standard Topology
- Wireless Bridge Topology
- Hybrid Mesh Topology

Standard Topology

The standard Smart Mesh topology consists of the Unleashed Master AP and a number of Root APs and Mesh APs. In this topology, the Unleashed Master and the upstream router are connected to the same wired LAN segment. You can extend the reach of your wireless network by forming and connecting multiple mesh trees to the wired LAN segment. In this topology, all APs connected to the wired LAN are considered "Root APs," and any AP not connected to the wired LAN is considered a "Mesh AP."

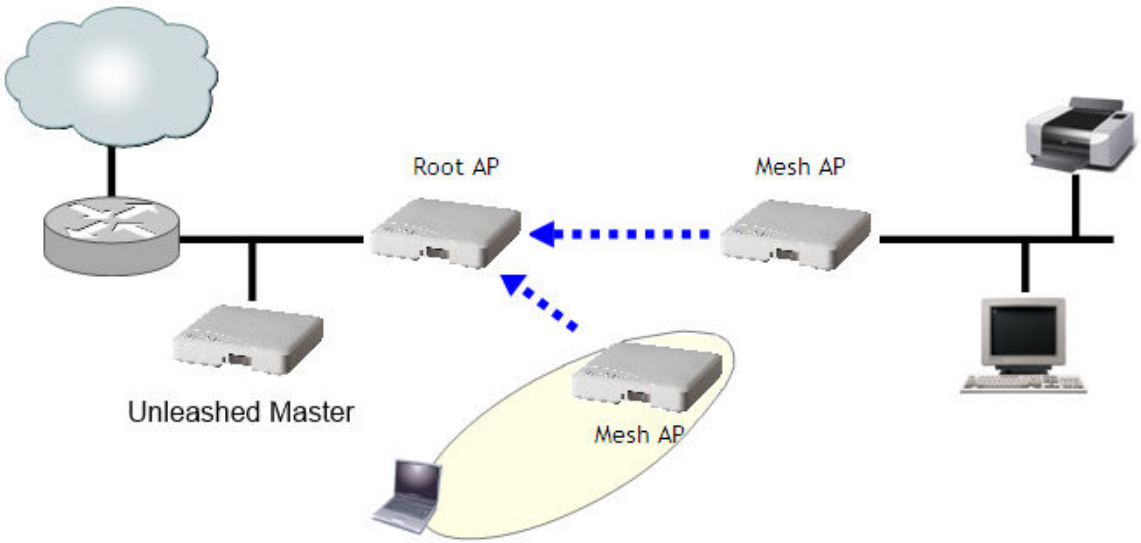
FIGURE 307 Mesh - standard topology



Wireless Bridge Topology

If you need to bridge isolated wired LAN segments, you can set up a mesh network using the wireless bridge topology. In this topology, the Unleashed Master and the upstream router are on the primary wired LAN segment, and another isolated wired segment exists that needs to be bridged to the primary LAN segment. You can bridge these two wired LAN segments by forming a wireless mesh link between the two wired segments, as shown in the figure below.

FIGURE 308 Mesh - wireless bridge topology



Hybrid Mesh Topology

A third type of network topology can be configured using the Hybrid Mesh concept.

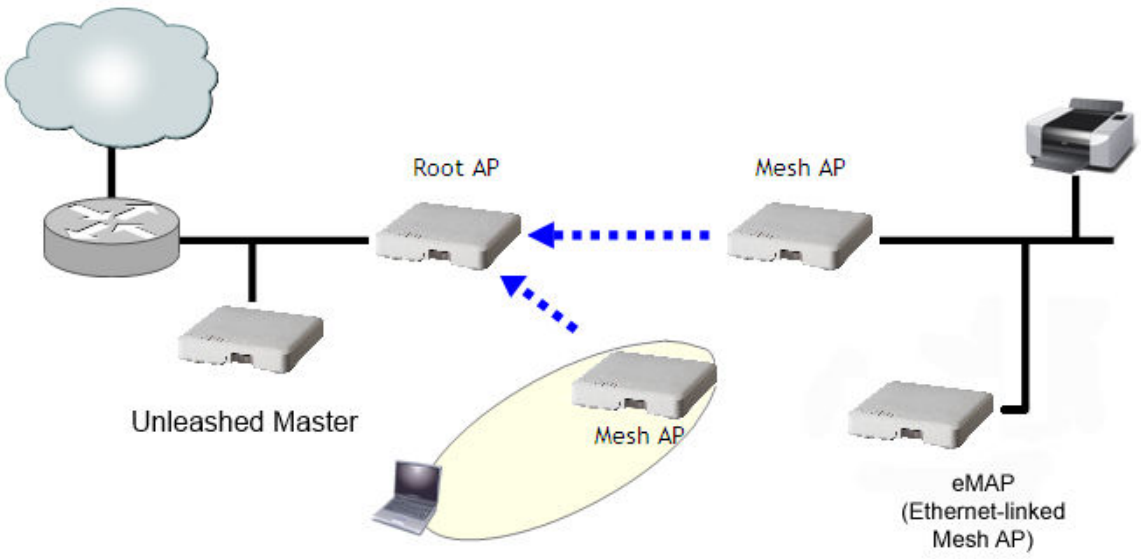
Ethernet-linked Mesh APs (eMAP) enable the extension of wireless mesh functionality to a wired LAN segment. An eMAP is a special kind of Mesh AP that uses a wired Ethernet link as its uplink rather than wireless. An eMAP is not considered a Root AP, despite the fact that it discovers the Unleashed Master through its Ethernet port.

Multiple eMAPs can be connected to a single Mesh AP to, for example, bridge a wired LAN segment inside a building to a wireless mesh outdoors.

In designing a mesh network, connecting an eMAP to a Mesh AP extends the Smart Mesh network without expending a wireless hop, and the eMAP can be set on a different channel to take advantage of spectrum reuse.

NOTE
The Unleashed Master AP cannot be an eMAP.

FIGURE 309 eMAP - Hybrid Mesh topology



Configuring Mesh Settings

You can configure Mesh settings from the **Admin & Services > System > Mesh** page.

To configure Mesh settings, select **Enable Mesh**. Optionally, you can change the **Mesh Name (ESSID)** and the **Mesh Passphrase**, or click **Generate** to generate a new random Mesh passphrase. Under **Mesh Radio Option**, select **2.4 GHz** or **5 GHz**.

NOTE
Once you have enabled Mesh, you cannot disable it again without resetting the Master AP to factory defaults (see Restore to Factory Settings on page 465).

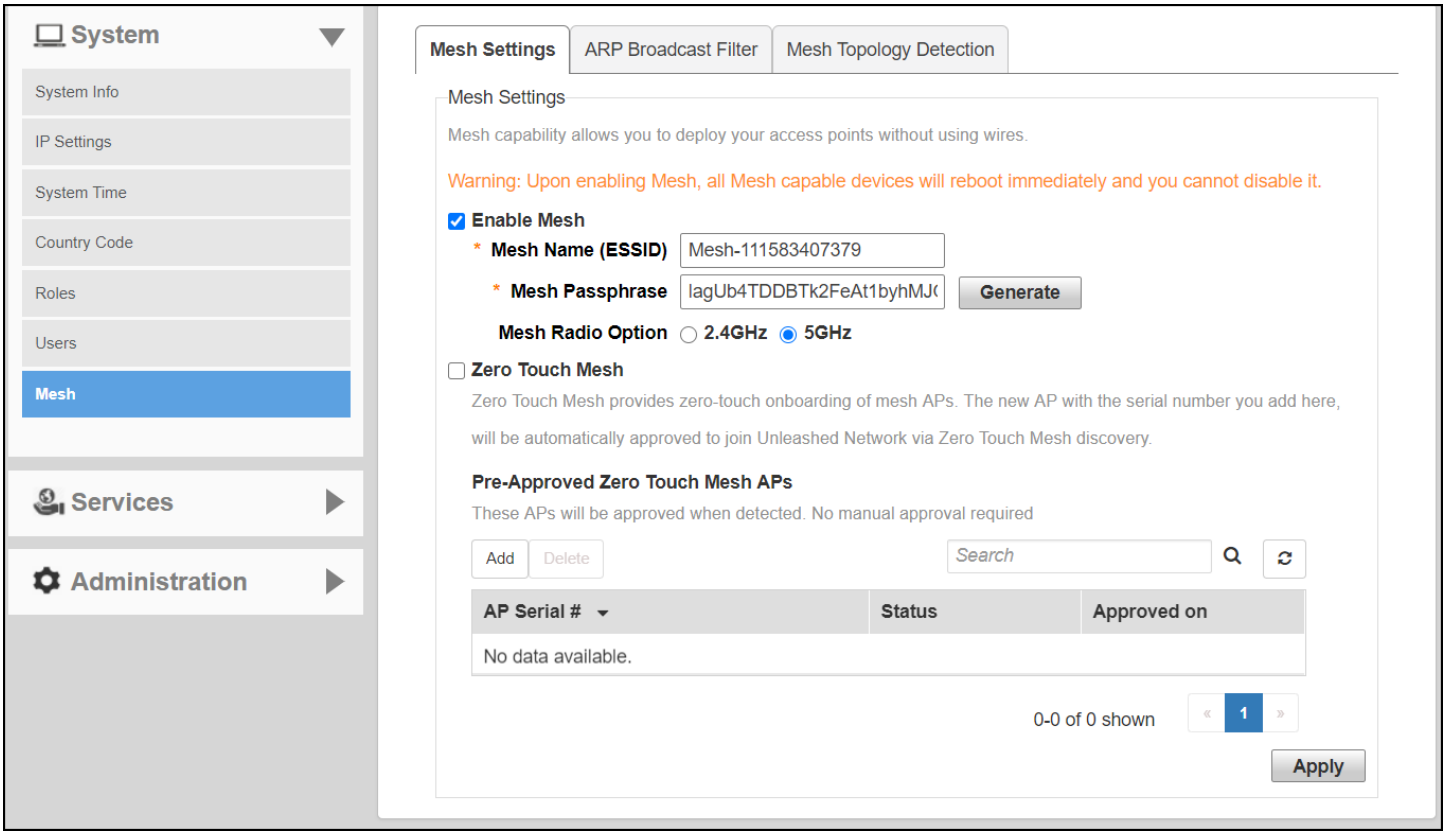
NOTE
If you enabled Mesh during the Setup Wizard process, you do not need to configure it again here.

NOTE
The Master AP cannot be a Mesh AP. The Master AP can only be a Root AP in a Mesh topology.

NOTE
2.4-GHz mesh radio does not support Zero Touch Mesh.

NOTE
Unleashed H320 does not support Mesh.

FIGURE 310 Mesh Settings



Zero Touch Mesh

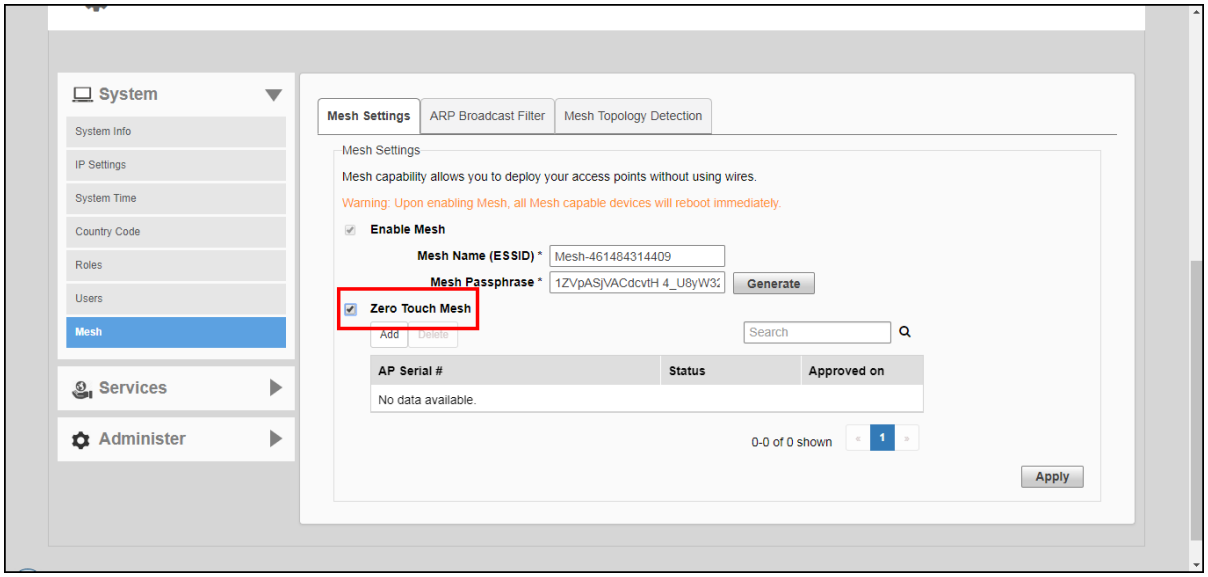
Zero Touch Mesh allows customers to skip the mesh configuration priming process, enabling Mesh APs already installed in their permanent locations to auto-discover, auto-provision and auto-form a mesh network without priming.

In most installations, Unleashed APs that are destined to become Mesh APs need to first be primed prior to deployment. They are first manually connected to the controller (Unleashed Master AP) via Ethernet to receive the provisioning parameters (Mesh SSID and PSK passphrase), and then unplugged from Ethernet and installed at their desired location.

Once installed, Mesh APs perform network discovery and associate to another Mesh AP (RAP, MAP or eMAP) that is beaconing the provisioned Mesh SSID.

This manual procedure can be skipped using the Zero Touch Mesh feature.

FIGURE 311 Enabling Zero Touch Mesh



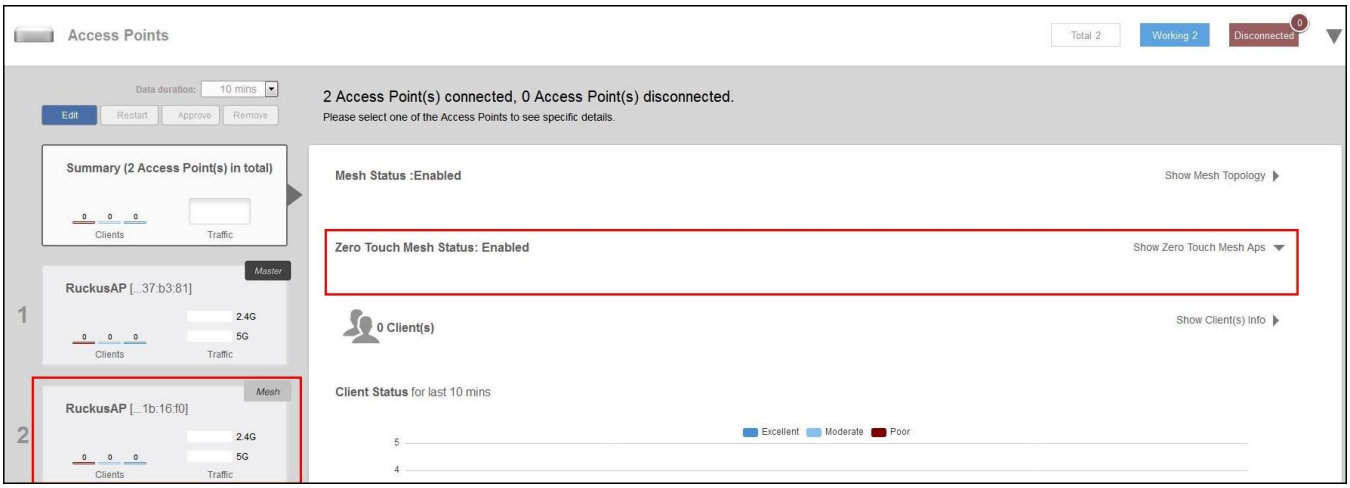
Onboarding Mesh APs with Zero Touch Mesh

To allow Unleashed Mesh APs to join the Mesh network without first connecting them via Ethernet, use the following procedure:

1. Go to **Admin & Services > System > Mesh**.
2. Select the check box to enable **Zero Touch Mesh**.
3. Click **Apply**.

   The changes to the mesh settings will propagate through the mesh network.
4. Go to **Access Points > Summary > Show Zero Touch Mesh APs**.

   FIGURE 312 Show Zero Touch Mesh APs



5. When a supported AP attempts to join, it will appear in the *Zero Touch Mesh AP* table. Click the **Approve** button to approve the AP.

FIGURE 313 Waiting for connection

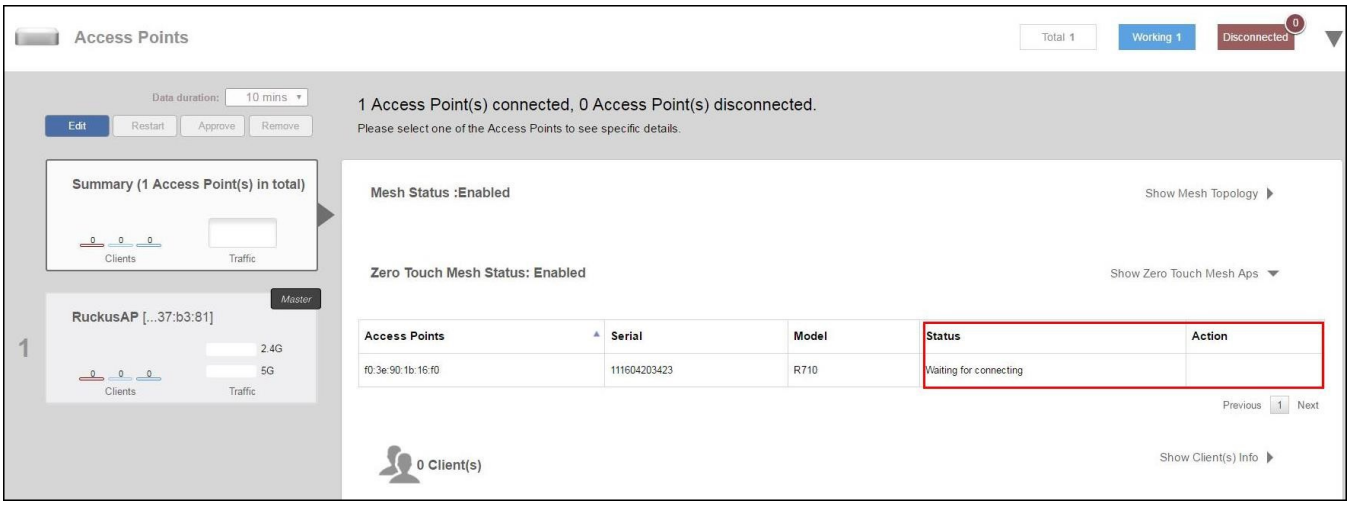
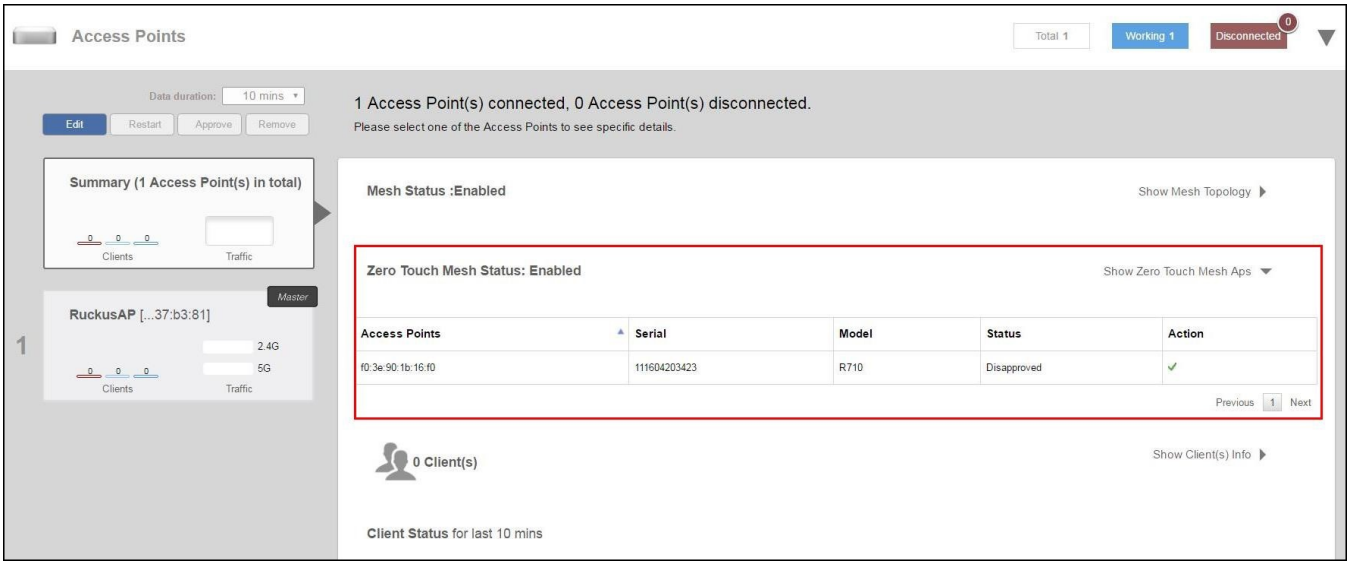


FIGURE 314 Click Approve to allow the AP to join

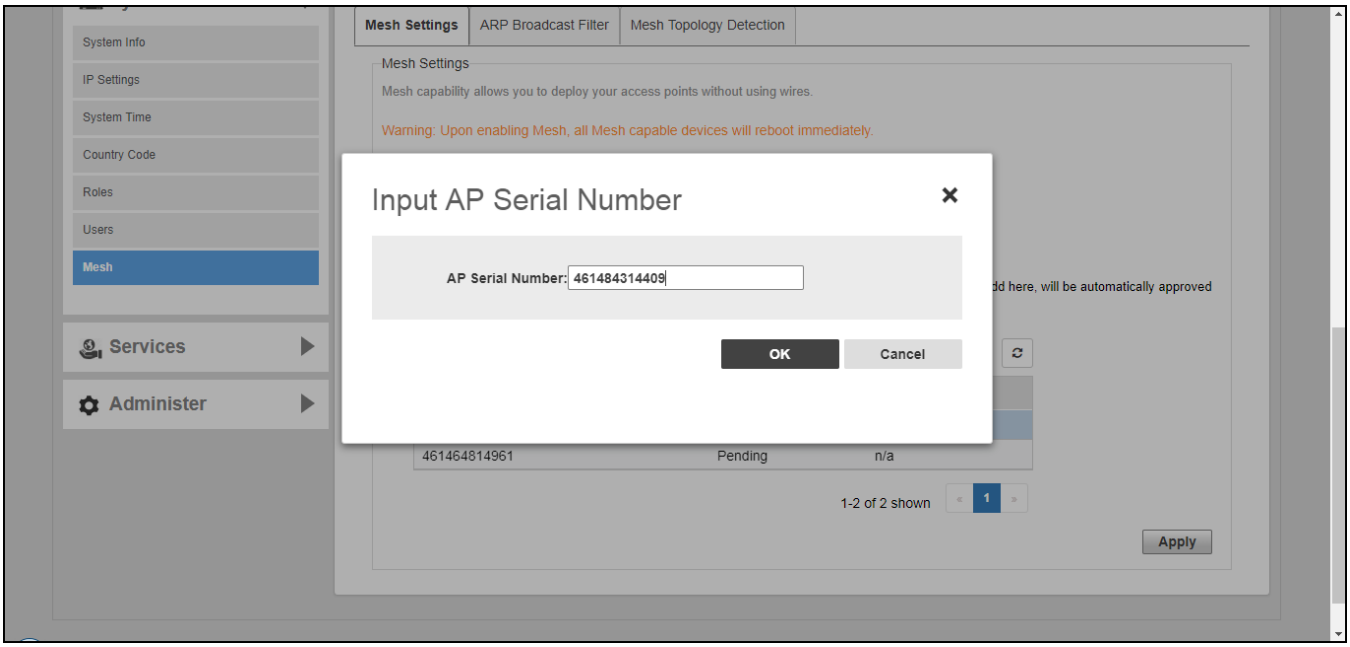


6. To pre-approve APs by serial number, go to **Admin & Services > System > Mesh > Zero Touch Mesh**, and locate the *Pre-Approved Zero Touch Mesh* section.
7. In the same section, click the **Add** button to add a new AP to the list of pre-approved Zero Touch Mesh APs.

   The *Input AP Serial* window appears.

8. Enter the **AP Serial Number** of the AP to autoprovision, and click **OK**.

   FIGURE 315 Add AP serial number



   The AP's serial number is added to the list.

9. Repeat for additional mesh APs.
10. Click **Apply**.

    A message box appears notifying you that the process may take several minutes for the changes to propagate through the mesh network.

11. When the listed APs in factory default state come online, they will begin performing network discovery, auto-provisioning and finally association to another upstream AP the Unleashed network.

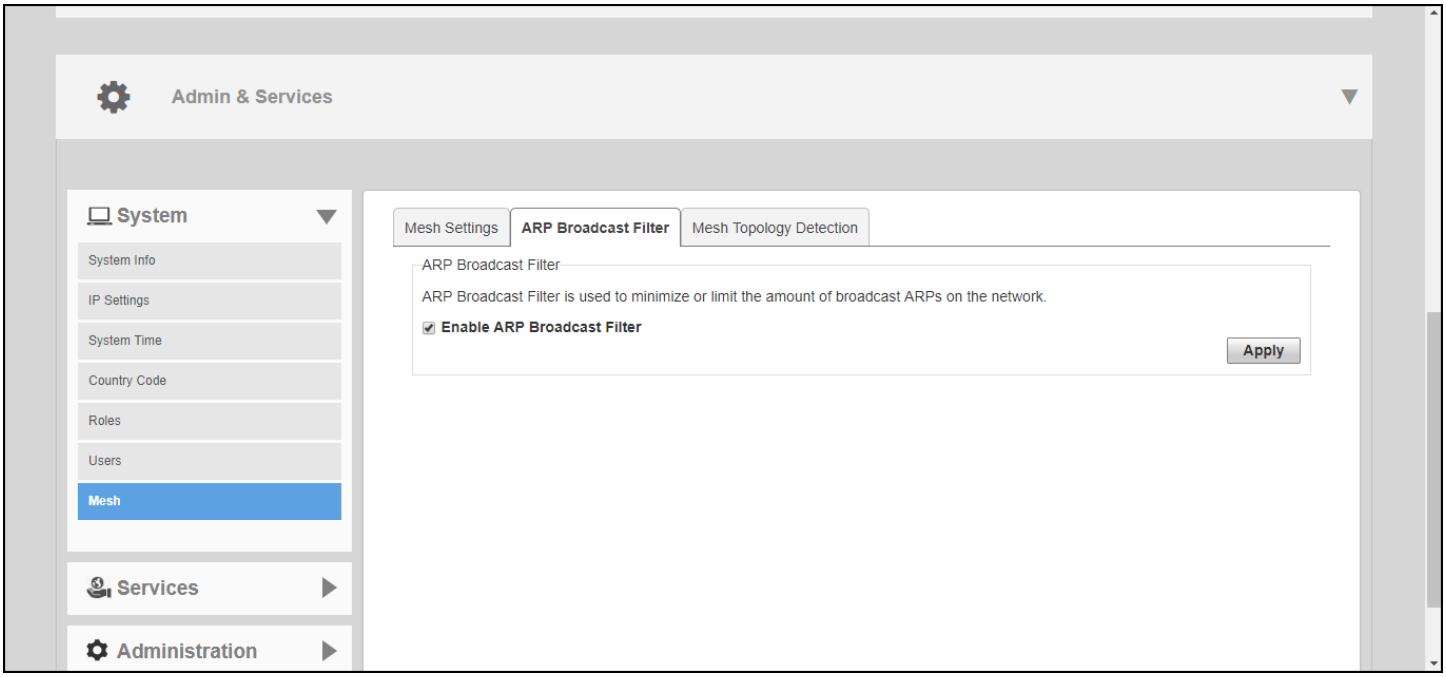
ARP Broadcast Filter

The ARP Broadcast Filter is used to minimize or limit the amount of broadcast ARP (Address Resolution Protocol) packets on the network.

The ARP Broadcast filter is designed to reduce IPv4 ARP broadcasts over the air. Once enabled, access points will sniff ARP responses and maintain a table of IP addresses to MAC address entries. When the AP receives an ARP broadcast request from a known host, the AP converts the broadcast request packet into a unicast request by replacing the broadcast address with the MAC address.

To enable ARP Broadcast Filter, select the check box and click **Apply**.

FIGURE 316 ARP Broadcast Filter



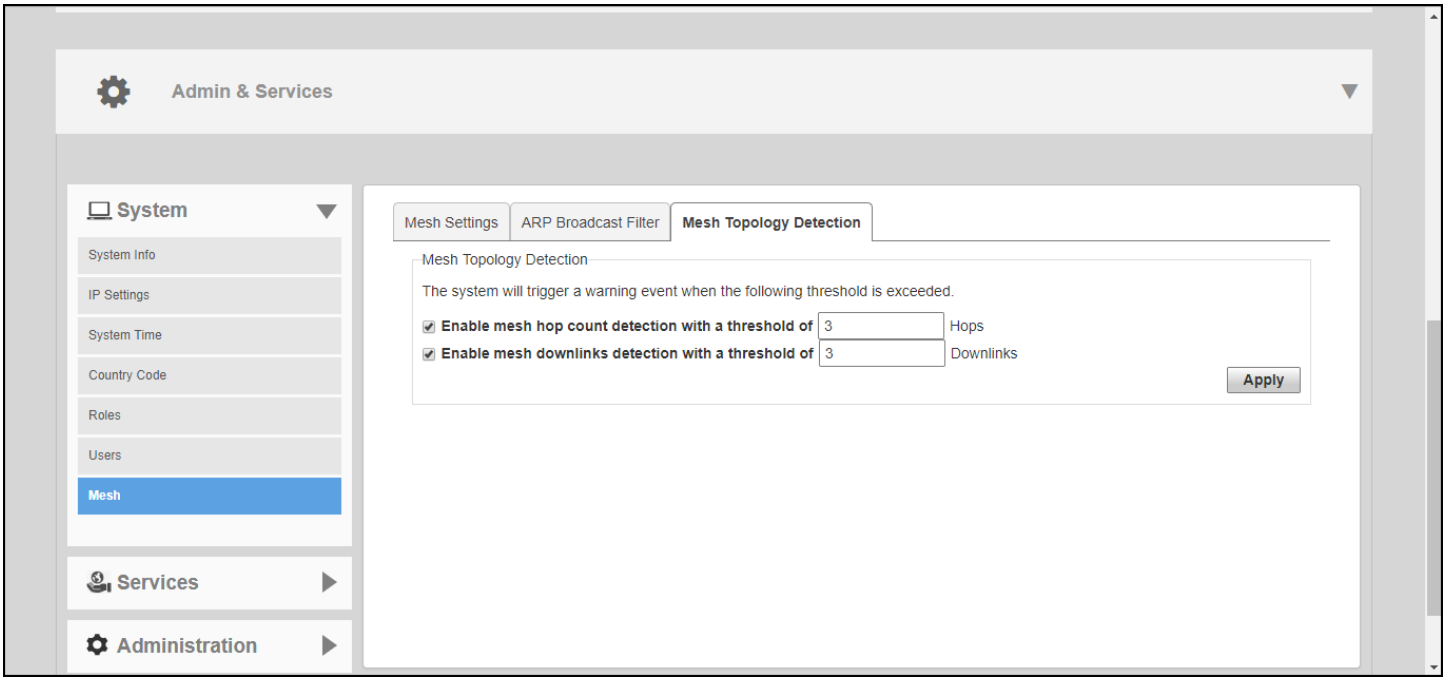
Mesh Topology Detection

The Mesh Topology Detection feature allows you to set the number of mesh hops and mesh downlinks after which Unleashed will trigger a warning message.

For example, if you enable both options with a threshold value of 3 for each (default), Unleashed will trigger a warning event message when either of the following events occurs:

- A Mesh AP with 4 or more hops from a Root AP is detected.
- A Root AP with 4 or more downlink Mesh APs connected to it is detected.

FIGURE 317 Mesh Topology Detection



Enabling Log Delivery to Remote Syslog Server

Unleashed's internal log files can be configured for automatic delivery to a remote syslog server.

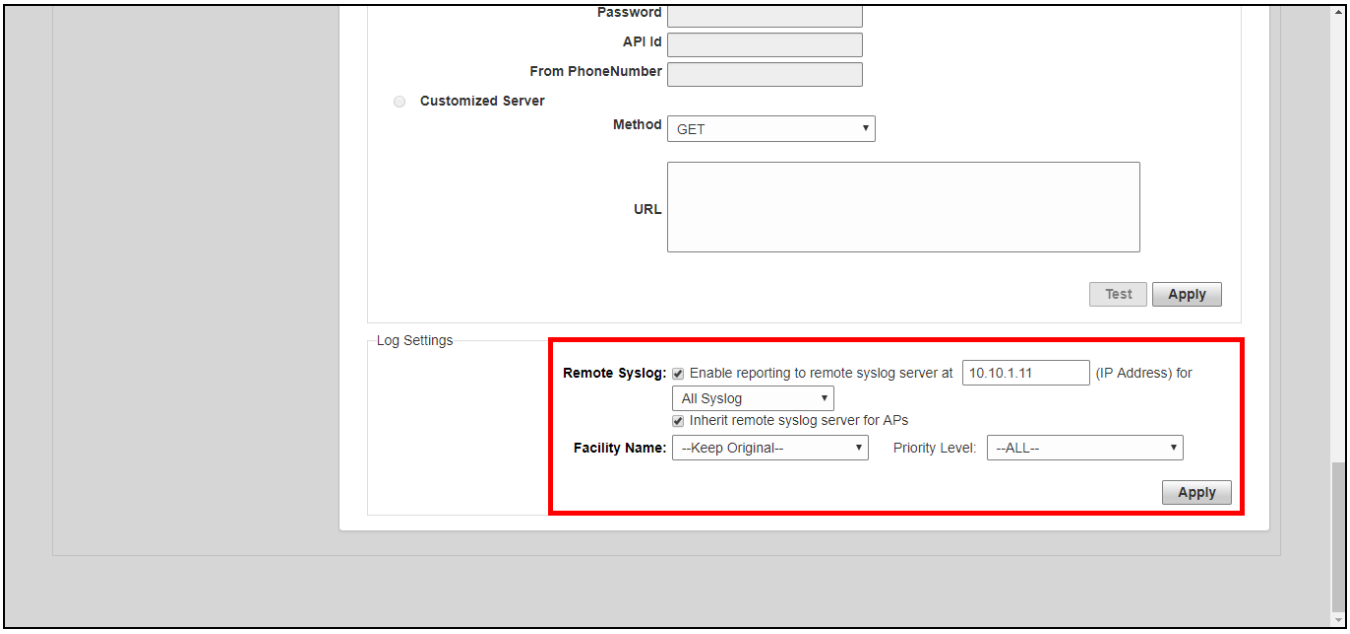
To enable log file delivery to a remote syslog server:

1. Go to **Admin & Services > System > System Info**, and scroll down to the *Log Settings* section at the bottom of the page.
2. Enable the **Remote Syslog** option and enter the IP address of the syslog server in the field provided.
3. Select one of the following options to control the content of the logs:
   - **All Syslog**: The controller sends all syslog messages configured in the *Debug Logs* section of the *Admin & Services > Administration > Diagnostics > Debug Info* page.
   - **Client Connection Logs Only**: The controller sends client connection logs only to the syslog server.
   - **Client Flow Data Only**: The controller sends client flow data only to the syslog server.
4. Optionally, enable the **Inherit remote syslog server for APs** option.

   Enabling this feature allows the controller to supply client association information to a third party application that can then deploy ACL policies to a firewall based on client association information such as user name, IP, MAC address, etc. First, Unleashed retrieves client association information, then reorganizes the information and sends it to the syslog server, from which it can be collected by the third party software and sent to the firewall for access restrictions based on client association information.
5. Configure the **Facility Name** as follows:
   - **Keep Original**: Retain the original facility name.
   - **local0 - local7**: Specify facility name.

6. Set the **Priority Level** as follows:
   - **All**: Include all syslog messages.
   - 0(emerg), 1(alert), 2(crit), 3(err), 4(warning), 5(notice), 6(info), 7(debug): Lower numbers indicate higher priority. The syslog server will only receive logs whose priority levels are the same as or higher than the configured level.

FIGURE 318 Configuring syslog settings

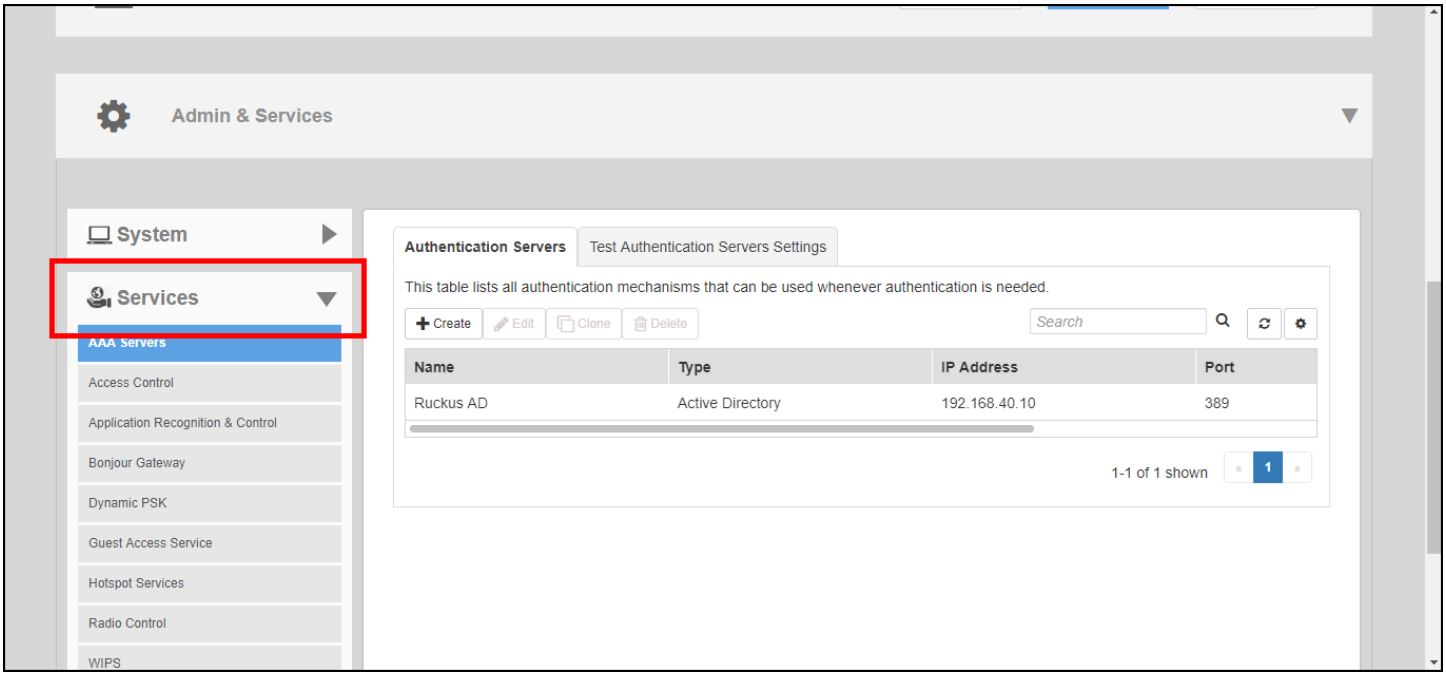


Services

The *Services* pages include options for configuring system services such as Application Recognition and Control, Bonjour Gateway, DPSK, Hotspot service and Guest Access services.

To configure system services, go to **Admin & Services > Services**.

FIGURE 319 The Admin & Services > Services page



AAA Servers

If you want to authenticate users against an external Authentication, Authorization and Accounting (AAA) server, you will need to first configure your AAA server, then point Unleashed to the AAA server so that requests will be passed through Unleashed before access is granted. This section describes the tasks that you need to perform on the Unleashed web interface to ensure your Unleashed APs can communicate with your AAA server.

For specific instructions on AAA server configuration, refer to the documentation that is supplied with your server.

Unleashed supports two types of AAA server:

- Microsoft Active Directory
- RADIUS

A maximum of 32 AAA server entries can be created, regardless of server type.

Configuring AAA Servers

Complete the following steps to configure RUCKUS Unleashed to authenticate users against an external Active Directory or RADIUS authentication server:

1. Go to **Admin & Services > Services > AAA Servers**.
2. In **Authentication Servers**, click **Create New**.
3. Enter the name for the AAA server.

4. Under **Type**, select the server type:
   - **Active Directory**: If you use a Microsoft AD server, configure the following settings:
     - **Global Catalog**: Enable Global Catalog for multi-domain AD authentication. If this option is enabled, you must also enter an Admin DN and Password so that RUCKUS Unleashed can query the Global Catalog.
     - **Encryption**: select Enable TLS encryption if you want to encrypt all authentication traffic between the client and the Active Directory server. The AD server must support TLS1.0, TLS1.1, or TLS1.2.
     - **Server Address**: Enter the IP address or the domain name of the AD server.
     - **Port**: The default port number (389, or 636 if you have enabled TLS encryption) should not be changed unless you have configured your AD server to use a different port.
     - **Windows Domain Name**: Enter a domain name for single domain authentication, or leave blank for multi-domain authentication.
   - **RADIUS**: If your authentication server is a RADIUS server, configure the following settings:
     - **Encryption**: If you want to enable encryption of RADIUS packets using Transport Layer Security (TLS), select the Enable TLS encryption check box. This allows RADIUS authentication and accounting data to be passed safely across insecure networks such as the Internet.
     - **Auth Method**: Choose PAP or CHAP according to the authentication protocol used by your RADIUS server.
     - **Backup RADIUS**: If a backup RADIUS or RADIUS Accounting server is available, enable the check box next to Backup RADIUS and additional fields appear. Enter the relevant information for the backup server and click **OK**. When you have configured both a primary and backup RADIUS server, an additional option is available in the Test Authentication Settings section to choose to test against the primary or the backup RADIUS server.
     - **Server Address**: Enter the IP address or the domain name of the RADIUS server (and backup RADIUS server, if enabled).
     - **Port**: The default port (1812) should not be changed unless you have configured your RADIUS server to use a different port.
     - **Shared Secret**: Enter a password for communication between RUCKUS Unleashed and the RADIUS server.
     - **Confirm Secret**: Repeat the shared secret.
     - **Retry Policy**: Enter a request timeout value (in seconds) and maximum number of retries value in the relevant fields.

       NOTE
       If Backup RADIUS is disabled, enter a value for **Max Number of Consecutive Drop Packets** and **Reconnect Primary** (in minutes).

5. Click **OK** to save your AAA server entry.

FIGURE 320 The AAA Servers Page

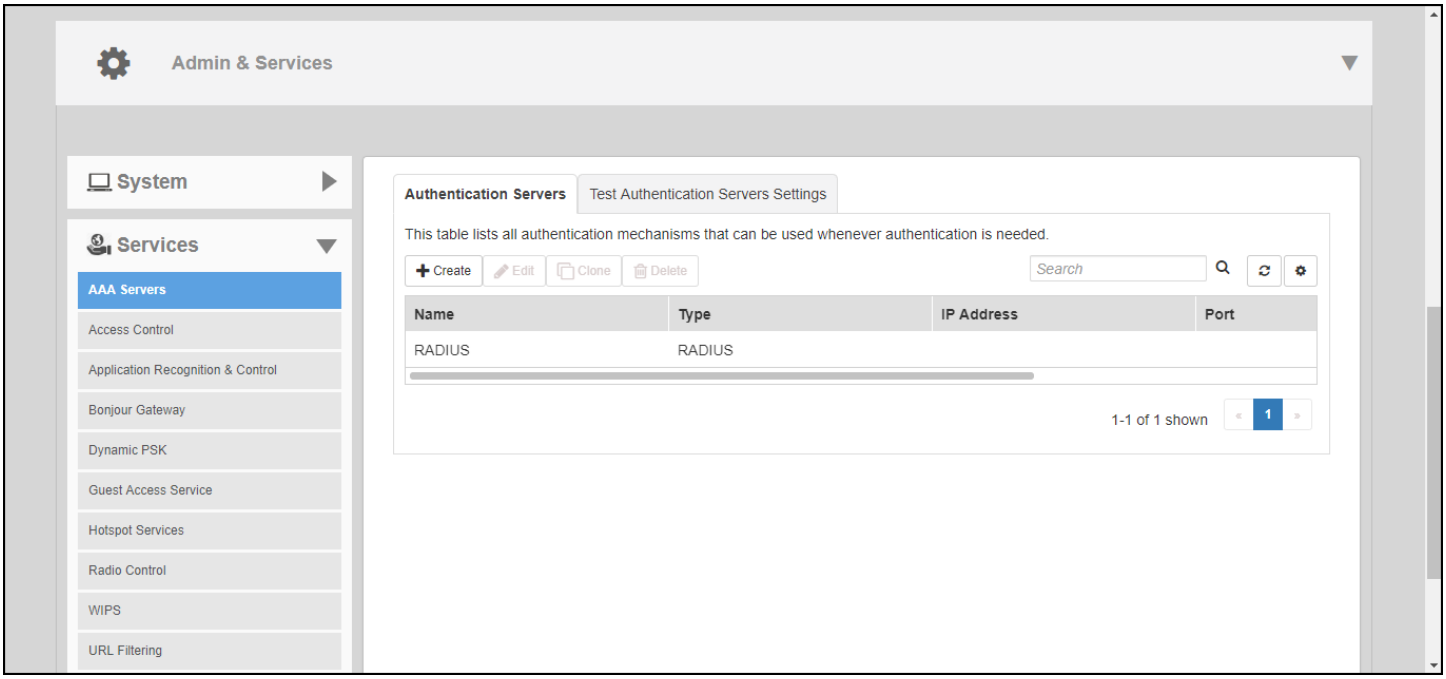


FIGURE 321 Microsoft Active Directory Server Configuration

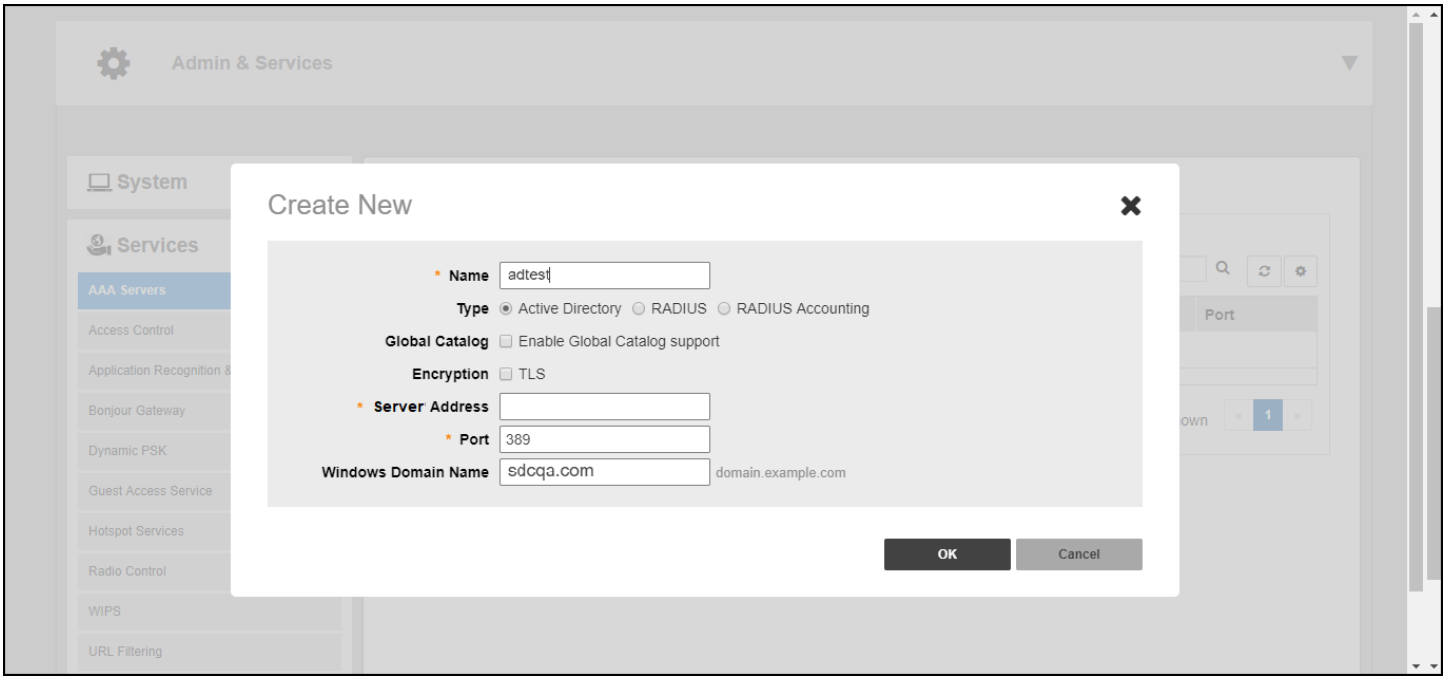
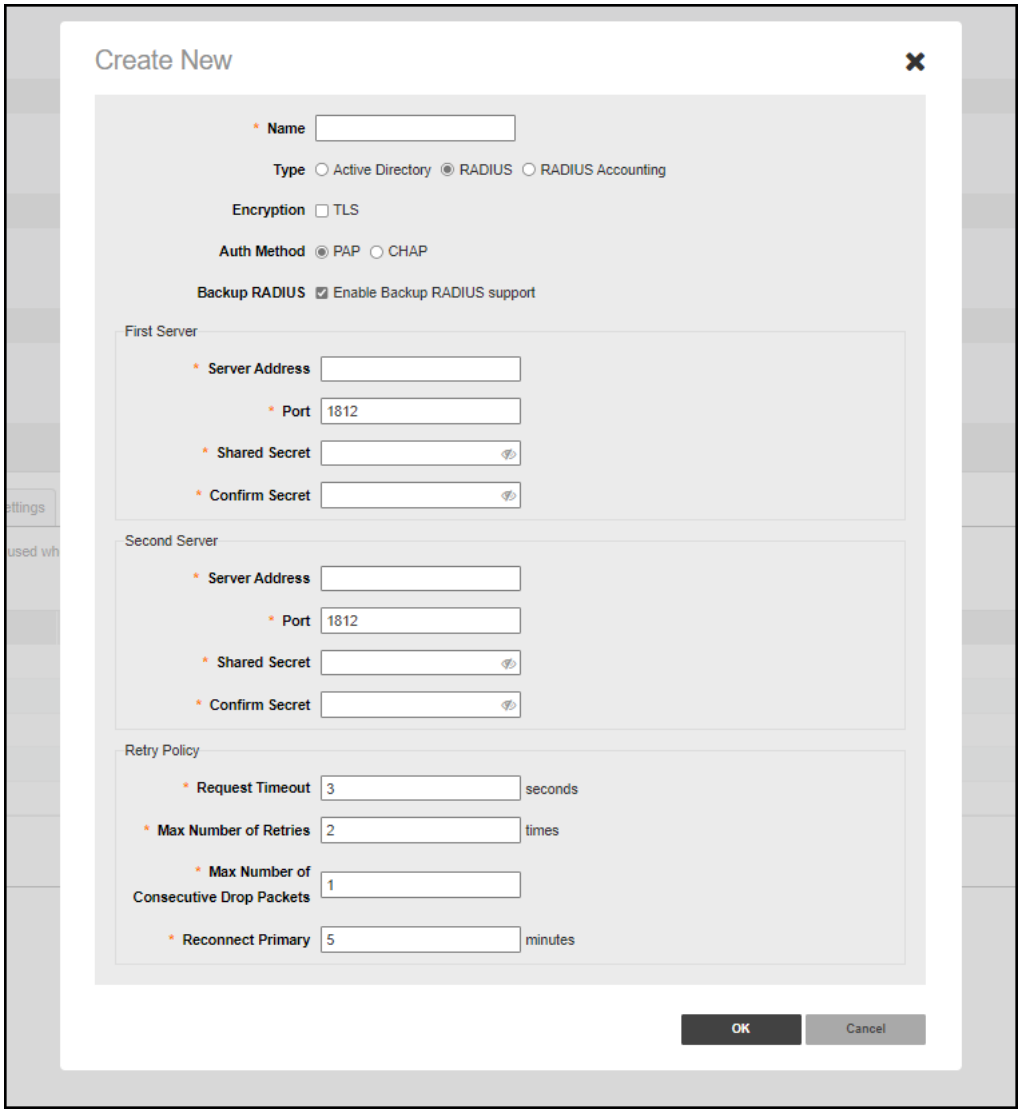


FIGURE 322 RADIUS or RADIUS Accounting Server Configuration



Limitations on configuring AAA Servers

- If a domain name can be resolved to more than one IP address, the first two IP addresses are used as the primary and secondary servers when the **Backup RADIUS** is disabled.
- If a domain name can be resolved to only one IP address, it is used as the primary server.
- If a domain name can resolve multiple IP addresses, only the first IP address is used as the server IP address when **Backup RADIUS** is enabled. Even if the first IP addresses of two domain names are the same, the first IP address is used as the server IP address.
- If the first two IP addresses change, the backend resolves the domain name every 2 hours and updates the AAA configuration.
- If the domain name resolution fails, the domain name is requested every 2 minutes until there is a successful resolution.

Testing Authentication Settings

The **Test Authentication Settings** feature allows you to query an AAA server for a known authorized user, and return Groups associated with the user that can be used for configuring Roles within Unleashed.

After you have configured one or more authentication servers in Unleashed, perform this task to ensure that Unleashed can connect to the authentication server and retrieve the groups/attributes that you have configured for each user account.

To test the connection to the authentication server:

1. Go to **Admin & Services > Services > AAA Servers > Test Authentication Servers Settings**.
2. Select the authentication server that you want to use from the **Test Against** drop-down menu.
3. In **User Name** and **Password**, enter an Active Directory or RADIUS user name and password.
4. Click **Test**.

If Unleashed was able to connect to the authentication server and retrieve the configured groups/attributes, the information appears at the bottom of the page. The following is an example of the message that will appear when Unleashed authenticates successfully with the server:

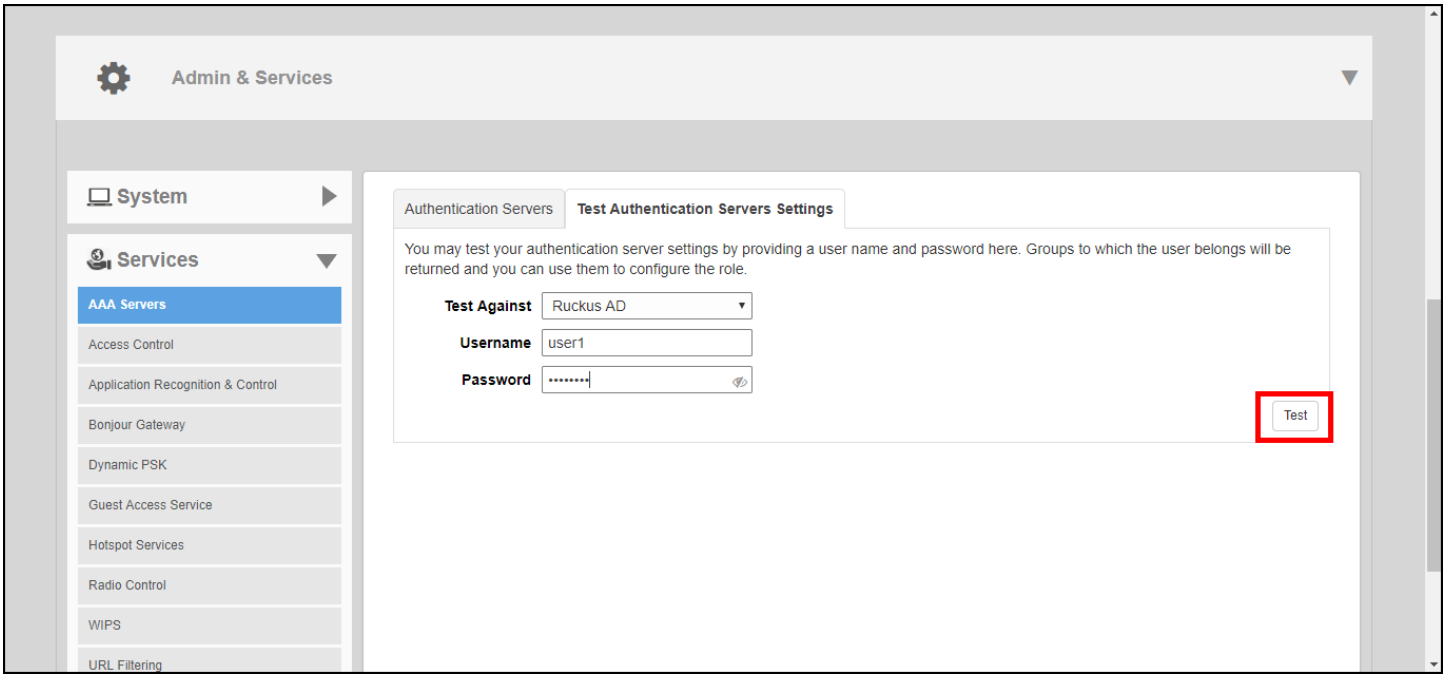
```
Success! Groups associated with this user are "{group_name}". This user will be assigned a role of {role}.
```

If the test was unsuccessful, there are several possible results (other than success) that will be displayed to inform you if you have entered information incorrectly:

- Admin invalid
- User name or password invalid

These results can be used to troubleshoot the reasons for failure to authenticate users to an AAA server.

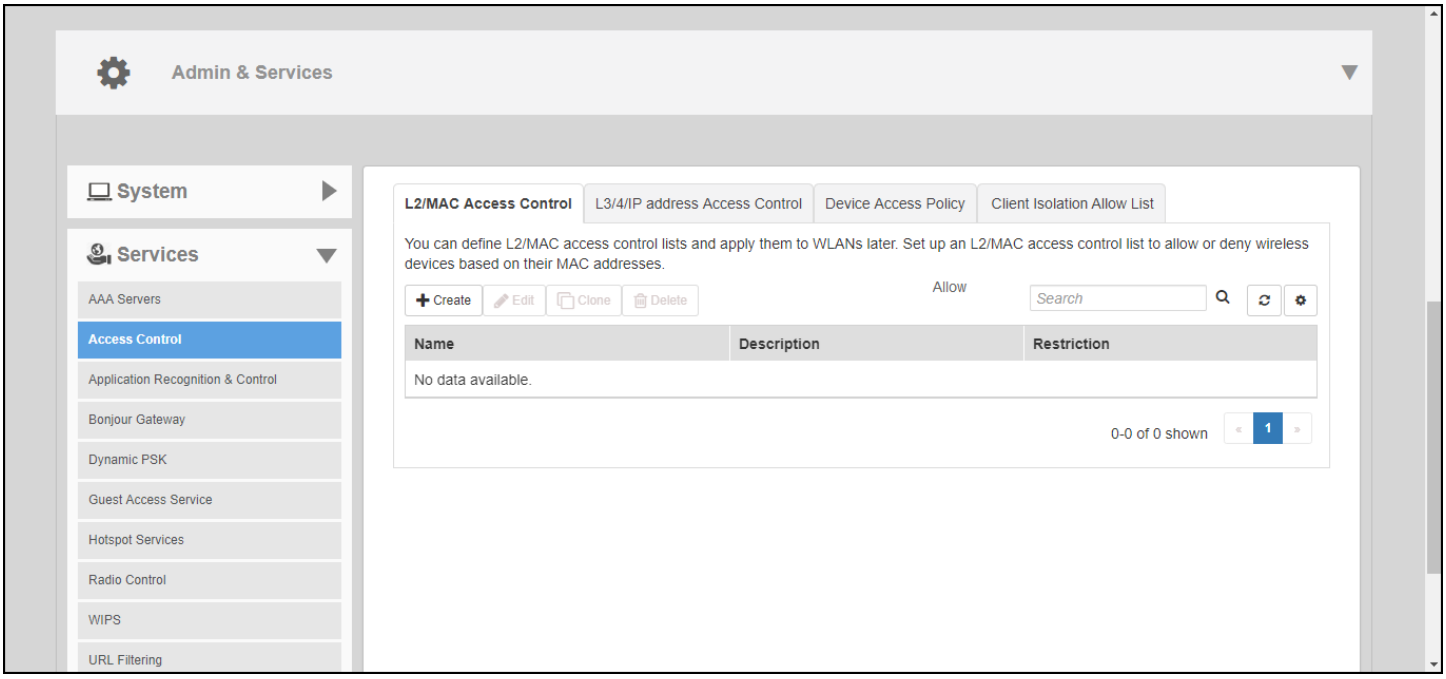
FIGURE 323 Testing authentication server settings



Access Control

RUCKUS Unleashed provides several options for controlling access to your networks, including Layer 2/MAC address level Access Control Lists (ACLs), Layer 3/Layer 4/IP Address ACLs, Device Access Policies to control clients by OS type, and Client Isolation Allowlists, which are necessary when Wireless Client Isolation is enabled on a WLAN.

FIGURE 324 Configuring Access Control



Creating a Layer 2/MAC Address Access Control List

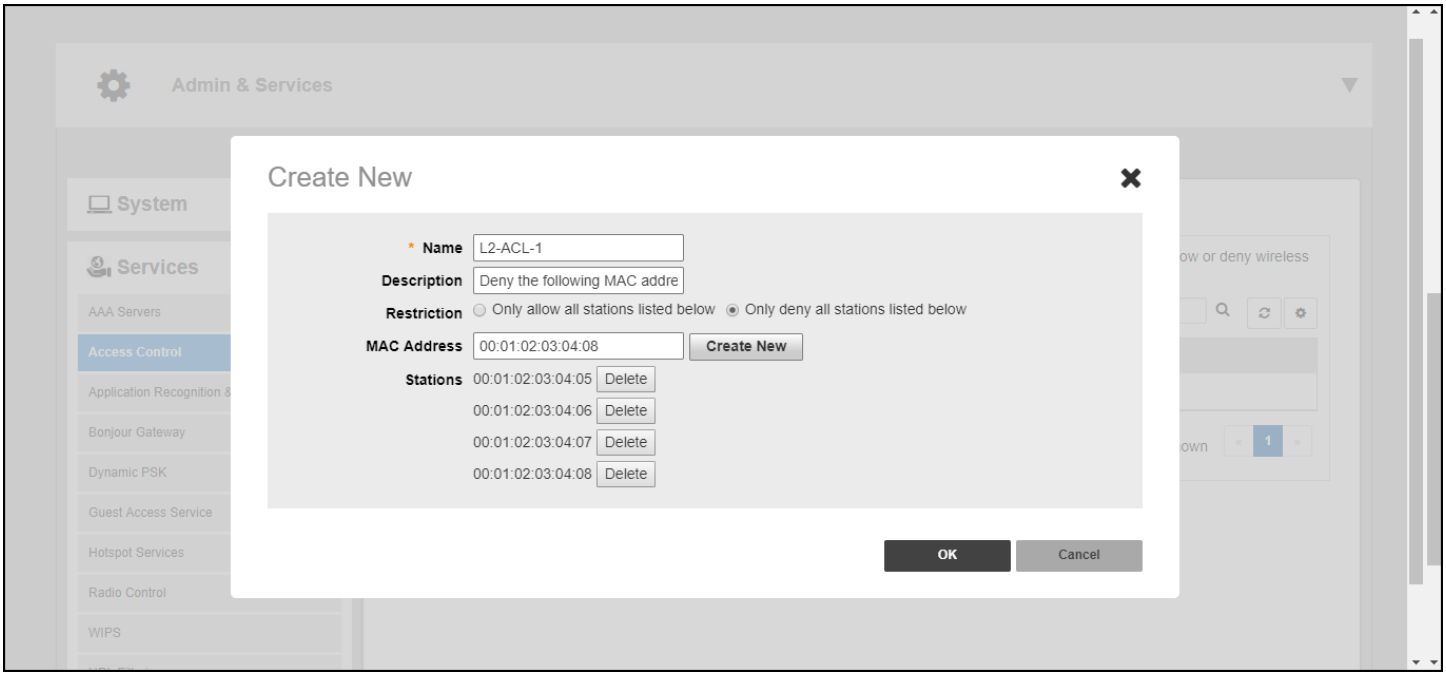
Using the Access Controls configuration options, you can define Layer 2/MAC address ACLs, which can then be applied to one or more WLANs (upon WLAN creation or edit). ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients or to deny only specified clients. MAC addresses that are in the deny list are blocked at the AP, not necessarily at the Unleashed Master AP.

To configure an L2/MAC ACL:

1. Go to **Admin & Services > Services > Access Control > L2/MAC Access Control**.
2. Click **Create New**. The ACL **Create New** form appears.
3. Type a **Name** for the ACL, and optionally, a **Description** of the ACL.
4. Select the **Restriction** mode as either allow or deny.
5. Type a MAC address in the **MAC Address** text box, and then click **Create New** to save the address. The new MAC address that you added appears next to the Stations field. You can enter up to 128 MAC addresses per ACL.
6. Click **OK** to save the L2/MAC based ACL.

You can create up to 32 L2/MAC ACL rules and each rule can contain up to 128 MAC addresses. Each WLAN can be configured with one L2 ACL.

FIGURE 325 Creating a Layer 2 ACL to deny specific MAC addresses



Creating a Layer 3/Layer 4/IP Address Access Control List

In addition to L2/MAC based ACLs, Unleashed also provides access control options at Layer 3 and Layer 4.

This means that you can configure the access control options based on a set of criteria, including:

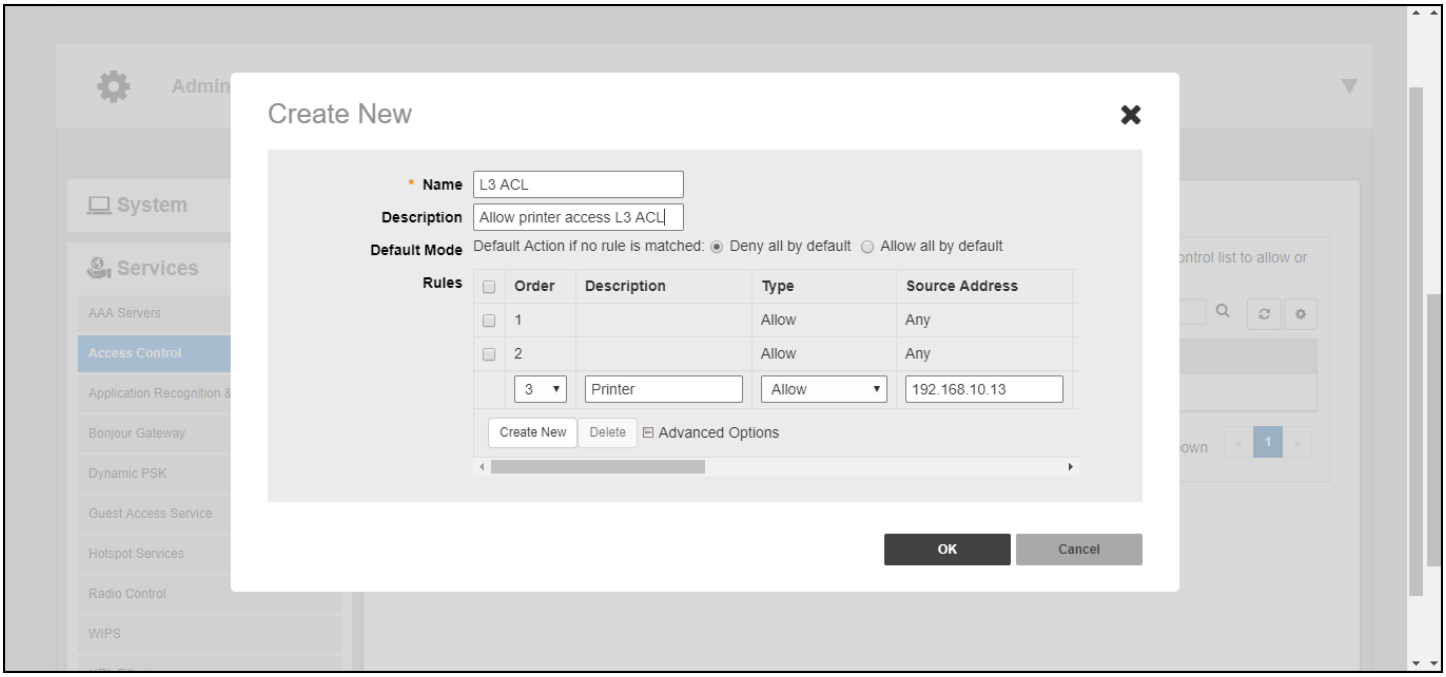
- Destination IP Address
- Application
- Protocol
- Destination Port

To create an L3/L4/IP address based ACL:

1. Go to **Admin & Services > Services > Access Control > L3/4/IP Address Access Control**.
2. Click **Create New**. The ACL **Create New** form appears.
3. Type a **Name** for the ACL, and optionally, a **Description** of the ACL.
4. In **Default Mode**, set the default access privilege (allow all or deny all) that you want to grant all users by default.
5. In **Rules**, click **Create New** or click **Edit** to edit an existing rule.

6. Define each access policy by configuring a combination of the following:
   - **Type**: The access privilege (allow or deny) that this policy grants.
   - **Destination Address**: Enter an IP subnet and netmask of the network target to which you want to allow or deny access. (IP address must be in the format A.B.C.D/M, where M is the subnet mask.) Otherwise, select Any. For example, if you enter 192.168.0.1/24, the rule would allow or deny the entire Class C subnet. To allow/deny a single host, use /32 as the netmask.
   - **Application**: If you select a specific application from the menu, the Protocol and Destination Port options are automatically filled with the relevant values and are not configurable.
   - **Protocol**: Enter a network protocol number (0-254), as defined by the IANA (http://www.iana.org/assignments/protocol-numbers/protocolnumbers.xhtml) to allow or deny. Otherwise, select Any.
   - **Destination Port**: Enter a valid port number (1-65534) or port range (e.g., 80-443).
7. Click **OK** to save the ACL.
8. Repeat these steps to create up to 32 L3/L4/IP address-based access control rules.

FIGURE 326 Configuring a Layer 3/4/IP address-based ACL



Configuring Device Access Policies

In response to the ever-growing numbers of personally owned mobile devices such as smart phones and tablets being brought into the network, IT departments are requiring more sophisticated control over how devices connect, what types of devices can connect, and what they are allowed to do once connected.

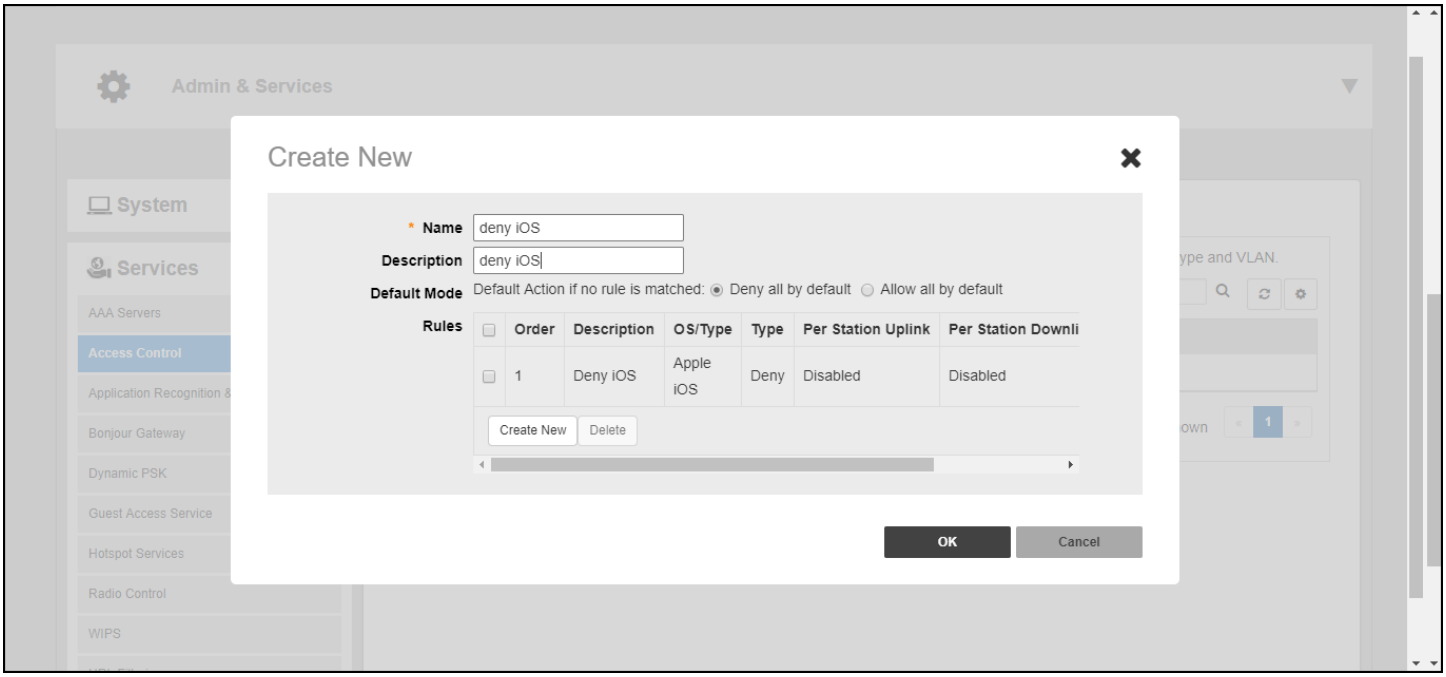
Using the **Device Access Policy** settings, the Unleashed system can identify the type of client attempting to connect, and perform control actions such as permit/deny and rate limiting based on the device type.

Once a Device Access Policy has been created, you can apply the policy to any WLANs for which you want to control access by device type. You could, for example, allow only Apple iOS devices on one WLAN and only Linux devices on another.

To create a Device Access Policy:

1. Go to **Admin & Services > Services > Access Control > Device Access Policy**.
2. Click **Create New**.
3. Enter a **Name** and optionally a **Description** for the access policy.
4. In **Default Mode**, select **Deny all by default** or **Allow all by default**.
5. In **Rules**, you can create multiple OS-specific rules for each access policy.
   - **Description**: Description of the rule.
   - **OS/Type**: Select from any of the supported client types.
   - **Type**: Select rule type (allow or deny).
   - **Uplink/Downlink**: Set rate limiting for this client type.
6. Click **Save** to save the rule you created. You can create up to nine rules per access policy (one for each OS/Type).
7. To change the order in which rules are implemented, click the up or down arrows in the **Action** column. You can also **Edit** or **Clone** rules from the **Action** column.
8. To delete a rule, select the box next to the rule and click **Delete**.
9. Click **OK** to save the access policy. You can create up to 32 access policies (one access policy per WLAN).

FIGURE 327 Creating a Device Access Policy



Configuring Client Isolation Allow Lists

When Wireless Client Isolation is enabled on a WLAN, all communication between clients and other local devices is blocked at the Access Point.

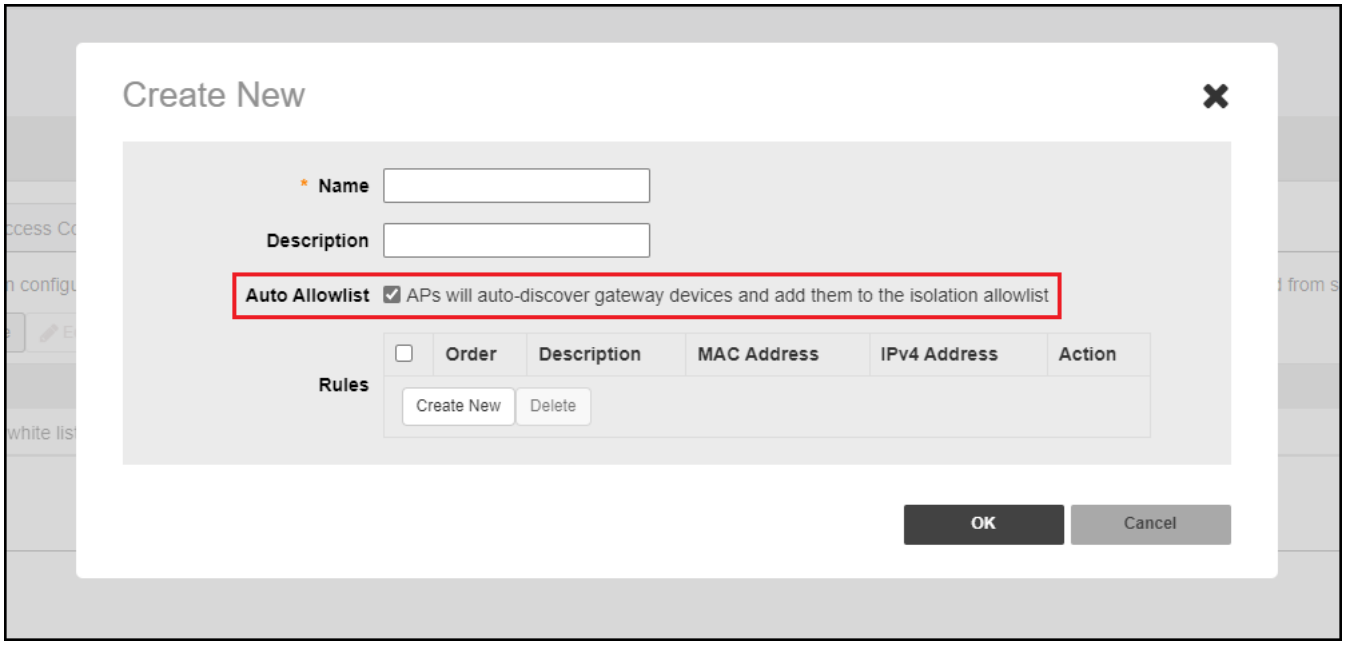
To prevent clients from communicating with other nodes, the AP drops all ARP packets from stations on the WLAN where client isolation is enabled and which are destined to IP addresses that are not part of a per-WLAN allow list.

You can create exceptions to client isolation (such as allowing access to a local printer, for example) by creating Client Isolation Allow Lists.

To create a Client Isolation Allow List:

1. Go to **Admin & Services > Services > Access Control > Client Isolation Allow List**.
2. Click **Create New**.
3. Enter a **Name** and optionally a description for the allowlist policy.
4. **Auto Allowlist** is enabled by Default, which allows the APs to auto-discover gateway devices and add them to the isolation allowlist.
5. In **Rules**, you can create multiple device-specific rules for each device to be allow listed.
   - **Description**: Description of the device.
   - **MAC Address**: Enter the MAC address of the device.
   - **IPv4 Address**: Enter the IP address of the device.
6. Click **Save** to save the rule you created.
7. To change the order in which rules are implemented, select the order from the drop-down menu in the Order column. You can also **Edit** or **Clone** rules from the **Action** column. To delete a rule, select the box next to the rule and click **Delete**.
8. Click **OK** to save the allow list.

FIGURE 328 Creating a Client Isolation Allow List



Application Recognition and Control

The Application Recognition and Control (ARC) features enable administrators to monitor which applications are generating the most wireless traffic, to apply filtering policies to prevent users from accessing certain applications or to rate limit certain applications, and to enhance the built-in application recognition capabilities with custom applications and port mappings.

Application Overview

The Application Overview page displays the top 10 applications and the top 10 clients by usage for the last 1 hour or 24 hour time period.

Use the drop-down menus at the top of the graphs to filter results by time period, AP group or SSID.

You can also choose to display applications by their application name or by port number. Hover over a section of the pie chart to display a breakdown of total, uplink and downlink values.

The Top 10 clients chart also shows the client's MAC address and percentage of total traffic for this client when you hover over the pie chart.

FIGURE 329 Application Overview page

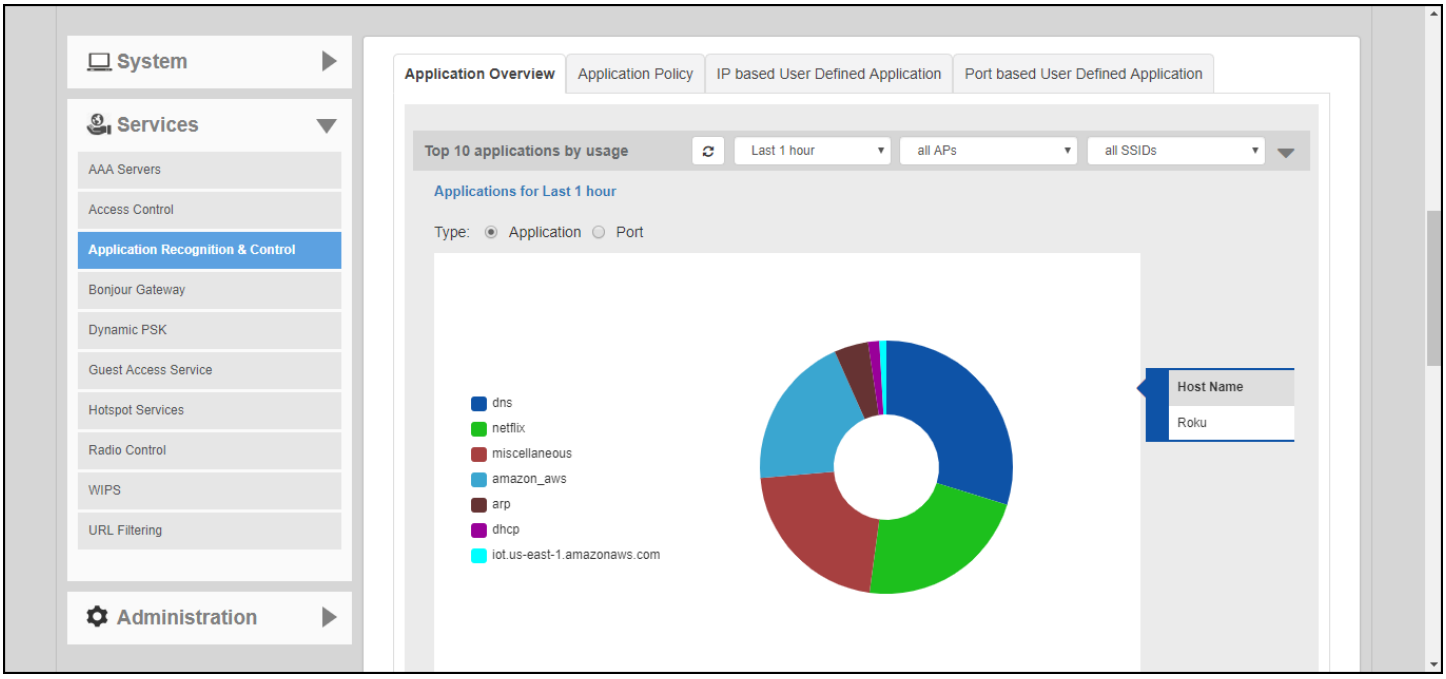


FIGURE 330 Application Performance

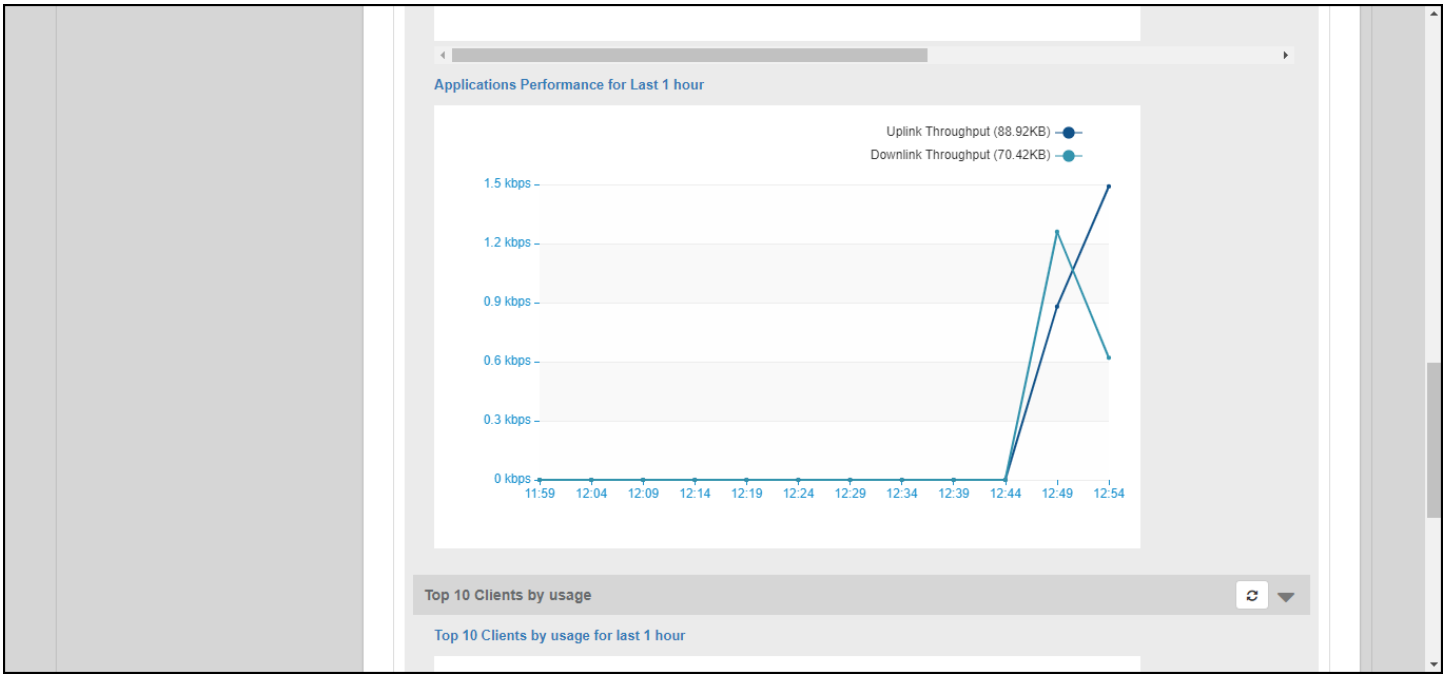
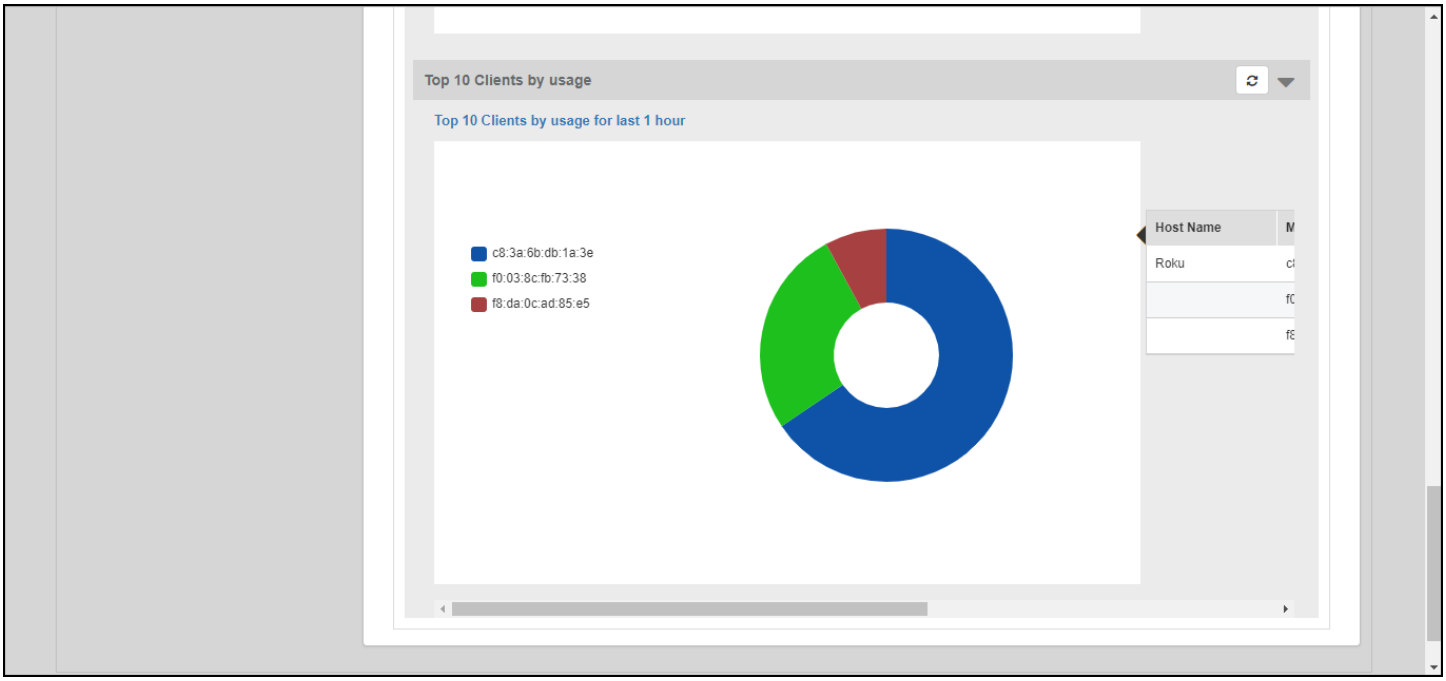


FIGURE 331 Top 10 clients by usage



Application Policy

Application Policies can be configured to control access to applications or to control traffic generated by applications.

NOTE
For more information on Application Policies, see Application Policies on page 281.

In addition to creating an Application Policy directly from the WLAN advanced options configuration screens, you can also create multiple policies from the **Admin & Services > Services > Application Recognition and Control > Application Policy** page, and then apply them to your WLANs one by one from the WLAN advanced options.

To create an Application Policy:

1. Go to **Admin & Services > Services > Application Recognition and Control**, and click the **Application Policy** tab.
2. Click **Create New** to create a new policy.
3. Enter a **Name** and optionally a **Description** for the policy.
4. In **Rules**, click **Create New** to create a new rule for this policy.
5. In **Rule Type**, select the type of application control policy to enforce:
   - **Denial Rules**: Block the application completely.
   - **QoS**: Apply QoS prioritization rules to the application.
   - **Rate Limiting**: Limit traffic volume consumed by the application.
6. In **Application Type**, Select **HTTP Domain Name** or **Port**.
   - **System Defined**: Choose from a number of built-in categories.
   - **IP Based User Defined Application**: Choose from user-defined applications.
   - **Port Based User Defined Application**: Choose from user-defined applications.

7. Select an application to control from the **Select an application** field.
8. If Rate Limiting or QoS rule type is selected, configure the uplink and downlink speeds for rate limiting or the QoS marking and priority rules for QoS rules.
9. Click **Save** to save the rule, and click **OK** to save the policy.

FIGURE 332 Application Policy

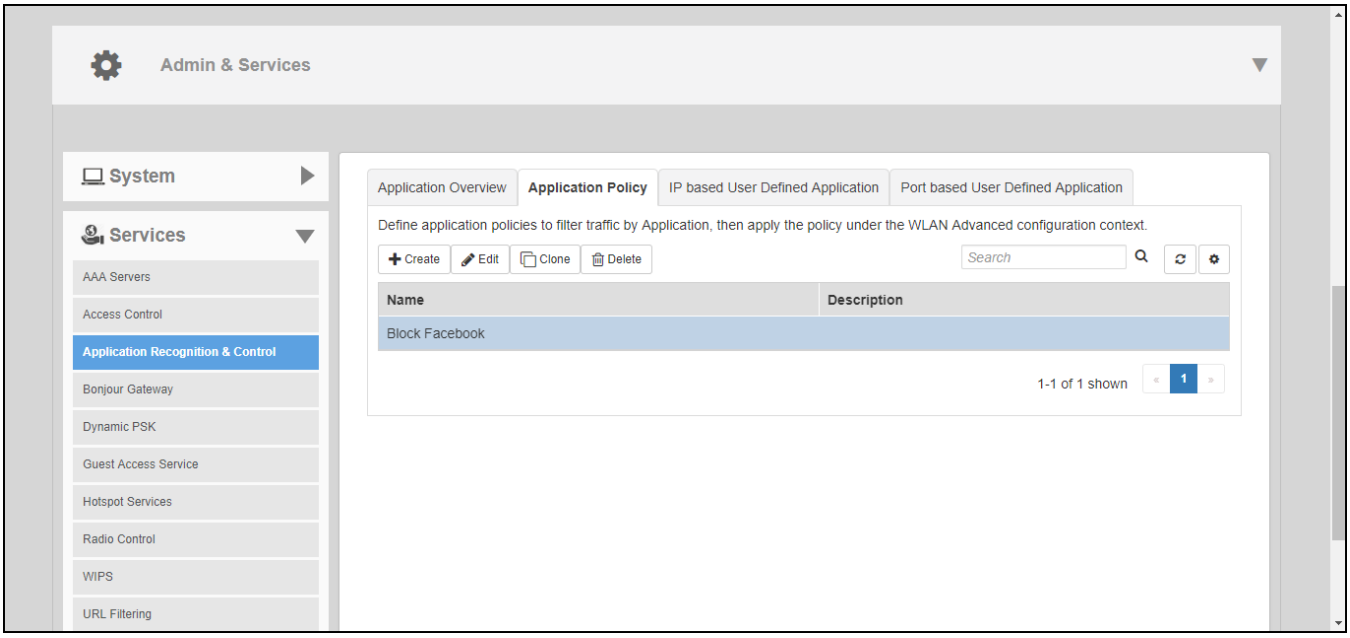
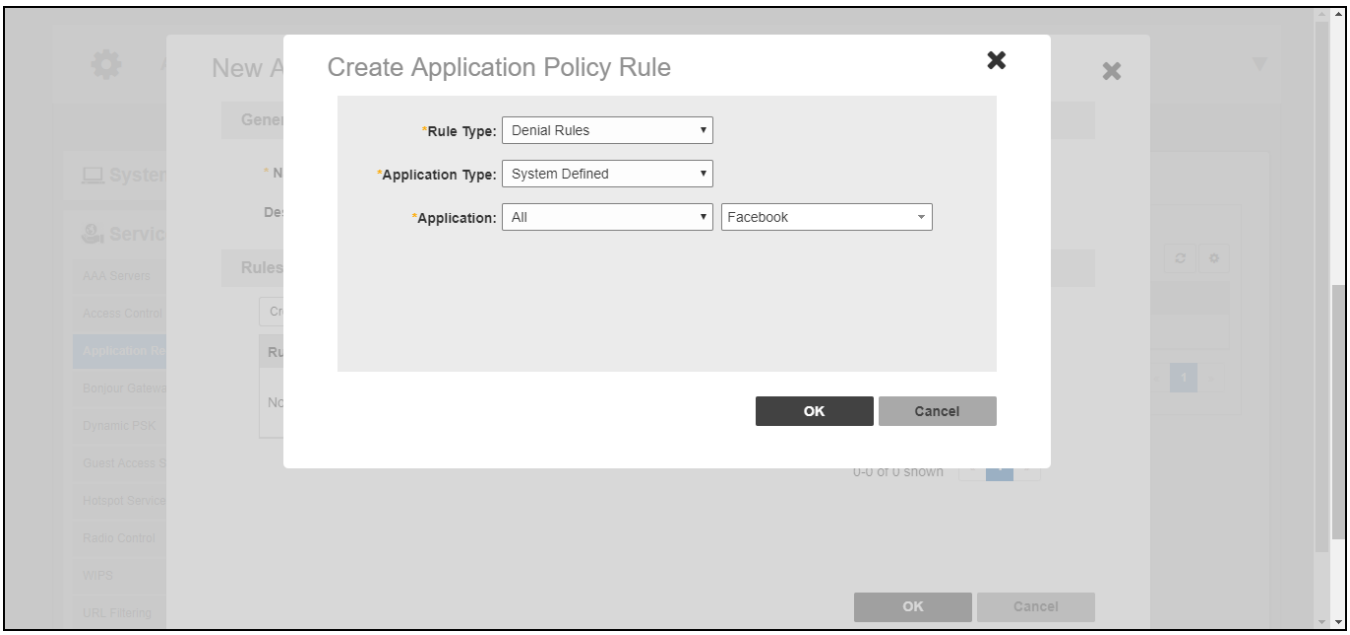


FIGURE 333 Creating a new Application Policy rule



Applying an Application Policy to a WLAN

For instructions on applying an application policy to a WLAN, see Configuring Advanced WLAN Options on page 269.

User Defined Applications

When an application is unrecognized and generically (or incorrectly) categorized, you can configure an explicit application identification policy by IP Address/Mask, Port and Protocol. Wireless traffic that matches the configured policy will be displayed using the policy's name on the **Application Overview** page.

Unleashed provides two methods to create new user-defined applications:

- IP-based User Defined Applications
- Port based User Defined Applications

Application identification policies are implemented according to the following priority order:

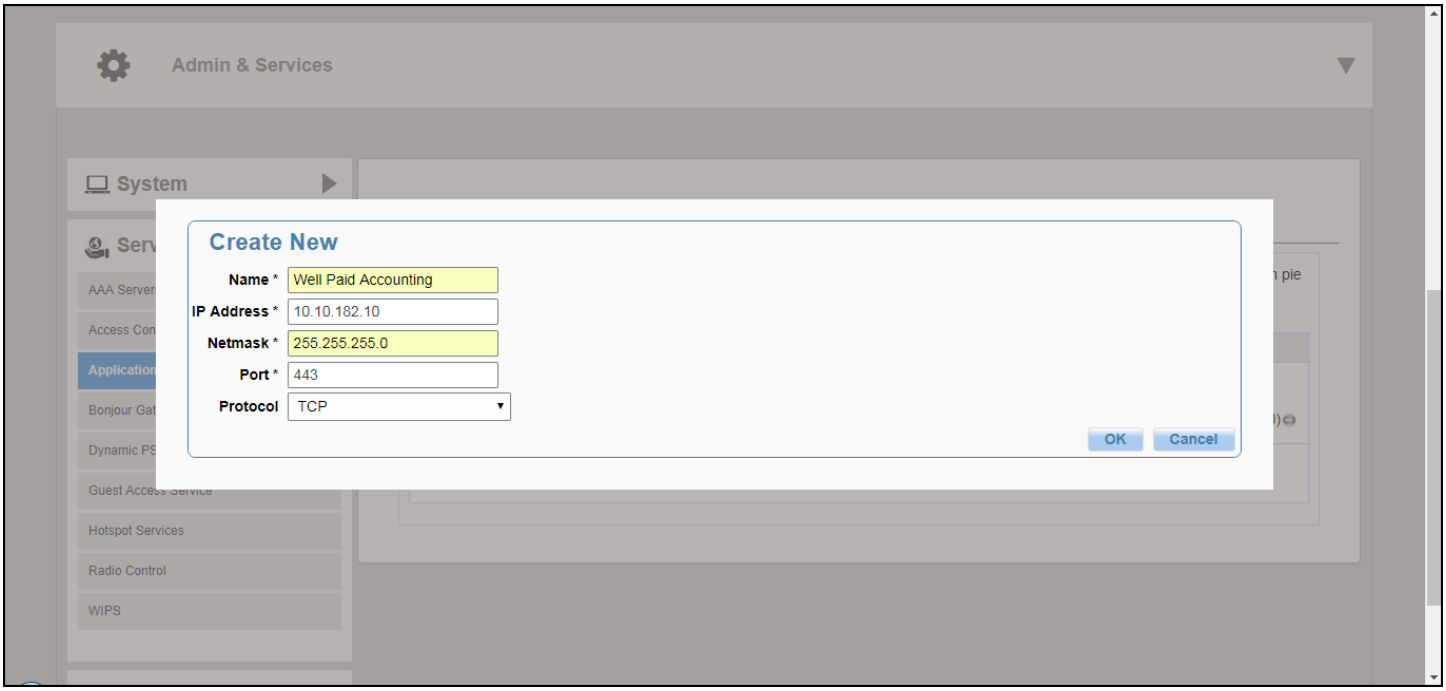
1. IP-based user defined applications
2. System defined applications
3. Port-based user defined applications

IP Based User Defined Applications

The following figure shows how to configure an IP-based user defined application policy to identify a corporate accounting application.

Unleashed identifies wireless traffic matching this policy as "Well Paid Accounting" and displays this name in the application recognition pie charts and tables.

FIGURE 334 Create new IP based User Defined Application



Port Based User Defined Applications

When an application is unrecognized and generically (or incorrectly) categorized you can configure an application identification policy by IP Port and Protocol.

Wireless traffic that matches a configured policy will be displayed using the policy's Description text in the Application Recognition pie charts. You can create new port-to-application name mappings individually using the *Port based User Defined Application* tab.

This type of application categorization is the least granular in configuration and hence it has the lowest priority as a means of application identification. If for example you configure a port-based user-defined Application for port 80/TCP, any such matching wireless traffic not identified by either an IP-based application or the default embedded applications will be identified as belonging to this application.

FIGURE 335 Application Port Mapping

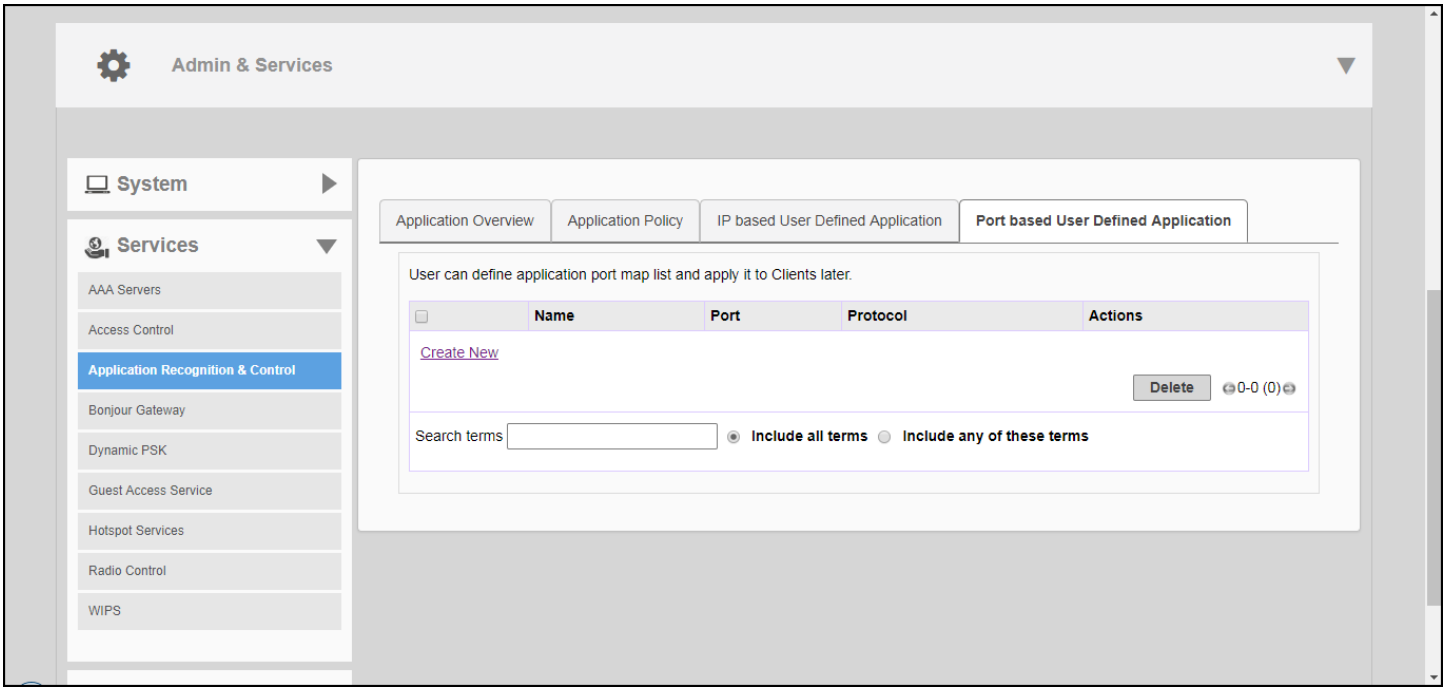
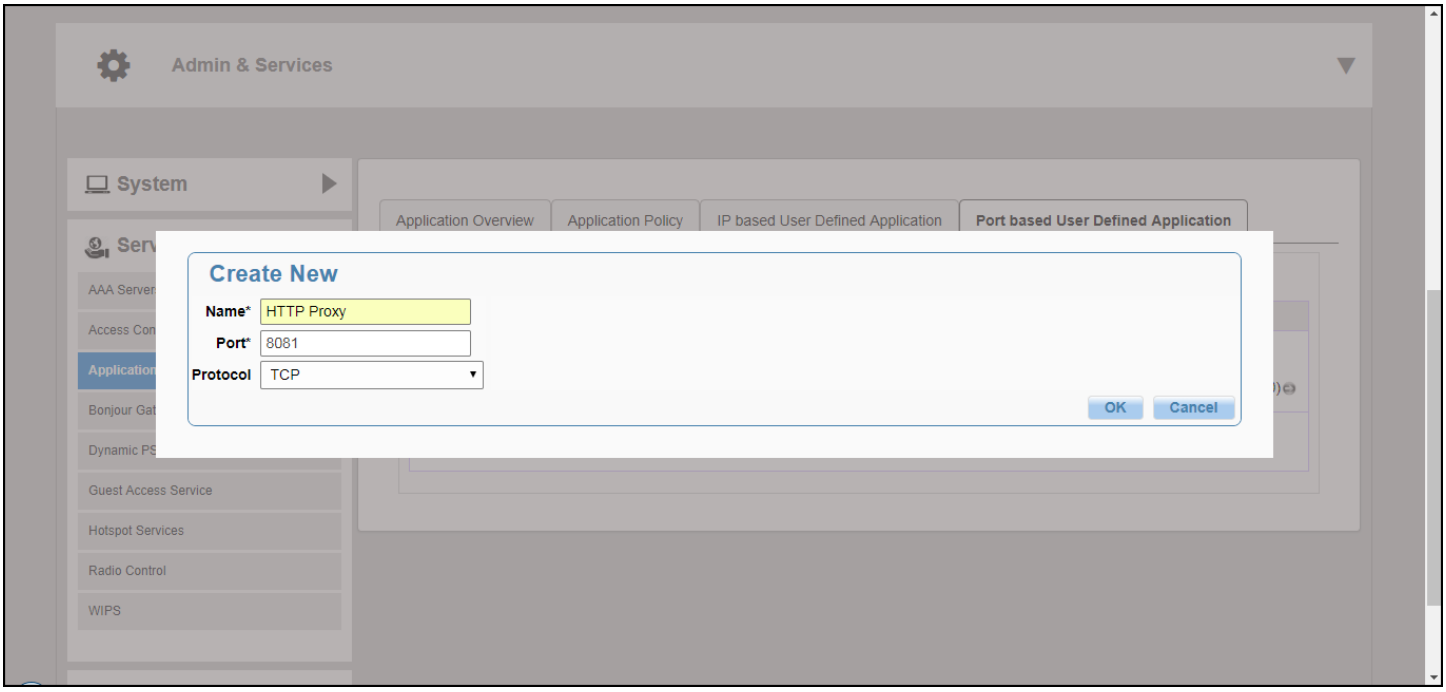


FIGURE 336 Create new port based user-defined application

The following figure shows how a port-based user-defined application policy could be used to identify all port 8081 wireless traffic as "HTTP Proxy" traffic and display this name in application recognition pie charts and tables.



Bonjour Gateway

Bonjour is a multicast-based discovery protocol (aka mDNS) that is primarily used by Apple and Google devices such as Apple TV, Apple Printers and Google Chromecast. As these devices advertise their services, client devices such as Apple Mac PCs and mobile devices such as iOS and Android phones can discover them using the Bonjour protocol.

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 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/to which VLANs.

In order for the Bonjour Gateway to function, the following network configuration requirements must be met:

- The target networks must be segmented into VLANs.
- VLANs must be mapped to different WLANs.
- The controller must be connected to a VLAN trunk port.

Additionally, if the VLANs to be bridged by the gateway are on separate subnets the network has to be configured to route traffic between them.

Creating a Bonjour Gateway Service

The Bonjour Gateway service is essentially a list of rules for mapping services from one VLAN to another. Using the Bonjour Gateway feature, the Unleashed AP serves as the proxy for forwarding Bonjour packets to the designated VLANs.

To configure rules for bridging Bonjour services across VLANs:

1. Go to **Admin & Services > Services > Bonjour Gateway**.
2. Enable the check box next to **Enable Bonjour gateway on AP**.
3. Click **Create New** to create a new Bonjour service.
4. Enter a **Name** and optionally a **Description** for the service.
5. Click **Create New** to create a new rule.
6. In the **Create New** form, configure the following options:
   - **Bridge Service**: Select the Bonjour service from the list.
     - Selecting "Other" allows you to create custom rules, for example, creating a rule for "_googlecast._tcp" would allow you to bridge Chromecast services across VLANs.
   - **From VLAN**: Select the VLAN from which the Bonjour service will be advertised.
   - **To VLAN**: Select the VLAN to which the service should be made available.
   - **Notes**: Add optional notes for this rule.
7. Click **OK** to save your changes.
8. Repeat for any additional rules.

9. Click **Apply** to save the Bonjour Service.

FIGURE 337 Bonjour Gateway configuration

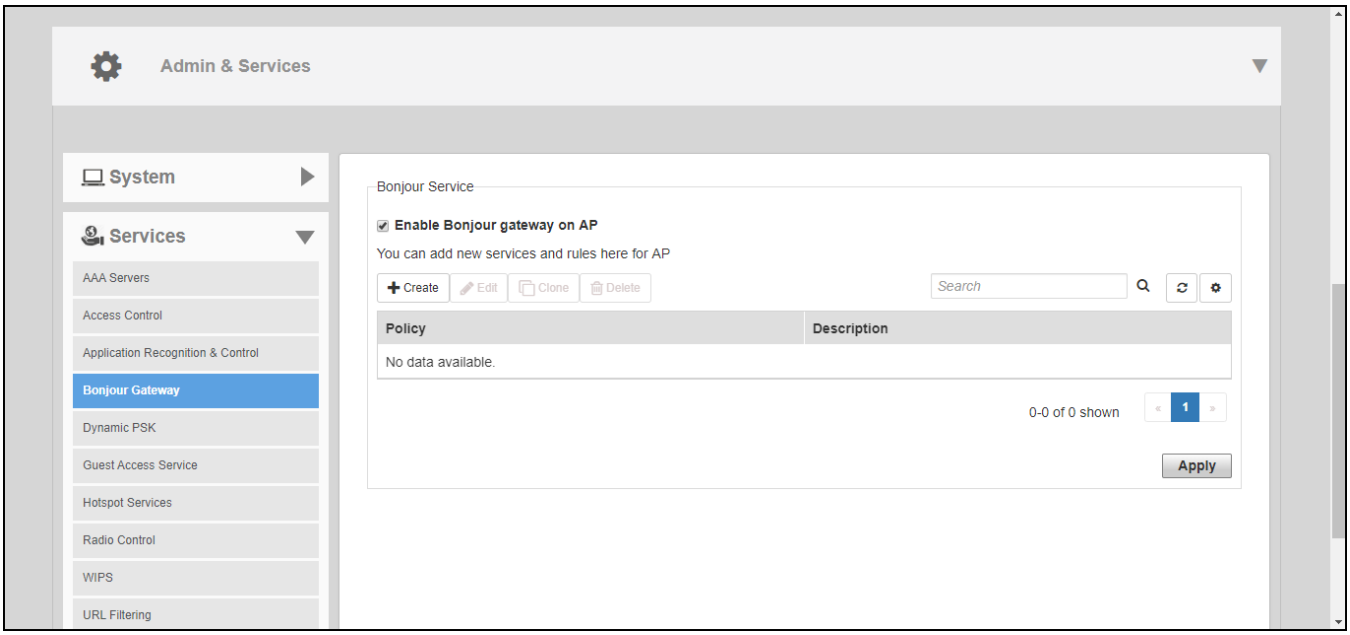
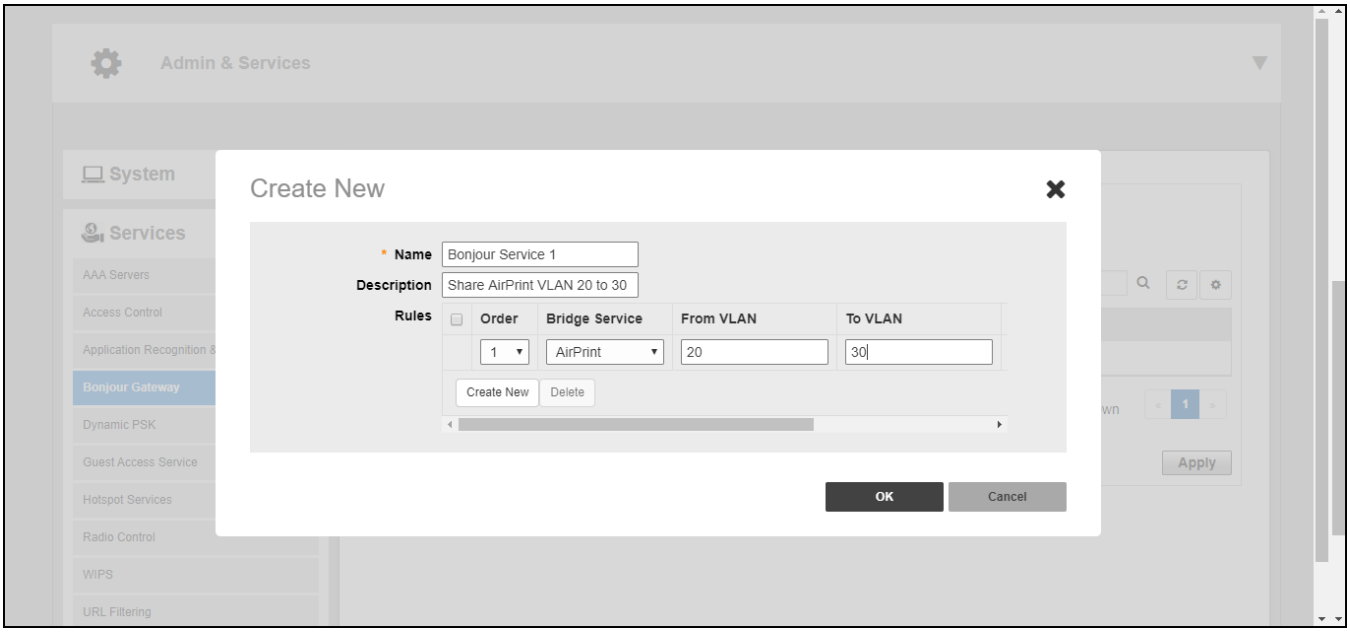


FIGURE 338 Create new Bonjour service



Deploying a Bonjour Service to an AP

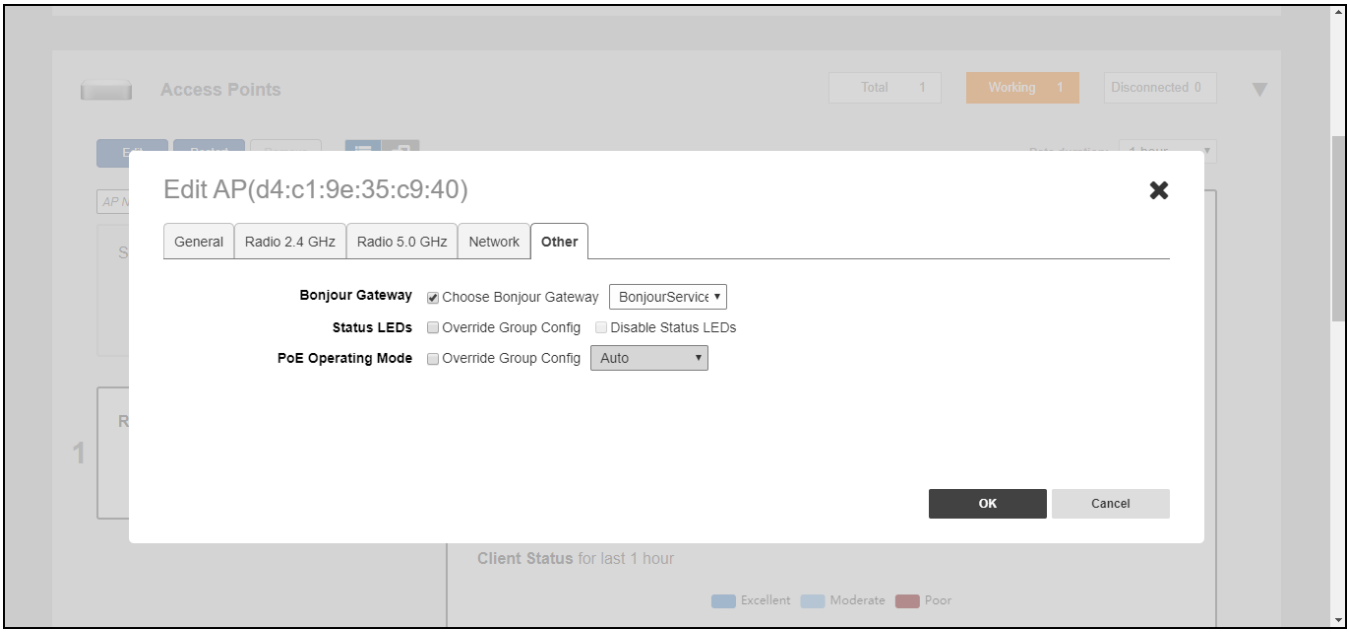
Once a Bonjour Service has been created, you can select it from any Unleashed AP's configuration page to deploy the Bonjour bridging service from that AP.

NOTE
Bonjour services can consume significant memory and CPU resources (especially when a large number of rules is created). Therefore, RUCKUS recommends deploying the Bonjour services to an AP that is *not* the Unleashed Master AP.

NOTE
It is only necessary to configure Bonjour service on one AP in the Unleashed network.

1. From the **Dashboard**, go to **Access Points > [select an AP] > Edit > Other**.
2. Enable the **Choose Bonjour Gateway** box, and select the service you created from the drop-down menu.
3. Click **OK** to save your changes.

FIGURE 339 Select Bonjour service to be deployed on an AP

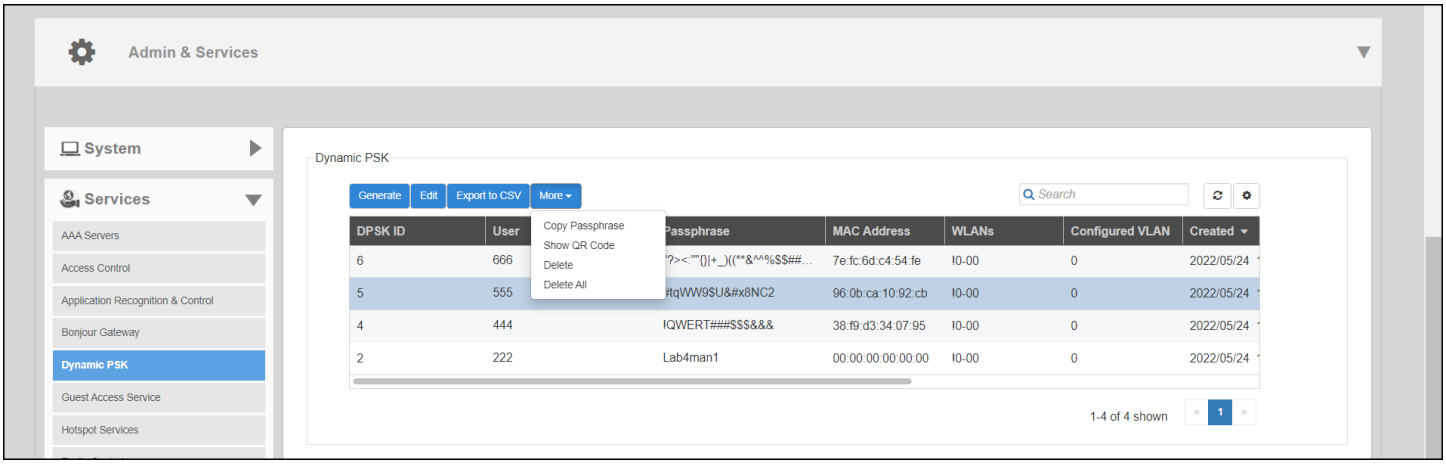


Dynamic PSK

Go to **Services** > **Dynamic PSK** to generate and manage administrator-generated DPSKs.

Only a DPSK-enabled WLAN can generate DPSKs. Refer to Enabling DPSK for a WLAN on page 273.

FIGURE 340 Dynamic PSK Page



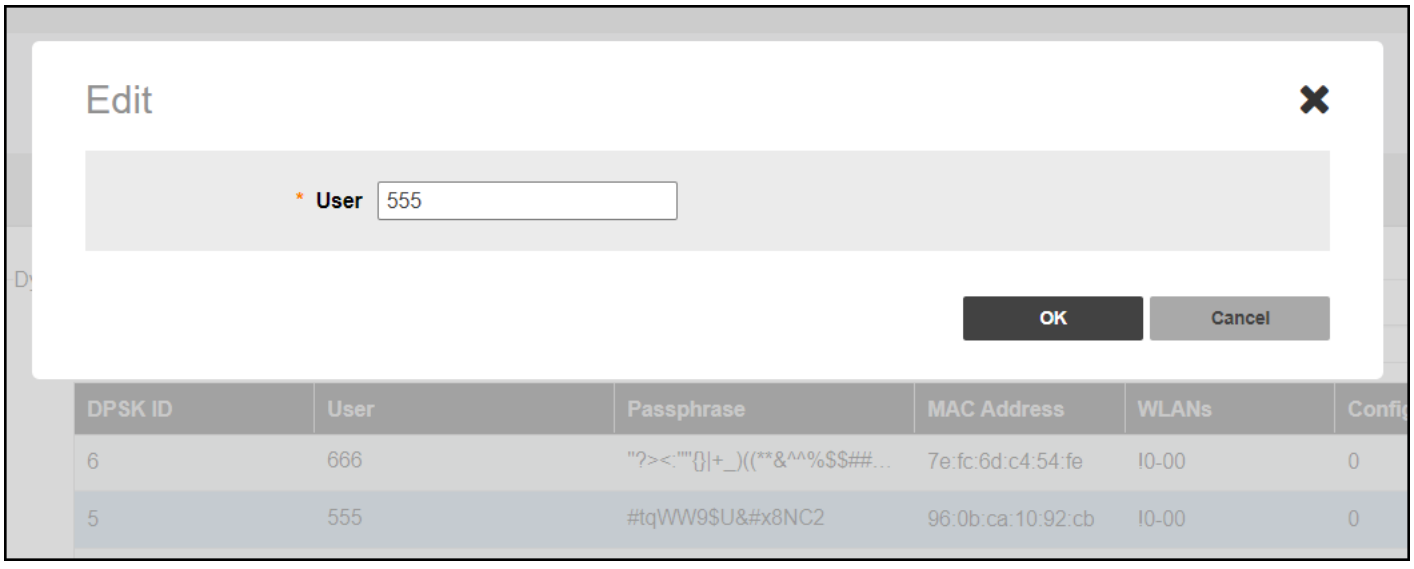
The following options are available from the **Dynamic PSK** page:

Generate: You can create DPSKs in one batch. For more information, refer to Generating DPSKs in Batch on page 431.

Edit: You can edit the DPSK user name using the **Edit** option.

1. From the DPSK table, select a DPSK entry and click **Edit**.
2. In the **Edit** dialog box, enter the new DPSK user name, and click **OK**.

FIGURE 341 Editing the DPSK User Name

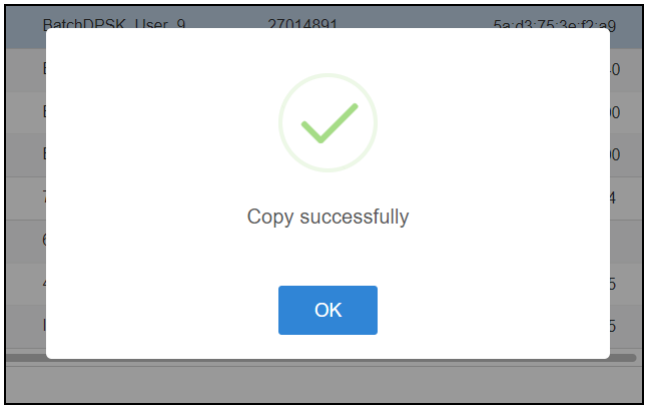


Export to CSV: Click **Export to CSV** to export all the generated DPSKs to a CSV file.

More: Click **More** to use the following options:

- **Copy Passphrase**: From the DPSK table, select a DPSK entry and click **More** > **Copy Passphrase** to copy a passphrase. When the confirmation message is displayed, click **OK**.

FIGURE 342 Successful Copying of the Passphrase



- **Show QR Code**: A WLAN-supported DPSK has the **Show QR Code** option to join a Wi-Fi network. From the DPSK table, select a DPSK entry and, click **More** > **Show QR Code** to display the **QR Code**. Click **Print** to print the QR code or scan the QR code using a smartphone camera.

FIGURE 343 QR Code Page

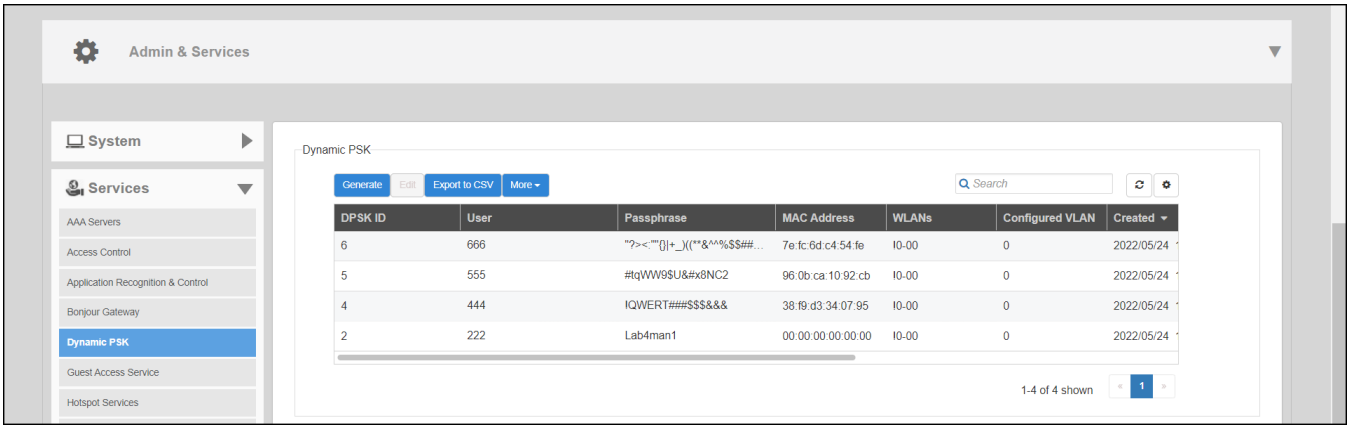
Generating DPSKs in Batch

You can create DPSKs at once (from 1 through 50) or upload a CSV file with the custom DPSKs.

Complete the following steps to generate DPSKs.

1. Go to **Admin & Services** > **Services** > **Dynamic PSK**.

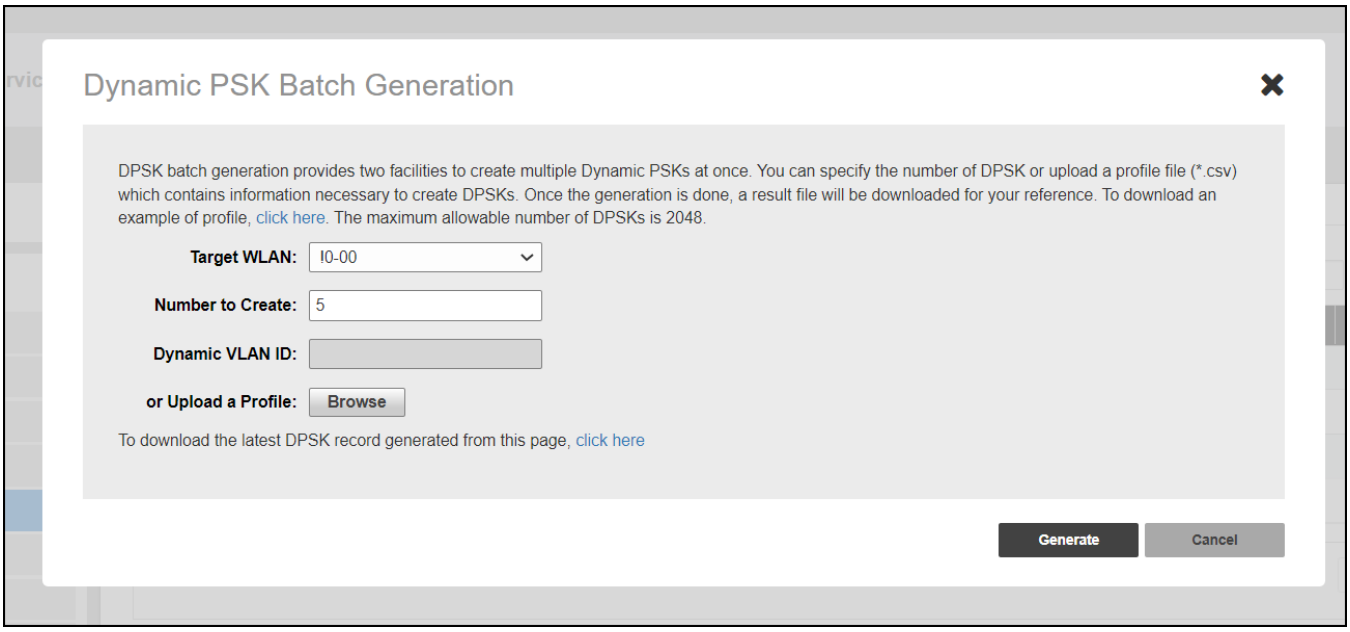
   FIGURE 344 Dynamic PSK Page



2. Click **Generate**.
3. In the **Dynamic PSK Batch Generation** dialog box, enter the following fields:
   - **Target WLAN**: Select the WLAN to which the DPSKs will be applied. (Only WLANs with the DPSK enabled are listed.)
   - **Number to Create**: Enter the number of DPSKs you want to generate (ranging from 1 through 50; the default value is 5).
   - **Dynamic VLAN ID**: Enter a valid VLAN ID, ranging from 1 through 4094 (if **Dynamic VLAN ID** is enabled for this WLAN).
   - **Upload a Profile**: Refer to Uploading a Dynamic PSK Profile on page 432.

4. Click **Generate** to generate the requested number of DPSKs.

   FIGURE 345 Generating DPSKs Automatically



   You can click the **click here** link to download the latest DPSK record that contains the generated DPSKs.

Uploading a Dynamic PSK Profile

Use the following procedure to batch generate multiple DPSKs using a CSV file that can be edited using a spreadsheet application (such as Microsoft Excel).

Creating a DPSK batch generation profile is useful if you want to customize the user names that are used for accessing the DPSK WLAN, as opposed to user names such as "BatchDPSK_User_1".

1. Go to **Admin & Services** > **Services** > **Dynamic PSK**.
2. Click **Generate**.

   Look for the following message: *To download an example of profile*, **click here**.
3. Click the **click here** link to download a sample profile.
4. Save the sample batch DPSK profile (in CSV format) to your computer.

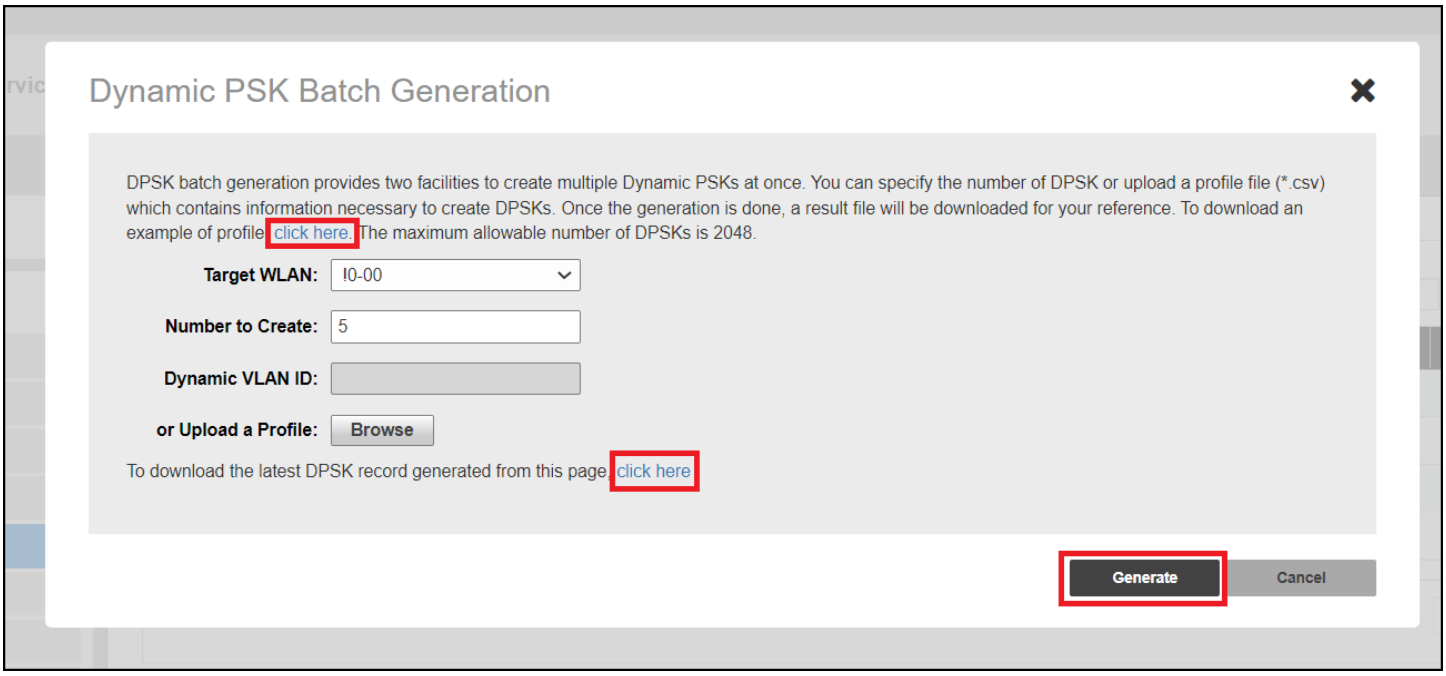
5. Using a spreadsheet application, open the CSV file and edit the batch dynamic PSK profile by filling out the following columns:
   - **User Name**: (Required) Enter the name of the user (one name per row). The length of the user name must be from 1 through 128 characters.
   - **MAC Address**: (Optional) If you know the MAC address of the device that the user will be using, enter it here.
   - **VLAN ID**: (Optional) Enter a valid VLAN ID.
   - **Passphrase**: The administrator can set the DPSK characters on their own. The DPSK length must be 8 through 62 characters. For DPSK rules, refer to DPSK Rules on page 433. If the **Passphrase** field is left empty, the system automatically generates DPSKs.

     NOTE
     The administrator is not allowed to set DPSKs using the batch method.

6. In the **Dynamic PSK Batch Generation** dialog box, click the **Browse** button to upload the CSV file you edited.
7. Click **Generate** to generate the custom DPSKs that you modified.

After the DPSKs have been generated, you can download the same file (with the passphrases filled in). Click the **click here** link to download the latest DPSK record generated.

FIGURE 346 Generating Batch Dynamic PSKs



DPSK Rules

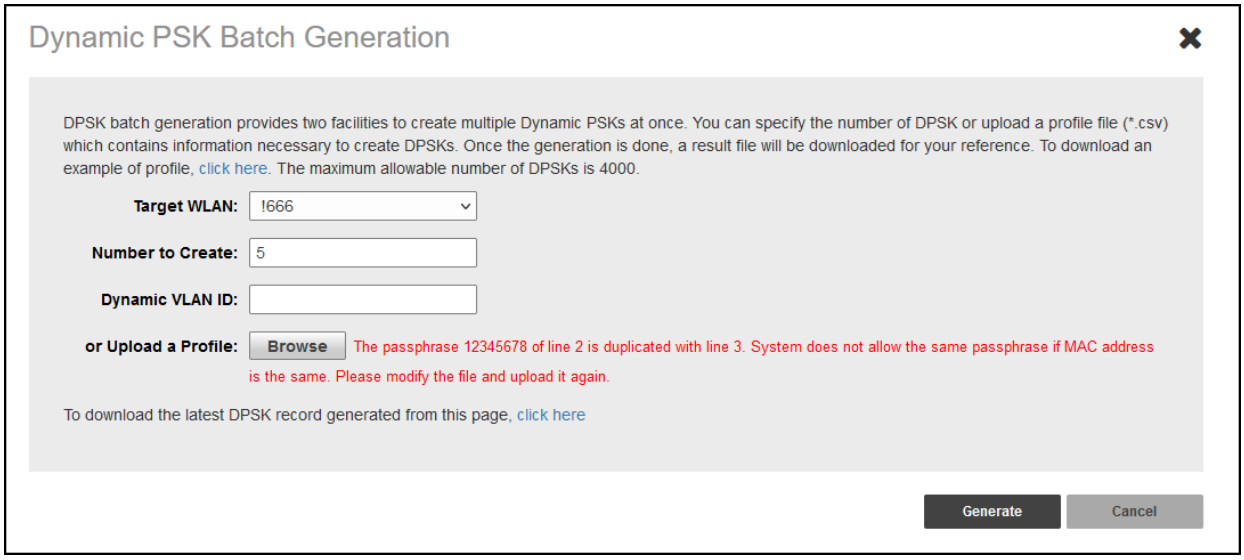
You must adhere to the following DPSK rules:

1. Multiple DPSKs are allowed in the same WLAN and unbound MAC address (when the MAC address is empty), but duplicate DPSKs are not allowed (shared DPSKs).
2. Multiple DPSKs are allowed in the same WLAN and the same bound MAC address, but duplicate DPSKs are not allowed (because the MAC address and the WLAN are used as an index in the DPSK hash table).
3. Multiple and duplicate (legacy device) DPSKs are allowed in the same WLAN and a different bound MAC address.

4. Multiple and duplicate DPSKs are allowed in a different WLAN, either for the same MAC address (bound) or an empty MAC address (unbound).

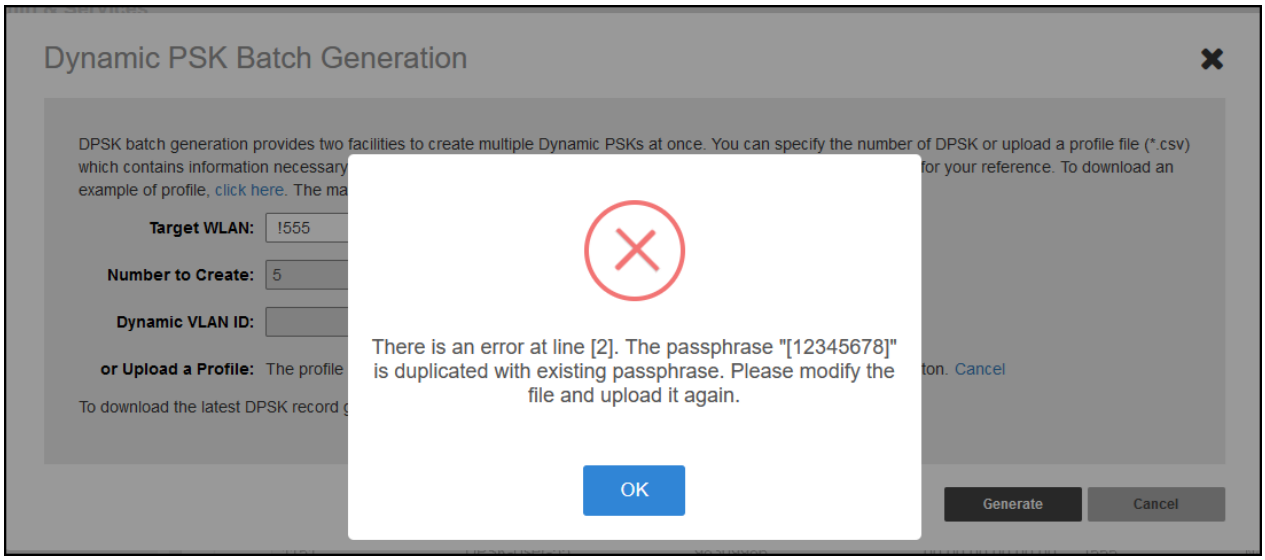
NOTE
In rules 1 and 2, if the DPSK CSV file includes the same passphrase that exists (for the same bound or unbound MAC address), Unleashed returns an error message when the administrator clicks **Upload** to import the DPSK CSV.

FIGURE 347 Duplicate Passphrase Error



NOTE
If a DPSK CSV file includes the same passphrase that is existing in the same WLAN, Unleashed returns an error message when the administrator clicks **Upload** to import the DPSK CSV file and clicks **Generate**.

FIGURE 348 Duplicate Passphrase in the Same WLAN Error



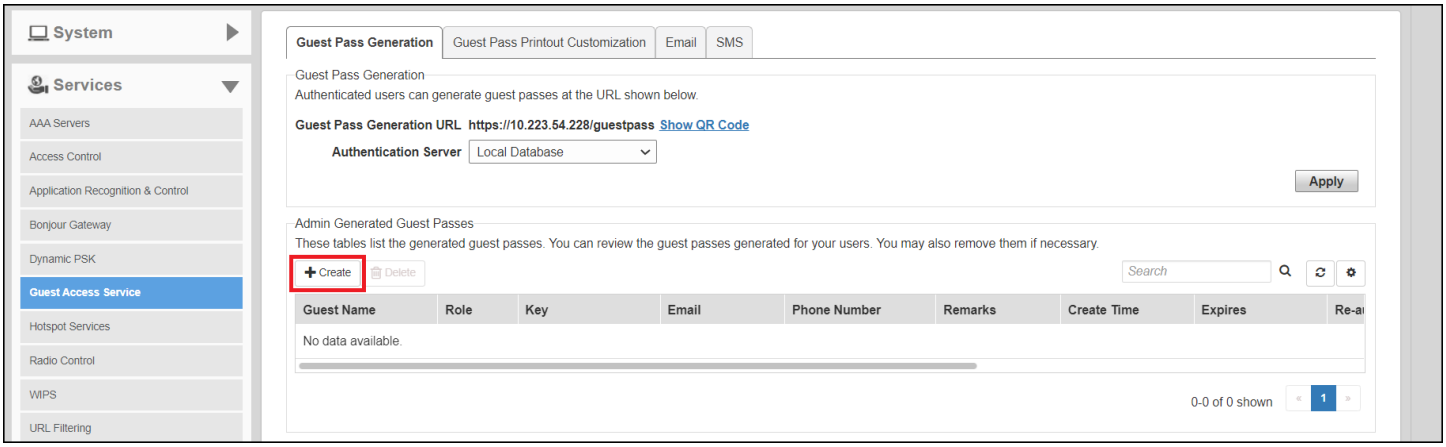
Guest Access Services

The *Guest Access Services* pages provide options for monitoring and managing existing guest passes, customizing guest pass format and delivery methods, and deleting admin-generated or self-service guest passes.

To configure guest access services, go to *Admin & Services > Services > Guest Access Service*.

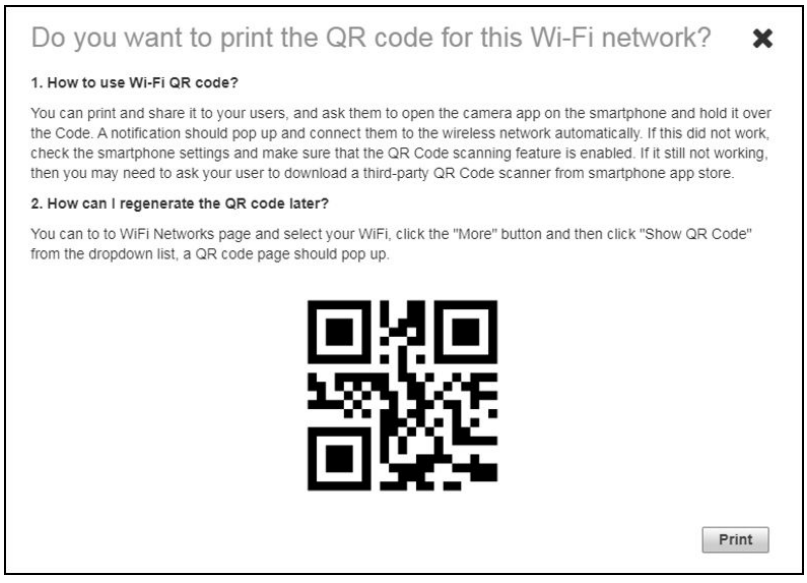
For more information on guest access and configuring a guest access WLAN, see Guest WLANs on page 198 in *Creating a New WLAN*.

FIGURE 349 Monitoring and Configuring Guest Pass Options



Click **Show QR Code** and the **QR Code** pop-up page is displayed. Click **Print** to print the QR code or scan the QR code using a smartphone camera.

FIGURE 350 QR Code Page



An administrator can generate guest passes from the web interface. Under **Admin Generated Guest Passes**, click **Create**. For more information, refer Generating a Guest Pass on page 216.

Hotspot Services

A Hotspot Service is required to deploy a Hotspot (WISPr 1.0) WLAN.

You can create a Hotspot service when creating a new WLAN (by clicking **Create New** after you select Hotspot Service as the WLAN type), or you can create multiple Hotspot services from the Administration settings and then deploy them to your Hotspot WLANs afterwards.

Additionally, you can use the **Admin & Services** pages to edit or reconfigure Hotspot service policy settings after WLAN creation.

Creating a Hotspot Service

The **Admin & Services > Services > Hotspot Services** page can be used to configure a WISPr Hotspot service to provide public access to users. In addition to the Unleashed APs, you will need the following to deploy a Hotspot:

- **Captive Portal**: A special web page, typically a login page, to which users that have associated with your Hotspot will be redirected for authentication purposes. Users will need to enter a valid user name and password before they are allowed access to the Internet through the Hotspot. Open source captive portal packages, such as Chillispot, are available on the Internet. For a list of open source and commercial captive portal software, visit https://en.wikipedia.org/wiki/Captive_portal#Software_Captive_Portals, and
- **RADIUS Server**: A Remote Authentication Dial-In User Service (RADIUS) server through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them. After completing the steps below, you will need to edit the WLAN(s) for which you want to enable Hotspot service, as described in *Assigning a WLAN to Provide Hotspot Service*.

Unleashed supports up to 32 WISPr Hotspot service entries, each of which can be assigned to multiple WLANs.

To create a Hotspot service:

1. Go to **Admin & Services > Services > Hotspot Service**. Alternatively, you can create a new Hotspot service from the WLAN creation page (**Dashboard > Wi-Fi Networks > Create > Hotspot > Hotspot Services > Create New**).
2. Click **Create New**. The **Create New** form appears.
3. From the **General** tab, in **Name**, enter a name for this Hotspot service.
4. In **WISPr Smart Client Support**, select whether to allow WISPr Smart Client support:
   - **None**: (default).
   - **Enabled**: Enable Smart Client support.

     NOTE
     The WISPr Smart Client is not provided by RUCKUS - you will need to provide Smart Client software/hardware to your users if you select this option.

     - **Only WISPr Smart Client allowed**: Choose this option to allow only clients that support WISPr Smart Client login to access this Hotspot. If this option is selected, a field appears in which you can enter instructions for clients attempting to log in using the Smart Client application.
     - **Smart Client HTTP Secure**: If Smart Client is enabled, choose whether to authenticate users over HTTP or HTTPS.
5. In **Login Page**, type the URL of the captive portal (the page where Hotspot users can log in to access the service).

6. Configure optional settings as preferred:
   - In **Start Page**, configure where users will be redirected after successful login. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected (for example, your company website).
   - In **User Session**, configure session timeout and grace period, both disabled by default.
     - **Session Timeout**: Specify a time limit after which users will be disconnected and required to log in again.
     - **Grace Period**: Allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. Enter a number in minutes, between 1 and 144,000.
7. In the **Authentication** tab, select the AAA server that you want to use to authenticate users from the **Authentication Server** drop-down menu.
   - Options include **Local Database** and any AAA servers that you configured on the **Configure > AAA Servers** page.
   - **Enable MAC authentication bypass (no redirection)**: Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. The MAC address format can be configured in one of the formats listed in MAC Authentication with an External RADIUS Server.
   - **Accounting Server**: (If you have an accounting server set up), select the server from the list and configure the frequency (in minutes) at which accounting data will be retrieved.
   - In **Wireless Client Isolation**: Choose whether clients connected to this Hotspot WLAN should be allowed to communicate with one another locally. See Configuring Advanced WLAN Options on page 269 for a description of the same feature for non-Hotspot WLANs.
   - **Location Information**: Enter *Location ID* and *Location Name* for this location if using RUCKUS Smart Positioning location services.
8. On the **Walled Garden** and **Policy** tabs, configure optional settings as preferred:
   - In **Location Information**, enter Location ID and Location Name WISPr attributes, as specified by the Wi-Fi Alliance.
   - In **Walled Garden**, enter network destinations (URL or IP address) 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.
9. On the **Policy** tab, define L3/4 IP address access control rules for the Hotspot service to allow or deny wireless devices based on their IP address, port or protocol.
10. Click **OK** to save the Hotspot settings.

The page refreshes and the Hotspot service you created appears in the list. You may now assign this Hotspot service to the WLANs that you want to provide Hotspot Internet access, as described in Assigning a WLAN to Provide Hotspot Service on page 439.

FIGURE 351 The Hotspot Services page

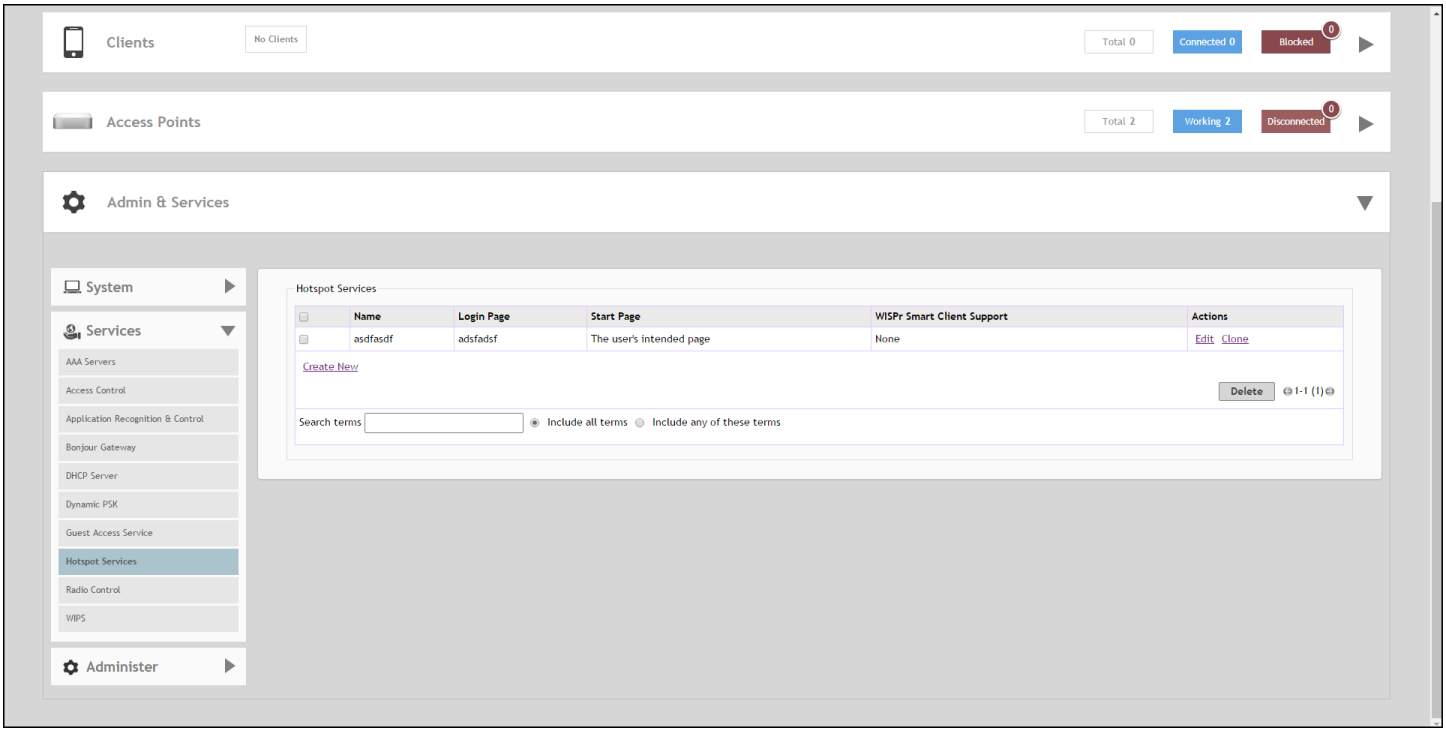
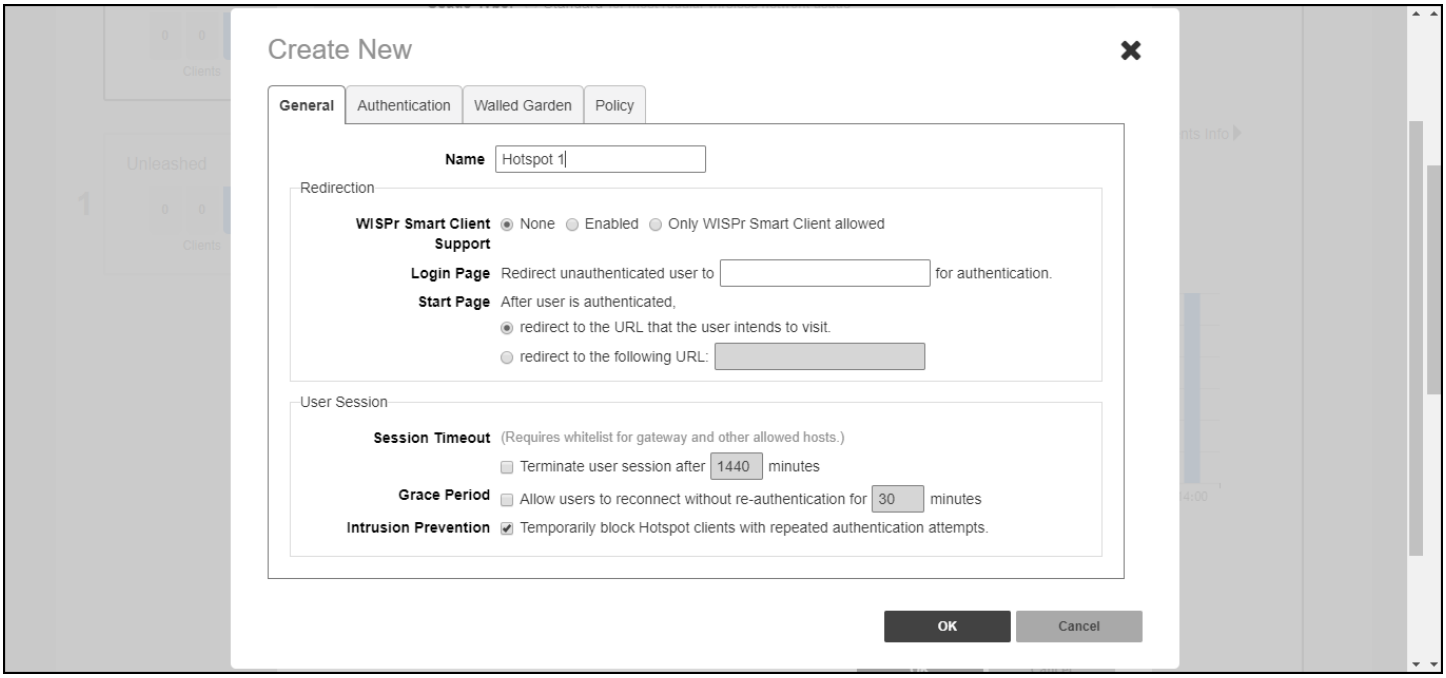


FIGURE 352 Creating a new Hotspot service



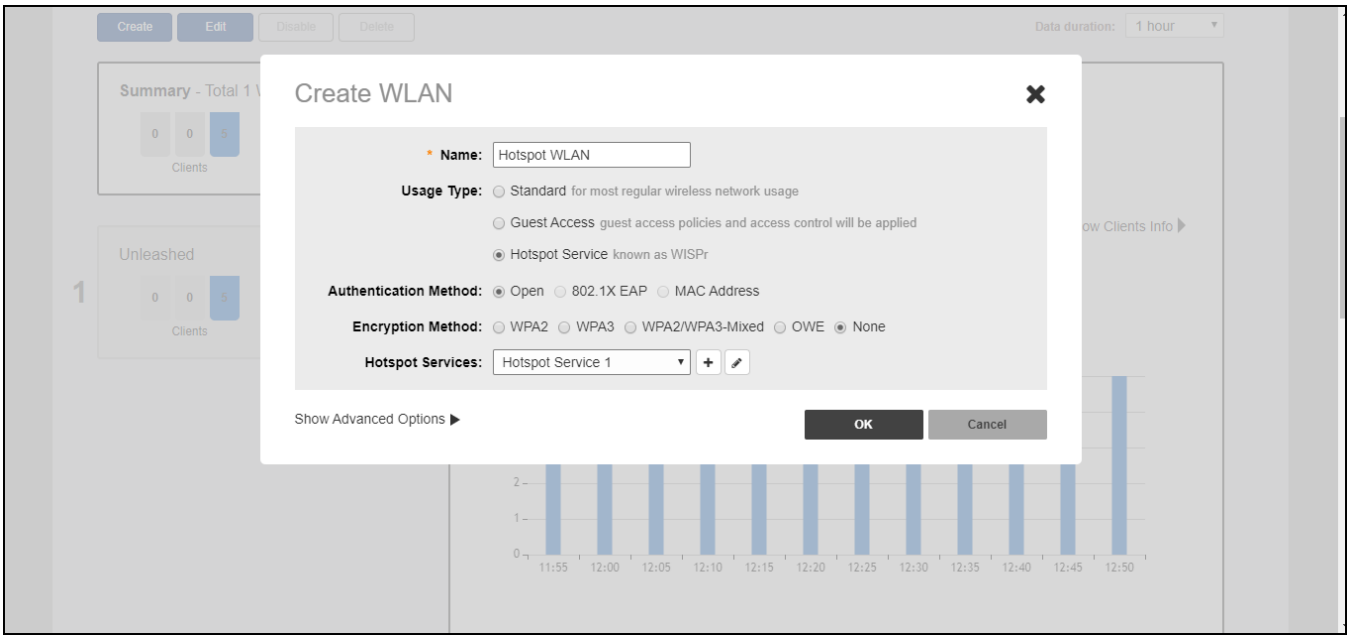
Assigning a WLAN to Provide Hotspot Service

Once you have created a Hotspot service, you need to specify the WLANs to which you want to deploy the Hotspot configuration.

To configure a WLAN to provide Hotspot service:

1. Go to **Dashboard > Wi-Fi Networks > [WLAN name] > Edit**.
2. In **Usage Type**, select **Hotspot Service**.
3. In **Hotspot Services**, select a Hotspot service from the list if you have already created one, or click **Create New** to begin creating a new Hotspot service for this WLAN. (See Creating a Hotspot Service on page 436).
4. In **Encryption Method**, choose one of the following:
   - **None**: (Default) Hotspot login is required.
   - **WPA2**: Requires the user to enter a WPA2 password to associate with the WLAN, in addition to the Hotspot login.
   - **WPA3**: Requires the user to enter a WPA3 password to associate with the WLAN, in addition to the Hotspot login.
   - **WPA2/WPA3-Mixed**: Requires the user to enter a WPA2 or WPA3 password to associate with the WLAN, in addition to the Hotspot login.
   - **OWE**: Does not require the user to enter an additional password (other than the Hotspot login).
5. Click **OK** to save your changes.

FIGURE 353 Assigning a Hotspot service to a Hotspot WLAN



Radio Control

The Radio Control options include settings for automatic radio channel selection using Background Scanning or ChannelFly, client Load Balancing, Band Balancing and Radar Avoidance Pre-Scanning.

Self Healing

RUCKUS Unleashed uses built-in network "self healing" diagnostics and tuning tools to maximize wireless network performance.

Automatically Adjust AP Radio Power

RUCKUS Unleashed provides a feature to automatically adjust AP radio power to optimize coverage when interference is present. This feature is designed to turn down the power of an access point if the following conditions are met:

- The power is set to Auto in the AP configuration.
- The AP can hear another AP that is on the same channel and same network.
- The AP can hear the other AP at a minimum of 50dB which means the Access Points are very close to each other.

Note that the 2.4G and 5G radio bands are considered independently. If all conditions are met, the AP will reduce its power by half. The other AP may or may not necessarily reduce its power simultaneously.

> **NOTE**
> In general, RUCKUS does NOT recommend enabling this feature as it can lead to non-optimal AP power levels. With BeamFlex access points, RUCKUS general guidelines are to run access points at full power to maximize the throughput and SINR levels, thus maximizing data rates and performance.

Automatically Adjust 2.4GHz/5GHz Radio Channels Using Background Scanning

Using Background Scanning, the Master AP regularly samples the activity in all Access Points to assess RF usage, to detect rogue APs and to determine the optimal channel for automatic channel selection.

These scans sample one channel at a time in each AP so as not to interfere with network use. You can, if you prefer, customize the automatic scanning of RF activity, deactivate it if you feel it's not helpful, or adjust the frequency, if you want scans at greater or fewer intervals (see Background Scanning on page 441).

> **NOTE**
> Background Scanning must be enabled to detect rogue APs on the network.

Automatically Adjust 2.4GHz/5GHz Radio Channels Using ChannelFly

The main difference between ChannelFly and Background Scanning is that ChannelFly determines the optimal channel based on real-time statistical analysis of actual throughput measurements, while Background Scanning uses channel measurement and other techniques to estimate the impact of interference on Wi-Fi capacity based on progressive scans of all available channels.

> **NOTE**
> If you enable ChannelFly, Background Scanning can still be used for adjusting radio power and rogue detection while ChannelFly manages the channel assignment. Both cannot be used at the same time for channel management.

Benefits of ChannelFly

With ChannelFly, the AP intelligently samples different channels while using them for service. ChannelFly assesses channel capacity every 15 seconds and changes channel when, based on historical data, a different channel is likely to offer higher capacity than the current channel. Each AP makes channel decisions based on this historical data and maintains an internal log of channel performance individually.

When ChannelFly changes channels, it utilizes 802.11h channel change announcements to seamlessly change channels with no packet loss and minimal impact to performance. The 802.11h channel change announcements affect both wireless clients and RUCKUS mesh nodes in the 2.4 GHz and/or 5 GHz bands.

Initially (in the first 30-60 minutes) there will be more frequent channel changes as ChannelFly learns the environment. However, once an AP has learned about the environment and which channels are most likely to offer the best throughput potential, channel changes will occur less frequently unless a large measured drop in throughput occurs.

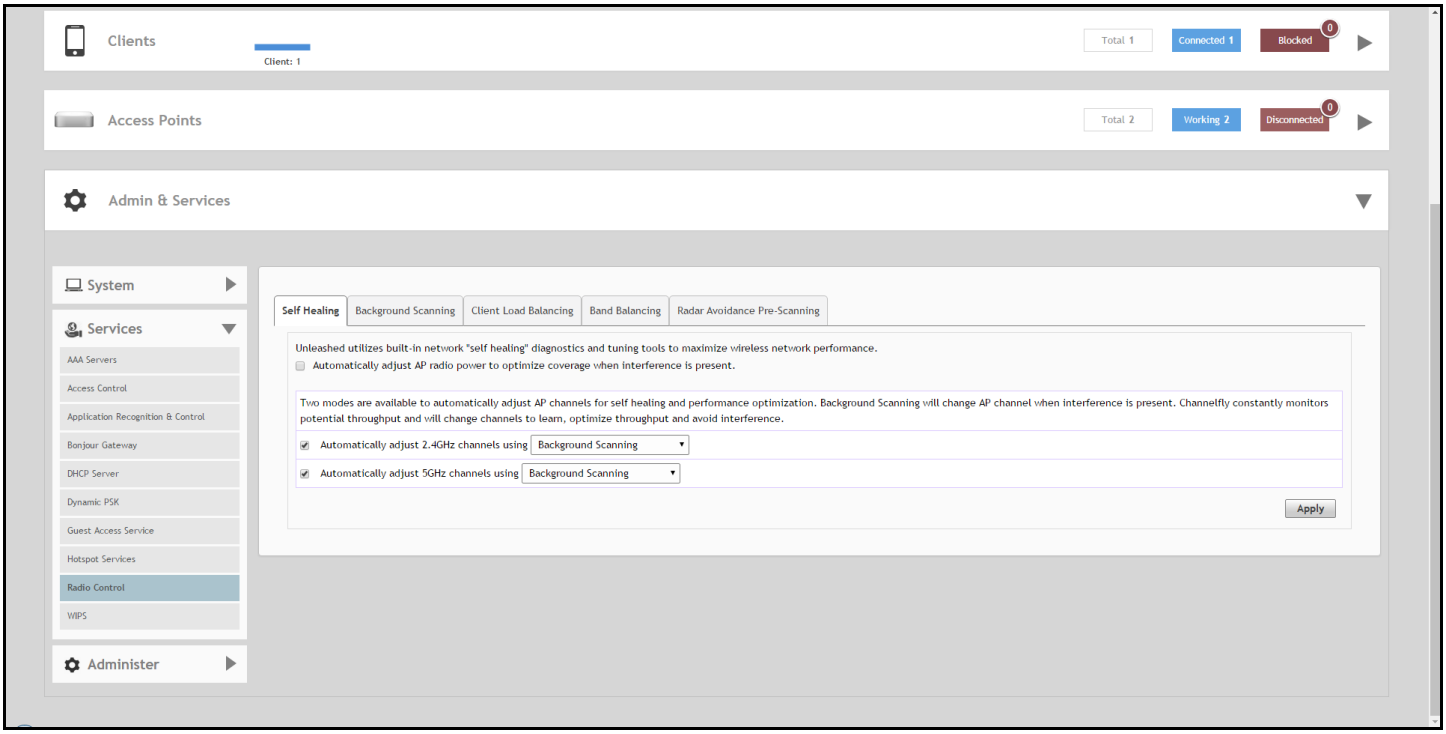
ChannelFly can react to large measured drops in throughput capacity in as little as 15 seconds, while smaller drops in capacity may take longer to react to.

Disadvantages of ChannelFly

Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you will be adding and removing APs to your network frequently, Background Scanning may be preferable. Additionally, if you have clients that do not support the 802.11h standard, ChannelFly may cause significant connectivity issues during the initial capacity assessment stage.

You can enable/disable ChannelFly per band. If you have 2.4 GHz clients that do not support 802.11h, RUCKUS recommends disabling ChannelFly for 2.4 GHz but leaving it enabled for the 5 GHz band.

FIGURE 354 Self Healing



Background Scanning

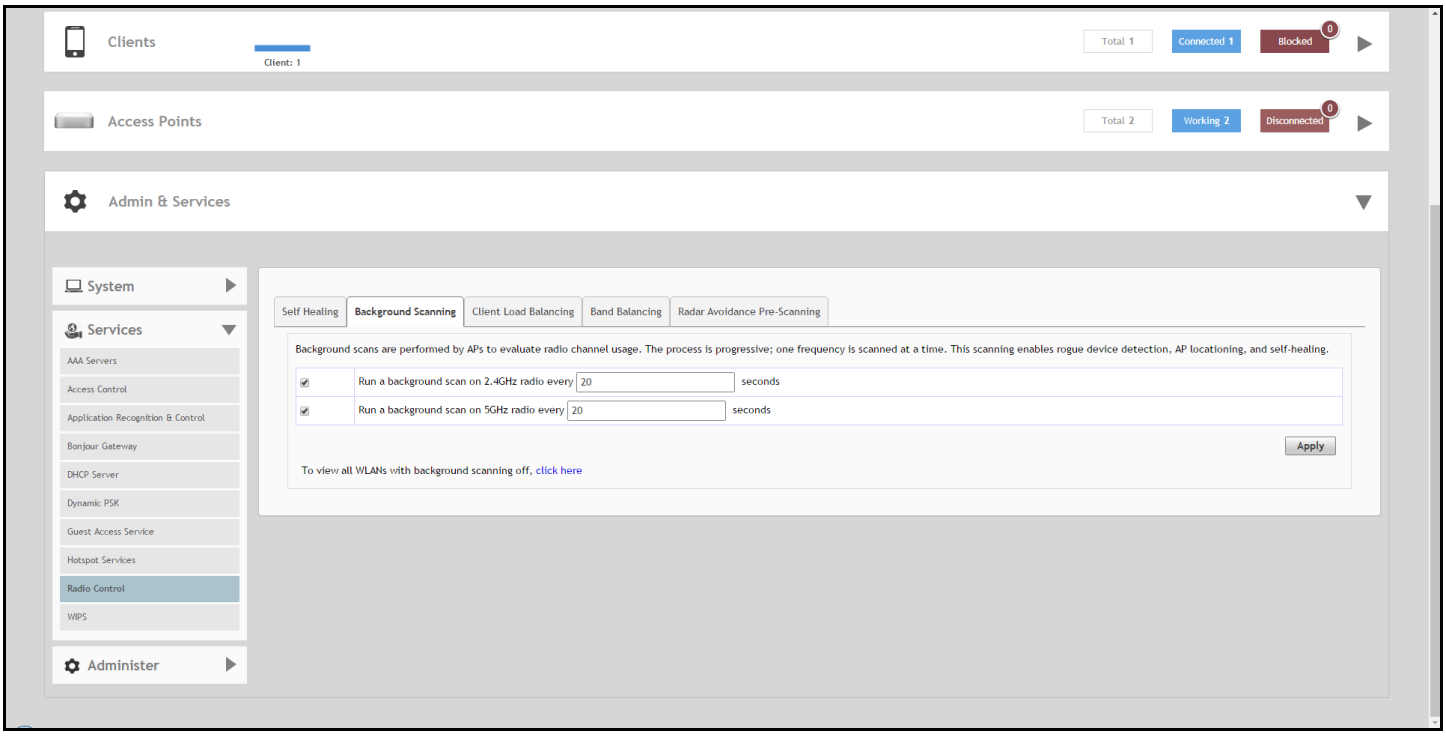
Scanning intervals can be configured on the 2.4 GHz and 5 GHz radios independently.

- **Run a background scan on the 2.4 GHz radio every [ ]**: Select this check box enter the time interval (1~65535 seconds, default is 300) that you want to set between each scan.
- **Run a background scan on the 5 GHz radio every [ ]**: Select this check box enter the time interval (1~65535 seconds, default is 300) that you want to set between each scan.

NOTE
If you want to disable Background Scanning, clear the check box; this should result in a minor increase in AP performance, but removes the detection of rogue APs. You can also decrease the scan frequency, as less frequent scanning improves overall AP performance.

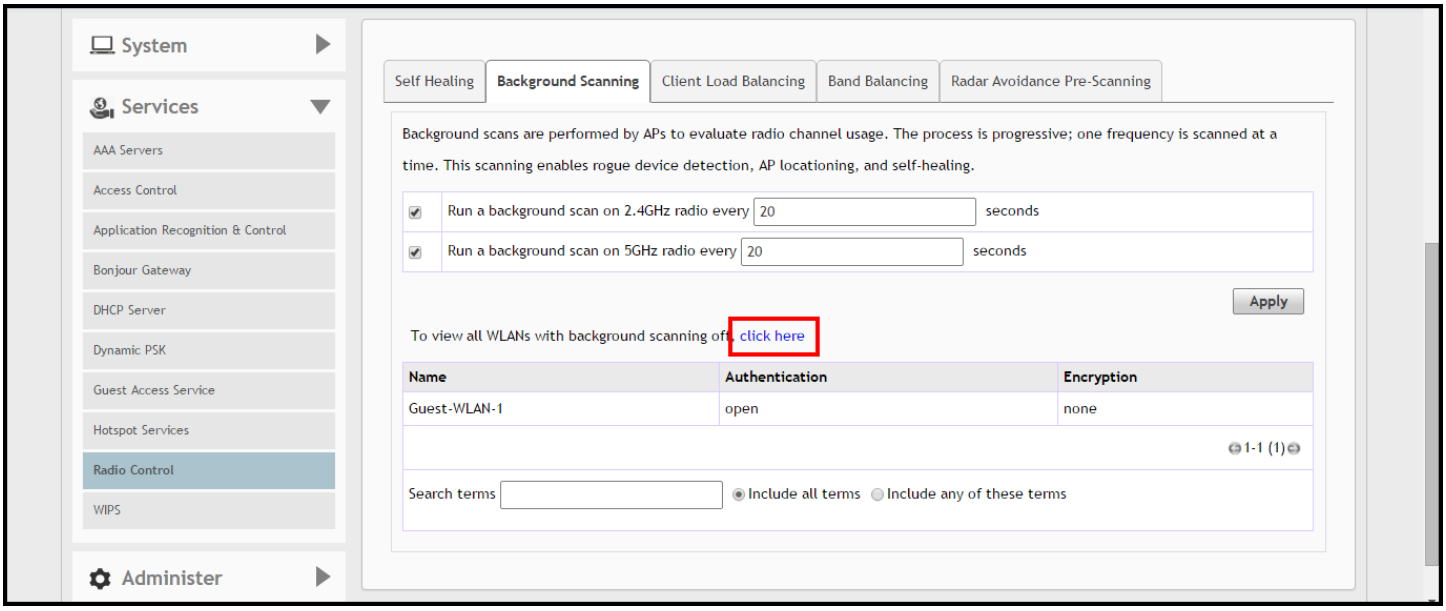
NOTE
You can also disable Background Scanning on a per-WLAN basis from the **Dashboard > Wi-Fi Networks** screen. To disable scanning for a particular WLAN, click the **Edit** link next to the WLAN for which you want to disable scanning, open **Advanced Options**, select the **Radio Control** tab, and click the check box next to **Disable Background Scanning**.

FIGURE 355 Background Scanning



To see whether Background Scanning is enabled or disabled for a particular WLAN, click the **click here** link at the bottom of the page.

FIGURE 356 Viewing the WLANs with Background Scanning Disabled



Client Load Balancing

Enabling load balancing can improve WLAN performance by helping to spread the client load between nearby access points, so that one AP does not get overloaded while another sits idle. The load balancing feature can be controlled from within the Unleashed web interface to balance the number of clients per radio on adjacent APs. "Adjacent APs" are determined at startup by measuring the RSSI during channel scans. After startup, Unleashed uses subsequent scans to update the list of adjacent radios periodically and when a new AP sends its first scan report. When an AP leaves, Unleashed immediately updates the list of adjacent radios and refreshes the client limits at each affected AP.

Once Unleashed is aware of which APs are adjacent to each other, it begins managing the client load by sending desired client limits to the APs. These limits are "soft values" that can be exceeded in several scenarios, including: (1) when a client's signal is so weak that it may not be able to support a link with another AP, and (2) when a client's signal is so strong that it really belongs on this AP.

The APs maintain these desired client limits and enforce them once they reach the limits by withholding probe responses and authentication responses on any radio that has reached its limit.

Key points on load balancing:

- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- The process does not require any time-critical interaction between APs.
- Provides control of adjacent AP distance with safeguards against abandoning clients.
- Can be disabled on a per-WLAN basis; for instance, in a voice WLAN, load balancing may not be desired due to voice roaming considerations.
- Background scanning must be enabled on the WLAN for load balancing to work.

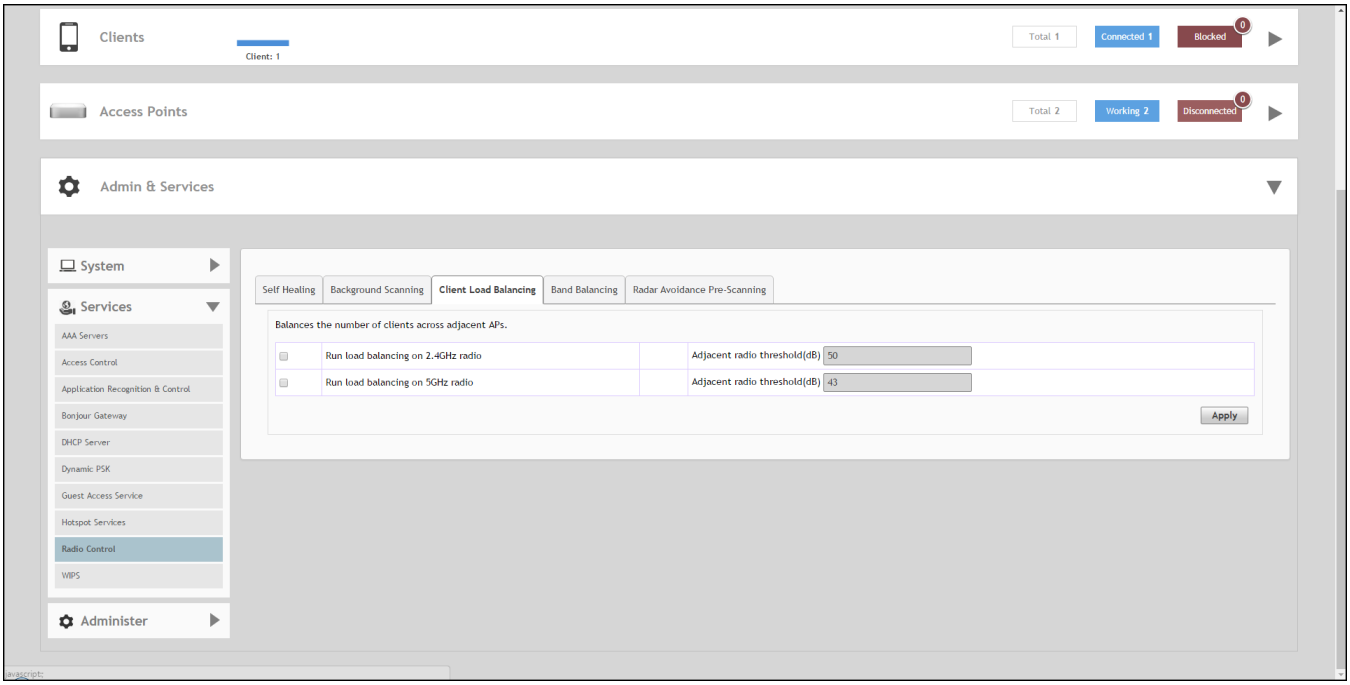
Enabling Load Balancing Globally

To enable Load Balancing globally:

1. Go to **Admin & Services > Services > Radio Control > Client Load Balancing**.

2. Enable the check box next to **Run load balancing on 2.4 GHz radio** or **Run load balancing on 5 GHz radio**, or both.
3. Enter **Adjacent Radio Threshold** (in dB), and click **Apply**.

FIGURE 357 Client Load Balancing



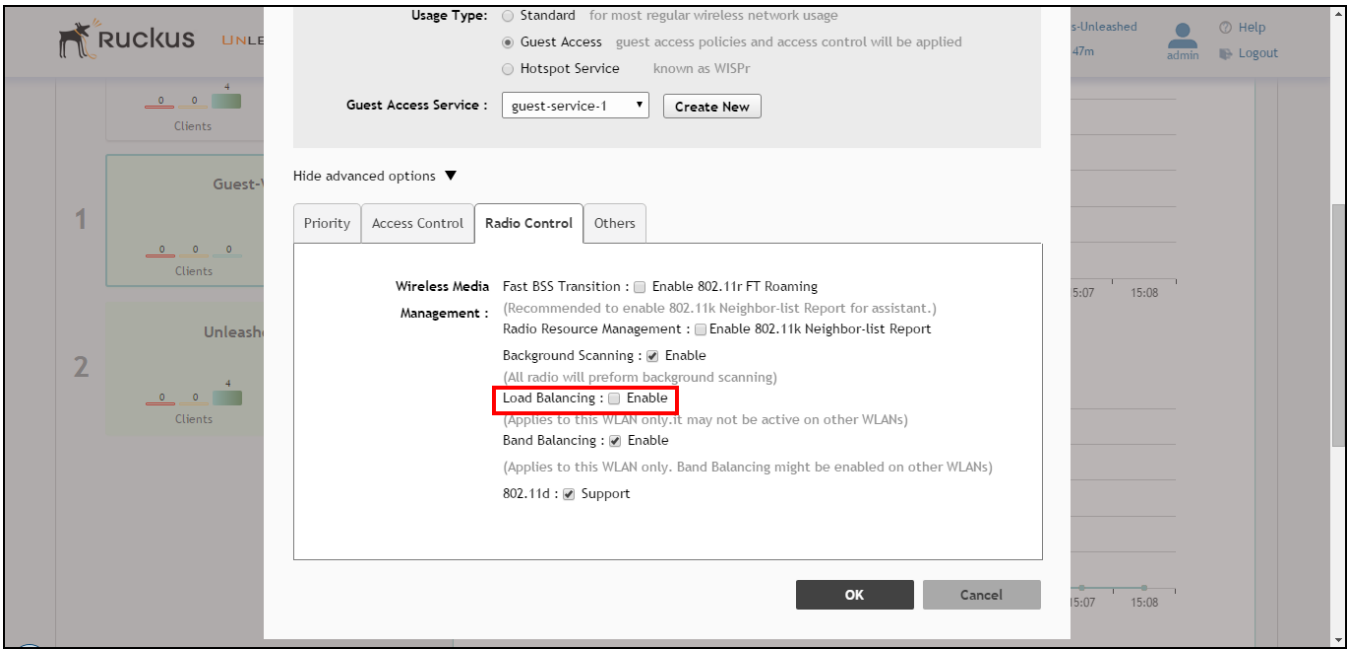
Disabling Load Balancing for a WLAN

To disable Load Balancing on a per-WLAN basis:

1. Go to **Wi-Fi Networks > Edit > Show advanced options > Radio Control**, and deselect the check box next to **Load Balancing**.

2. Click **OK** to save your changes.

FIGURE 358 Disable Load Balancing for a WLAN



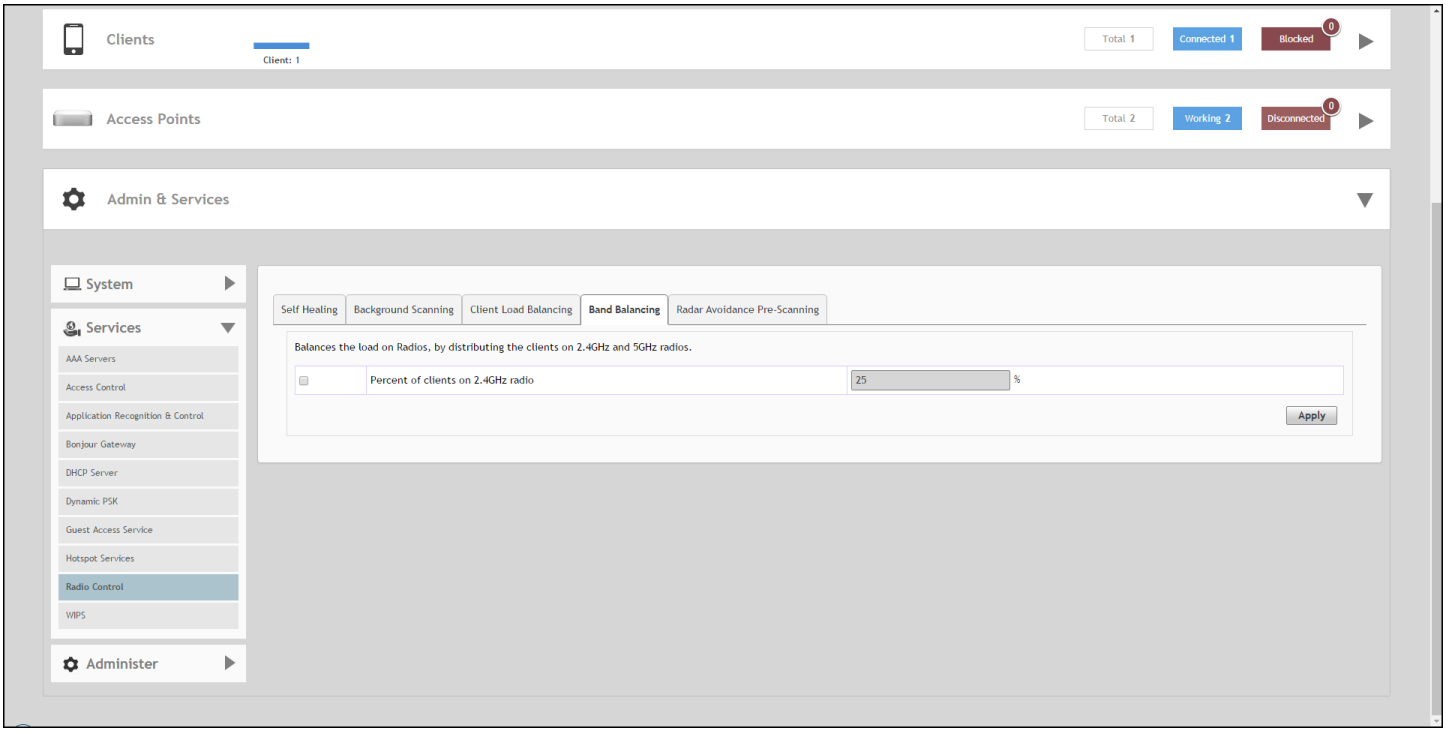
Band Balancing

Band balancing attempts to balance the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios. This feature is disabled by default. To balance the number of clients connecting to the two radios on an AP, the AP encourages dual-band clients to connect to the 5 GHz band when the configured percentage threshold is reached.

To enable Band Balancing, select the check box next to **Percent of clients on 2.4 GHz radio**, and enter a value in the **%** field, which denotes the threshold above which dual-band clients will be encouraged to connect to the 5 GHz radio rather than the 2.4 GHz radio.

NOTE
When enabled globally here, this feature will be applied to all WLANs by default. To disable Band Balancing for a specific WLAN, edit the Radio Control Settings on page 284 for the WLAN using the WLAN Advanced Options.

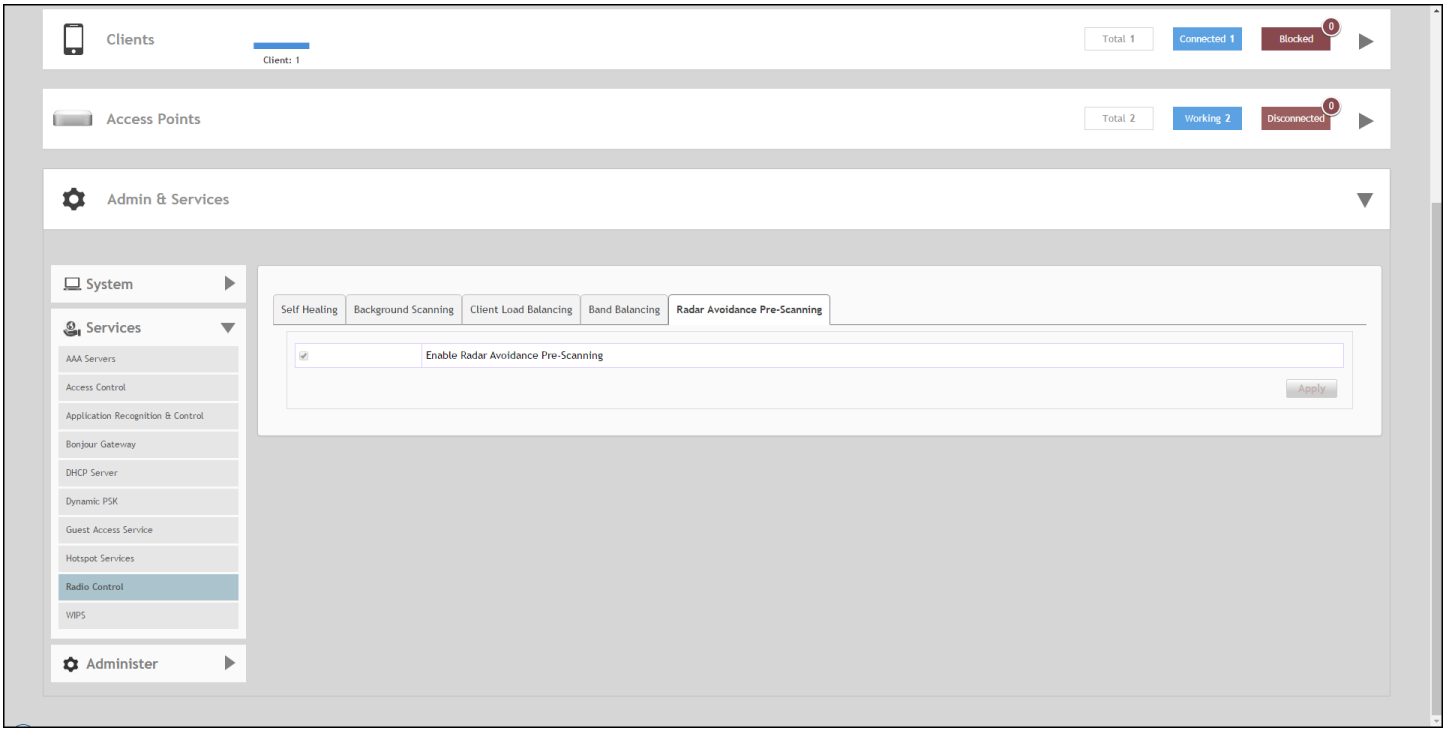
FIGURE 359 Band Balancing



Radar Avoidance Pre-Scanning

The Radar Avoidance Pre-Scanning (RAPS) setting allows pre-scanning of DFS channels in the 5 GHz band to ensure the channel is clear of radar signals prior to transmitting on the channel. This setting affects select outdoor dual band 802.11n/ac AP models only and has no impact on APs that do not support the feature. The option will also only be available if the Country Code settings are configured to allow use of DFS channels (see Setting the Country Code on page 390).

FIGURE 360 Radar Avoidance Pre-Scanning



WIPS

Unleashed provides several built-in intrusion prevention features designed to protect the wireless network from security threats such as Denial of Service (DoS) attacks and intrusion attempts. These features, called Wireless Intrusion Prevention Services (WIPS), allow you to customize the actions to take and the notifications you would like to receive when each of the different threat types is detected.

Denial of Service (DoS)

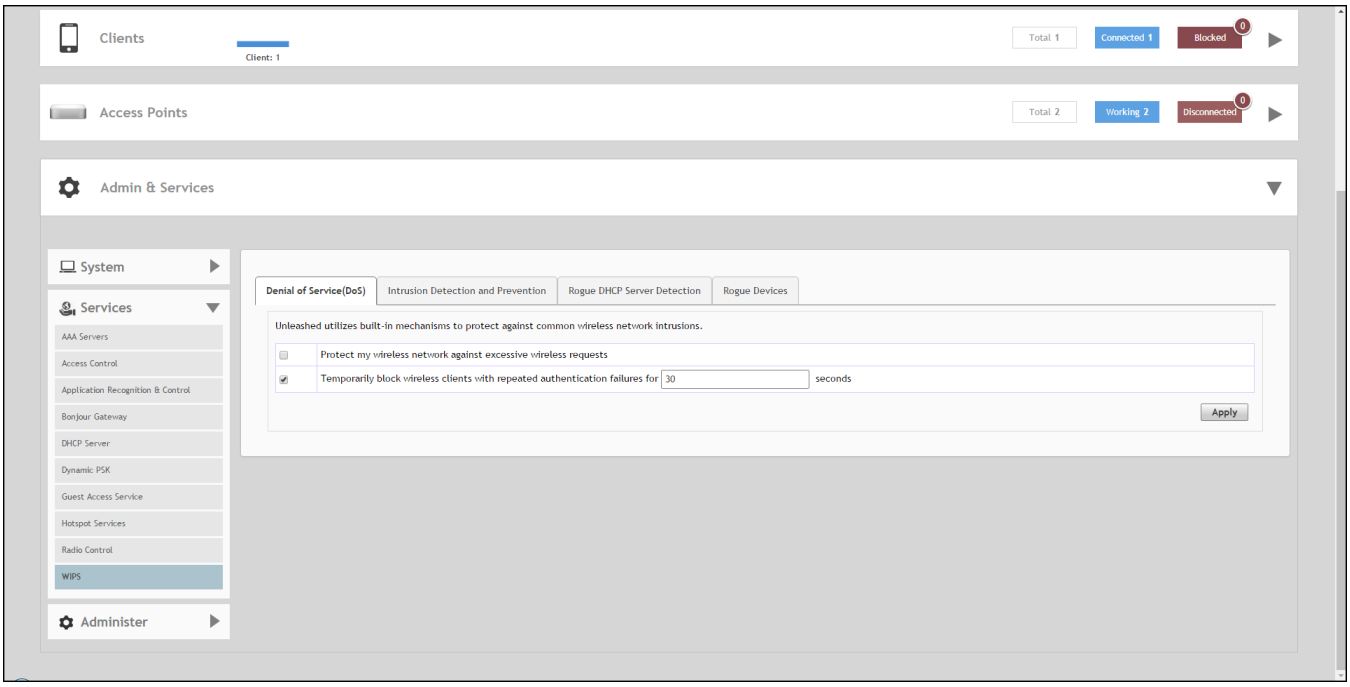
Two options are provided to protect the wireless network from Denial of Service attacks.

To configure the DoS protection options:

1. Go to **Admin & Services > Services > WIPS > Denial of Service (DoS)**.
2. Configure the following settings:
   - **Protect my wireless network against excessive wireless requests**: If thiscapability is activated, excessive 802.11 probe request frames and management frames launched by malicious attackers will be discarded.
   - **Temporarily block wireless clients with repeated authentication failures for [ ] seconds**: If this capability is activated, any clients that repeatedly fail in attempting authentication will be temporarily blocked for a period of time (10~1200 seconds, default is 30).

3. Click **Apply** to save your changes.

FIGURE 361 Denial of Service (DoS)



Intrusion Detection and Prevention

Intrusion detection and prevention features rely on background scanning results to detect rogue access points connected to the network and optionally, prevent clients from connecting to malicious rogue APs.

Rogue Access Points

A "Rogue Access Point" is any access point detected by an Unleashed access point that is not part of the Unleashed network. Rogue devices are detected during off channel scans (background scanning) and are simply other access points that are not part of the Unleashed network (e.g., an access point at a nearby coffee shop, a neighbor's apartment or shopping mall).

Typically, rogue access points are not a threat, however there are certain types that do pose a threat that will be automatically identified as "malicious rogue APs." The three automatically identified malicious access point categories are as follows:

- WLAN-Spoofing: These are rogue access points that are beaconing the same WLAN name as an Unleashed access point. They pose a threat as someone may be attempting to use them as a honey pot to attract your clients into their network to attempt hacking or man-in-the-middle attacks to exploit passwords and other sensitive data.
- Same-Network: These are rogue access points that are detected by other access points as transmitting traffic on your internal network. They are detected by Unleashed access points seeing packets coming from a 'similar' MAC address to one of those detected from an over the air rogue AP. Similar MAC addresses are +-5 MAC addresses lower or higher than the detected over the air MAC address.
- MAC-spoofing: These are rogue access points that are beaconing the same MAC address as an Unleashed access point. They pose a threat as someone may be attempting to use them as a honey pot to attract your clients into their network to attempt hacking or man-in-the-middle attacks to exploit passwords and other sensitive data.

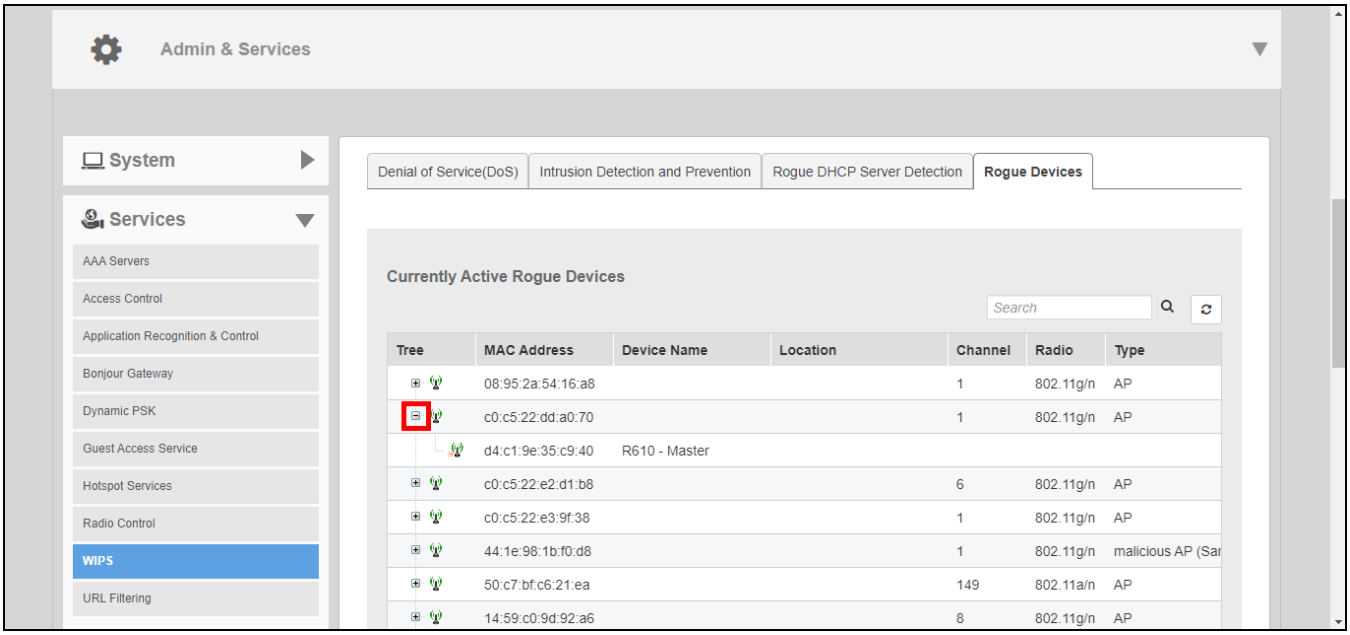
Managing Rogue Devices

The Rogue Devices screen displays all currently active rogue APs that have been detected by any of the Unleashed APs on the network.

To monitor rogue devices and mark specific rogues as either "known" or "malicious" rogue APs:

1. Go to **Admin & Services > Services > WIPS > Rogue Devices**.
2. View the list of *Currently Active Rogue Devices* and take note of any rogues marked as "malicious."
3. To view which Unleashed APs are detecting this rogue AP, click the **+** icon next to the rogue AP to expand the display. Use this information to help investigate where the rogue device is located in your site for removing it.

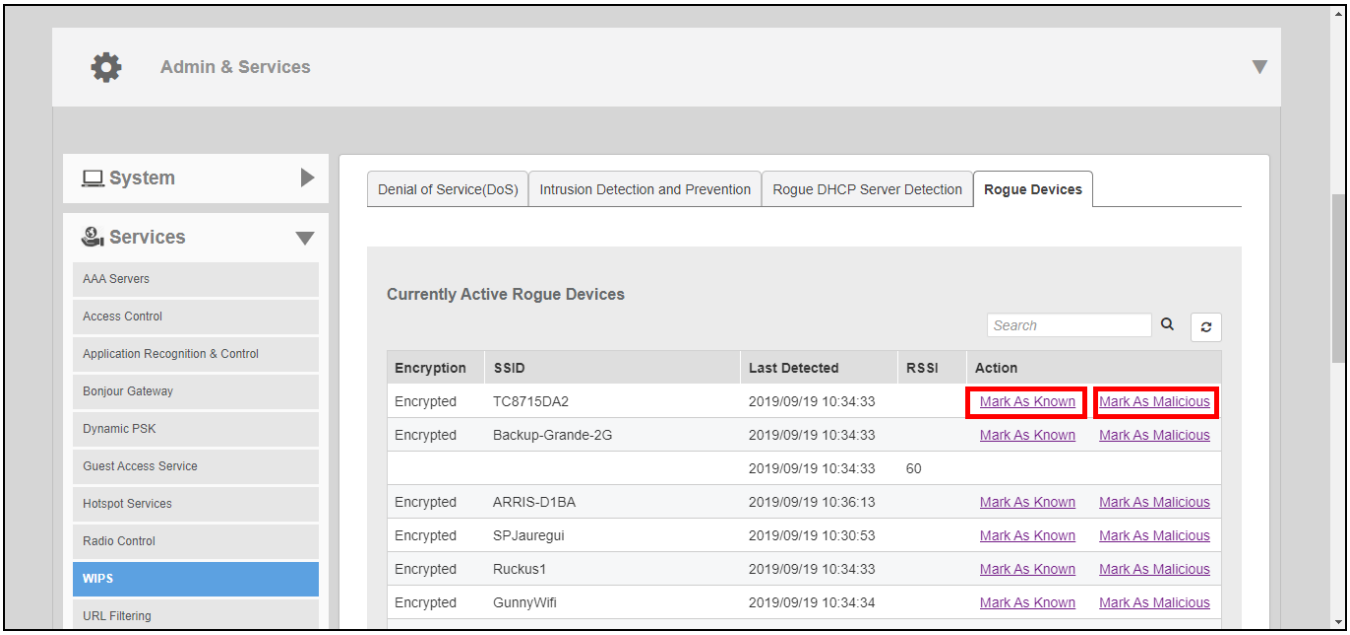
FIGURE 362 Monitoring rogue devices - expand the view to show which APs are detecting this rogue device



4. To mark a rogue device as a "Known" device (for example, a nearby neighbor's network), click **Mark As Known**. This device will no longer trigger rogue device detection alarm events on the *Administration > Diagnostics* pages.

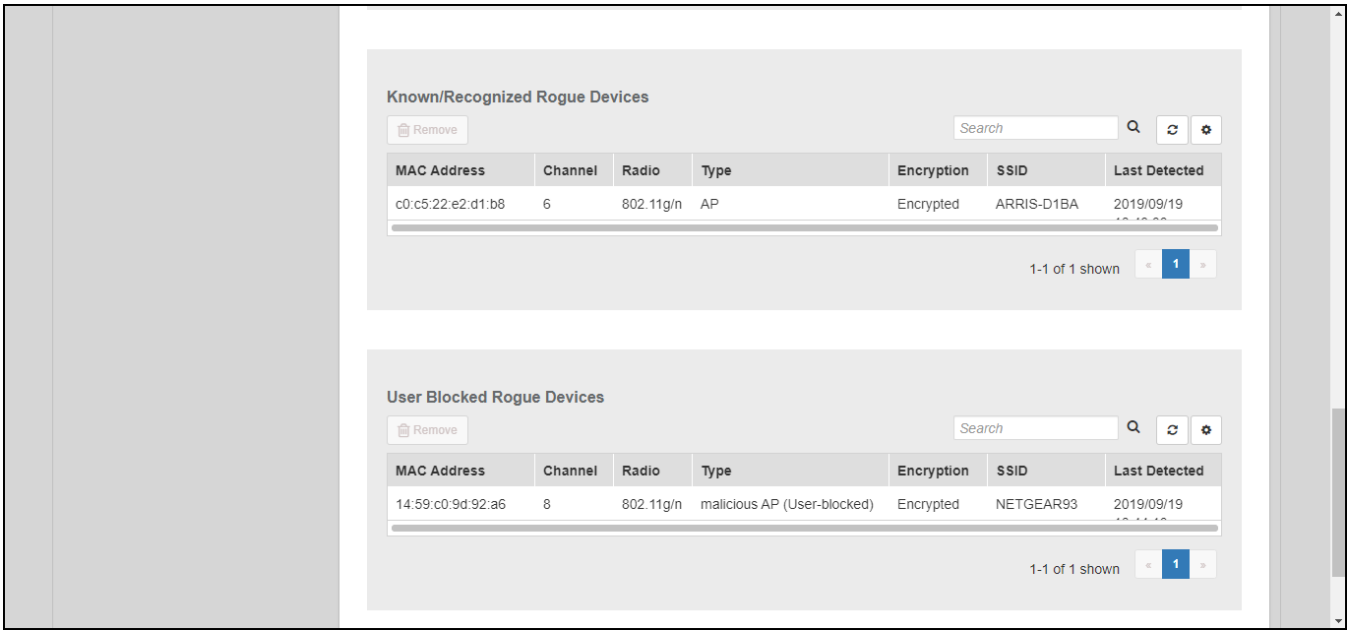
5. To mark a rogue device as "Malicious" rogue (with the goal of physically locating and removing the offending device), click **Mark as Malicious**.

FIGURE 363 Marking rogue devices as known or malicious



6. You can monitor and manage the lists of known/recognized and user-blocked rogue devices using the two tables below.

FIGURE 364 Manage known rogue devices

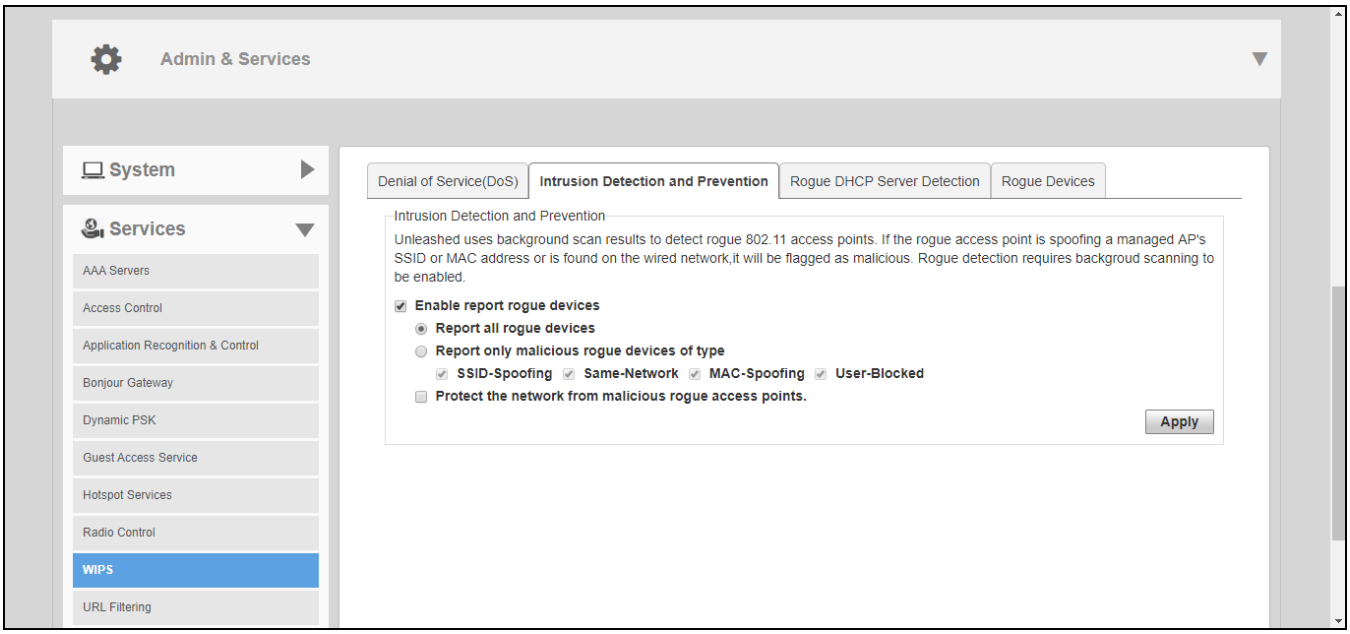


Rogue AP Detection

To enable/disable and configure Rogue Access Point detection:

1. Go to **Admin & Services > Services > WIPS > Intrusion Detection and Prevention**.
2. Enable the **Enable report rogue devices** option to include rogue device detection in logs and email alarm event notifications.
3. Select which devices to include in rogue device reports:
   - **Report all rogue devices**: Send alerts for all rogue AP events.
   - **Report only malicious rogue devices of type**: Select which event types to report.
     - **SSID-spoofing**: A malicious rogue AP that uses the same SSID as ZoneDirector's AP, also known as an "Evil-twin" AP.
     - **Same-Network**: A malicious rogue AP that is connected to the same wired network.
     - **MAC-spoofing**: A malicious rogue AP that has the same BSSID (MAC) as one of the virtual APs managed by ZoneDirector.
     - **User-Blocked**: A rogue AP that has been marked as malicious by the user.
4. Enable the **Protect the network from malicious rogue access points** feature to automatically protect your network from network connected rogue APs, WLAN-spoofing APs and MAC-spoofing APs. When one of these rogue APs is detected (and this check box is enabled), the RUCKUS AP automatically begins sending broadcast de-authentication messages spoofing the rogue's BWLAN (MAC) to prevent wireless clients from connecting to the malicious rogue AP. This option is disabled by default.
5. Click **Apply** to save your changes.

FIGURE 365 Intrusion Detection and Prevention



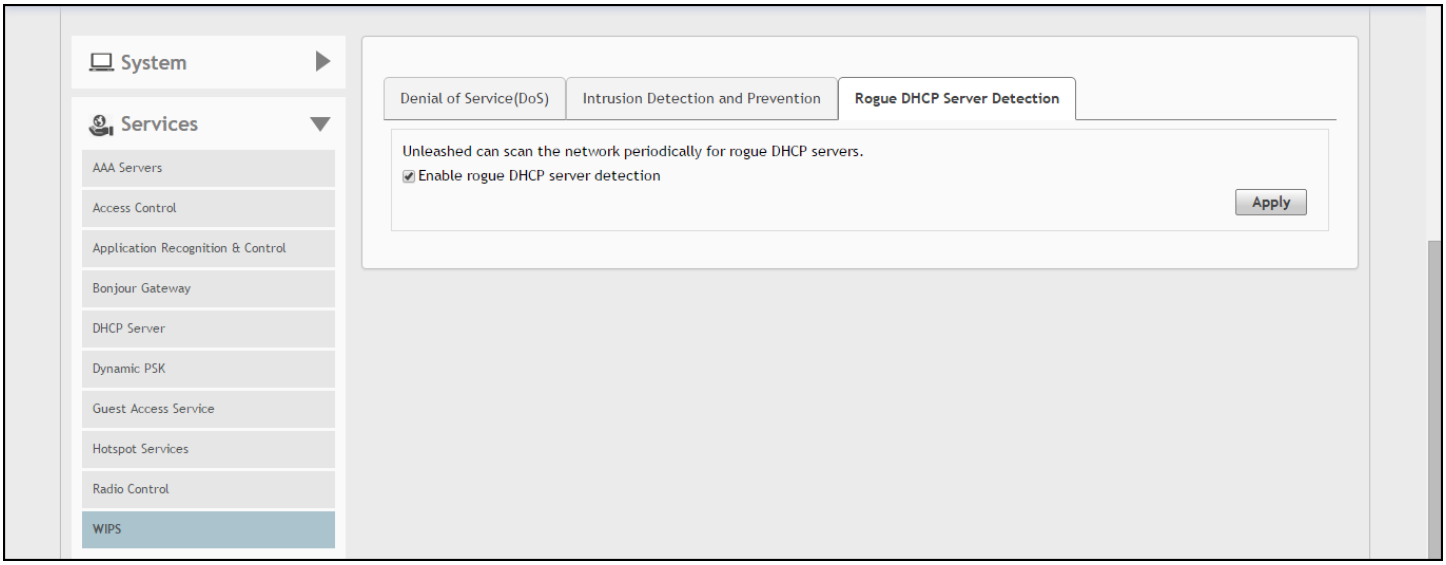
Rogue DHCP Server Detection

A rogue DHCP server is a DHCP server that is not under the control of network administrators and is therefore unauthorized. When a rogue DHCP server is introduced to the network, it could start assigning invalid IP addresses, disrupting network connections or preventing client devices from accessing network services. It could also be used by hackers to compromise network security.

Typically, rogue DHCP servers are network devices (such as routers) with built-in DHCP server capability that has been enabled (often, unknowingly) by users. The rogue DHCP server detection feature can help you prevent connectivity and security issues that rogue DHCP servers may cause. When

this feature is enabled, RUCKUS Unleashed scans the network every five seconds for unauthorized DHCP servers and generates an event every time it detects a rogue DHCP server.

FIGURE 366 Rogue DHCP Server Detection



URL Filtering

URL filtering allows administrators to manage internet usage by preventing access to inappropriate websites using a customizable combination of blocklists and allowlists.

The RUCKUS URL filtering implementation uses a third-party web classification system that groups a wide variety of internet domains into various levels of inappropriate content, and allows flexible control according to the deployment environment.

Each website is categorized into one of the 83 categories. To find out which category a website falls into, see the Webroot BrightCloud Server site lookup tool (https://www.brightcloud.com/tools/url-ip-lookup.php).

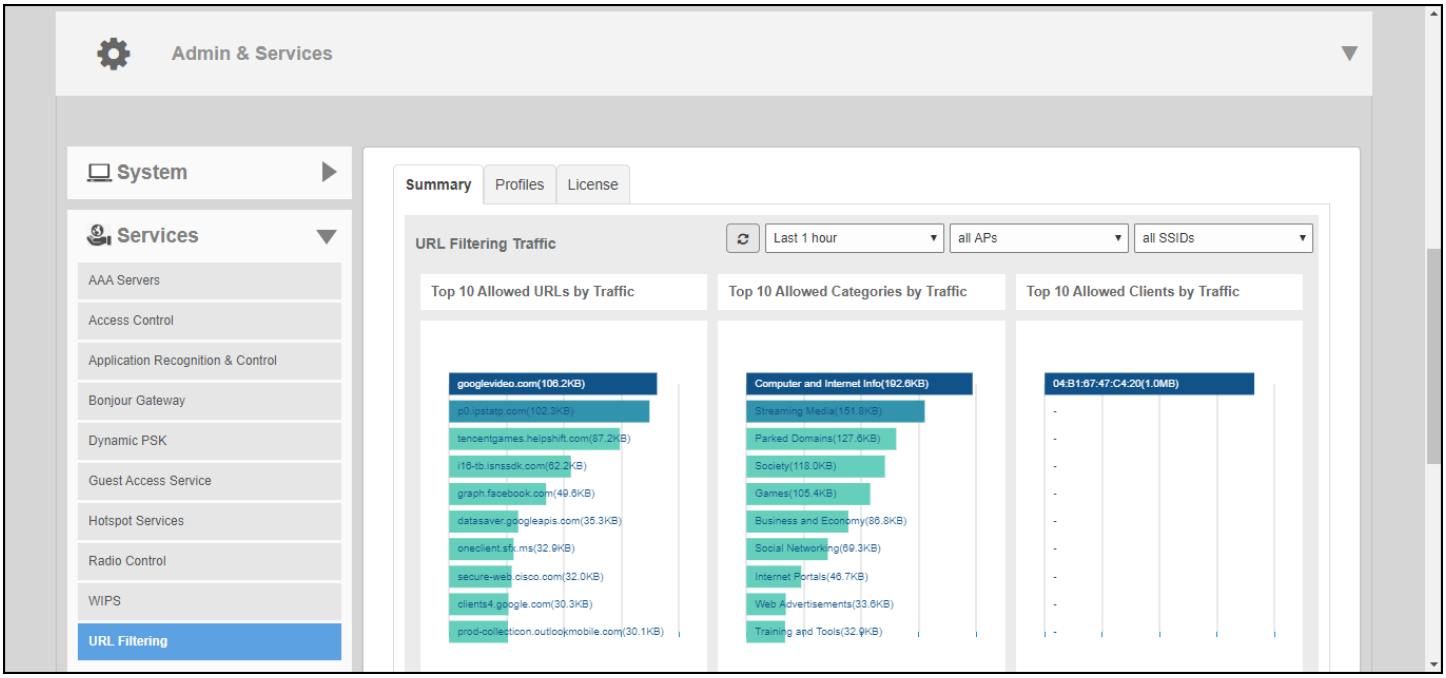
To deploy URL filtering, you must create a URL filtering profile using either one of the preset category groups or a customized selection of categories. Once a profile is created, you can apply it to one or more WLANs.

There are four pre-defined category groups and one custom category group:

- **No adult content**: No adult content or nudity.
- **Clean and safe**: No adult content plus no malware, spyware, phishing, botnets or spamware.
- **Child and student friendly**: Clean and safe plus no alcohol, intimate apparel, dating, or weapons.
- **Strict**: Child and student friendly plus no streaming media, personal storage and games.
- **Custom**: Select the categories of traffic to block from the list.

Once enabled, you can view lists of the top URLs blocked by the system, top clients attempting to visit restricted domains, top allowed URLs and content categories by traffic volume, and other useful metrics from the URL Filtering Summary tab.

FIGURE 367 URL Filtering



Creating a URL Filtering Profile

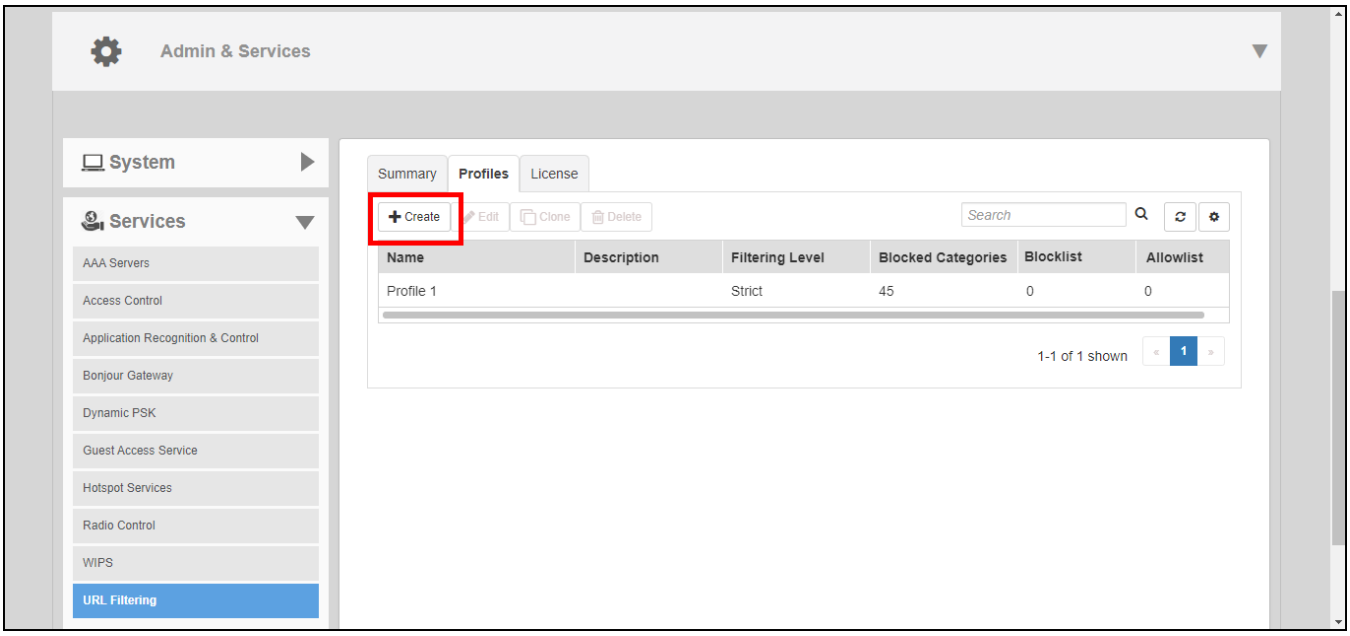
You must create a URL filtering profile before you can apply the profile to a WLAN or to a user role.

To create a URL filtering profile:

1. Go to **Admin & Services Services > URL Filtering**.
2. Click the **Profiles** tab.

3. Click **Create**. The *Create New* form appears.

FIGURE 368 Creating a URL Filtering Profile



4. Enter a **Name** and optionally a **Description** for this profile.

5. Select one of the content filtering category groups, in increasing order of strictness, or select **Custom**, and select any number of individual categories.

FIGURE 369 Selecting Level of Strictness

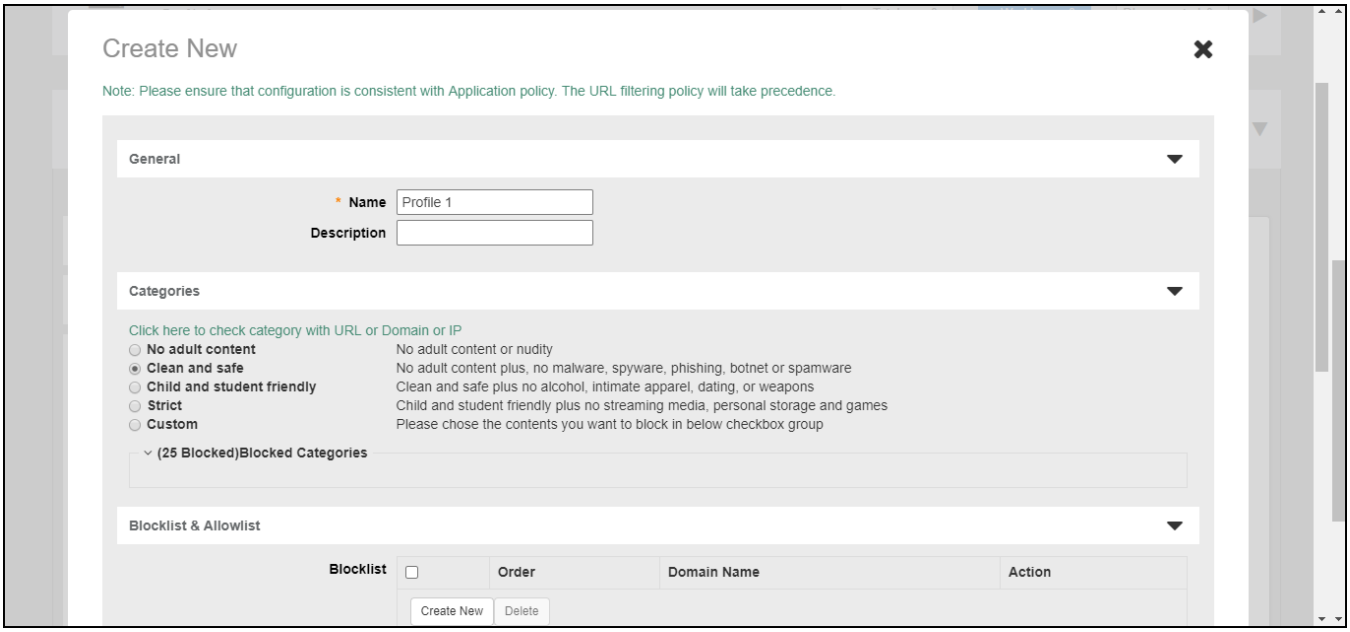
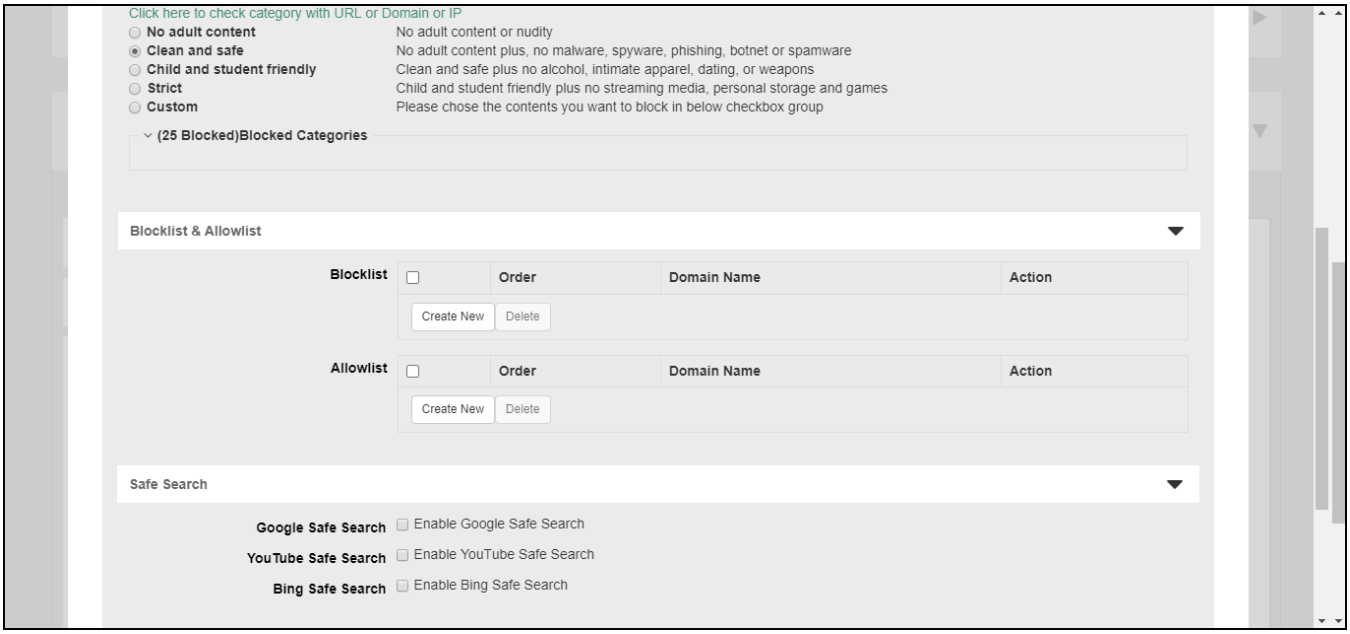


FIGURE 370 Blocklisting or Allowlisting a Specific URL



6. Optionally, in *Blocklist & Allowlist*, you can add custom URLs to either block or allow. Allowlist and blocklist entries override the rules configured above. A maximum of 16 blocklist and 16 allowlist entries can be created per profile.
7. Optionally, in *Safe Search*, enable or disable "Safe Search" functionality from Google, Youtube, or Bing.

8. Click **OK** to save your changes. A maximum of 32 profiles can be created.

Applying a URL Filtering Policy to a WLAN

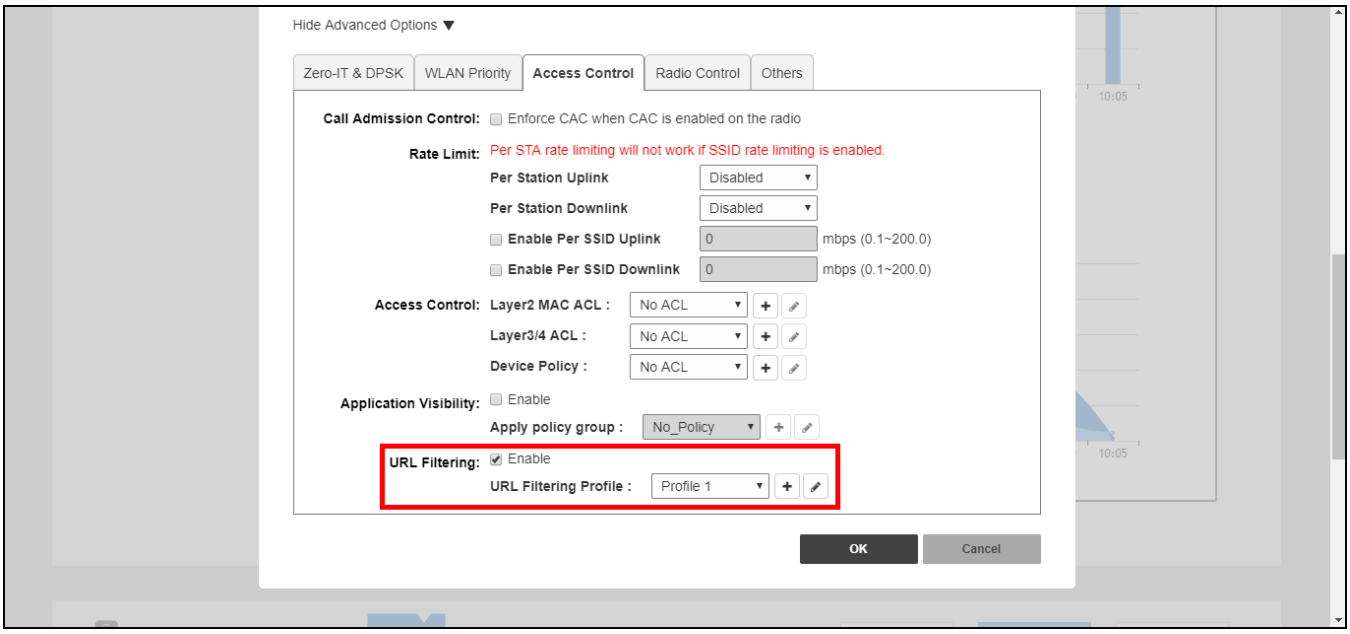
Once a URL filtering policy has been created, you can apply it to your wireless networks using the following procedure.

To apply a URL filtering policy to a WLAN:

1. Go to **WiFi Networks**, select the WLAN you would like to configure, and click **Edit**.
2. Scroll down and expand the **Advanced Options** section.
3. Click the **Access Control** tab.
4. In *URL Filtering*, select **Enable** and choose a **URL Filtering Profile** from the drop-down list.

   Alternatively, click the **+** (Create New) icon to create a new profile and apply it to this WLAN.
5. Click **OK** to save your changes.

FIGURE 371 Enabling URL filtering for a WLAN

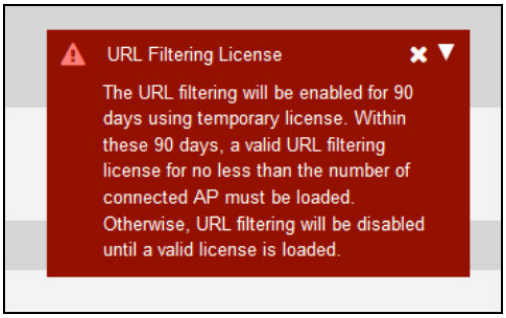


Working with URL Filtering Licenses

URL filtering service requires an active URL filtering license to function. URL filtering licenses can be purchased from RUCKUS partners and distributors, and a temporary license is also available to allow customers to try out the service for a limited time of 90 days before purchasing.

Within 90 days, a valid URL filtering license that is greater or equal to the number of connected APs must be loaded; otherwise, URL filtering will be disabled until a valid license is loaded.

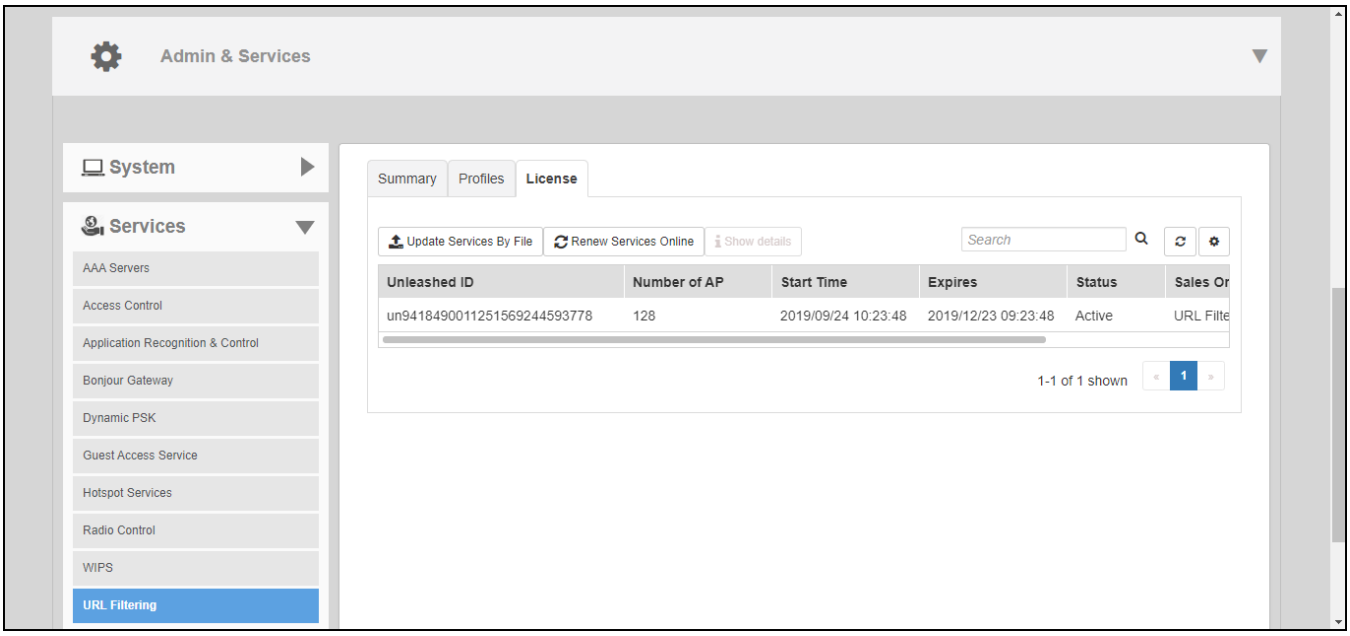
FIGURE 372 URL Filtering License Warning Message



Complete the following steps to manage URL filtering licenses.

1. Go to **Admin & Services** > **Services** > **URL Filtering**.
2. Click the **License** tab and select one of the following options:
   - **Update Services By File**: Import a new locally saved license file.
   - **Renew Services Online**: Connect to the RUCKUS license server to download a license file.
   - **Show Details**: Select the license file from the list and click **Show Details** to view the license expiration details.

FIGURE 373 Working with URL Filtering Licenses



Wi-Fi Calling

The RUCKUS Unleashed Wi-Fi Calling feature aims to provide better call quality by reducing latency, jitter, and roaming delays for voice calls over Wi-Fi.

To achieve this, the RUCKUS Unleashed access point must perform identification, classification, and marking of voice calls when Wi-Fi calling is enabled and a call is made from a supported client device. Once a call is identified, voice packets are classified and marked to be delivered over an Internet Protocol Security (IPsec) tunnel from the client through the AP and the controller and on to the mobile operator's data center.

The Wi-Fi calling provides the following benefits:

- Faster inter-AP roaming using RUCKUS SmartRoam along with standards-based .11r/k technologies minimizes IPsec session timeouts or teardowns to avoid call drops.
- Voice-aware SmartCast prioritization helps maintain sustained call quality even when there are other clients generating regular Internet packet data.
- A voice call on one SSID will be prioritized in the voice queue over Internet packet data from other SSIDs.

The process consists of the following steps:

1. User turns on Wi-Fi Calling in the phone menu, or turns on Wi-Fi and connects to the wireless network.
2. Client initiates a DNS lookup to the domain name of the Evolved Packet Data Gateway (ePDG) (for example, T-Mobile: ss.epdg.epc.mnc260.mcc310.pub.3gppnetwork.org).

   NOTE
   The ePDG on an LTE network acts as an interface between the user device and the non-trusted 3rd Generation Partnership Project (3GPP) access network (for example, Wi-Fi hostpot), providing a security mechanism through a secure IPsec tunnel that is established with the user device.

3. Client initiates an Internet Key Exchange version 2 (IKEv2) handshake towards the ePDG to authenticate and set up an IPsec tunnel.
4. Client initiates an IPsec session towards the ePDG.
5. User is notified that Wi-Fi Calling is activated.
6. User initiates a voice call. All voice traffic is tunneled to the ePDG within the IPsec tunnel.

Creating a Wi-Fi Calling Profile

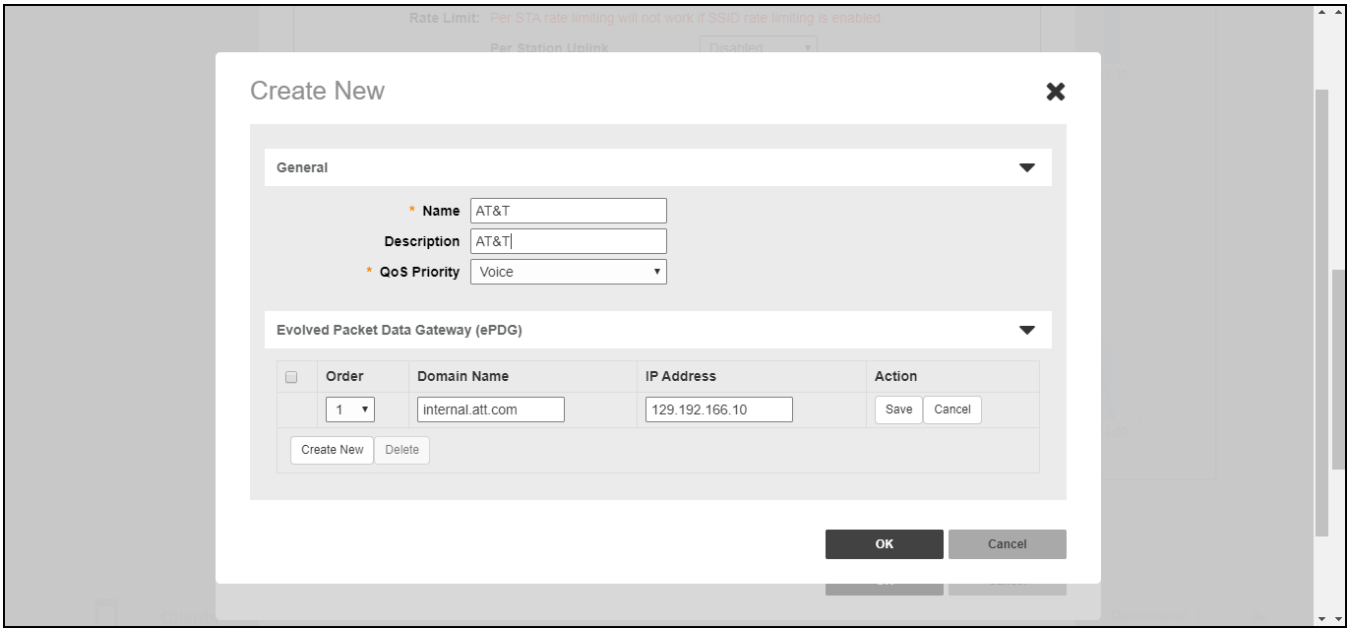
A Wi-Fi calling profile must be associated to any WLAN with Wi-Fi calling enabled.

To create a Wi-Fi calling profile:

1. Go to **Admin & Services > Services > W-Fi Calling** and click the **Profiles** tab.
2. Click **Create** to create a new profile.

3. In the *Create New* dialog, enter the following to create a new profile:
   - **Name**: Enter a name for the profile.
   - **Description**: Optionally, enter a description of the profile.
   - **QoS Priority**: Select a priority from the list (typically, Voice for highest QoS priority).
   - **Evolved Packet Data Gateway (ePDG)**: Click **Create New** to create a new ePDG entry. Enter **Domain Name** and optionally **IP address**, and click **Save** to save the entry.

FIGURE 374 Create a Wi-Fi calling profile



Enabling Wi-Fi Calling for a WLAN

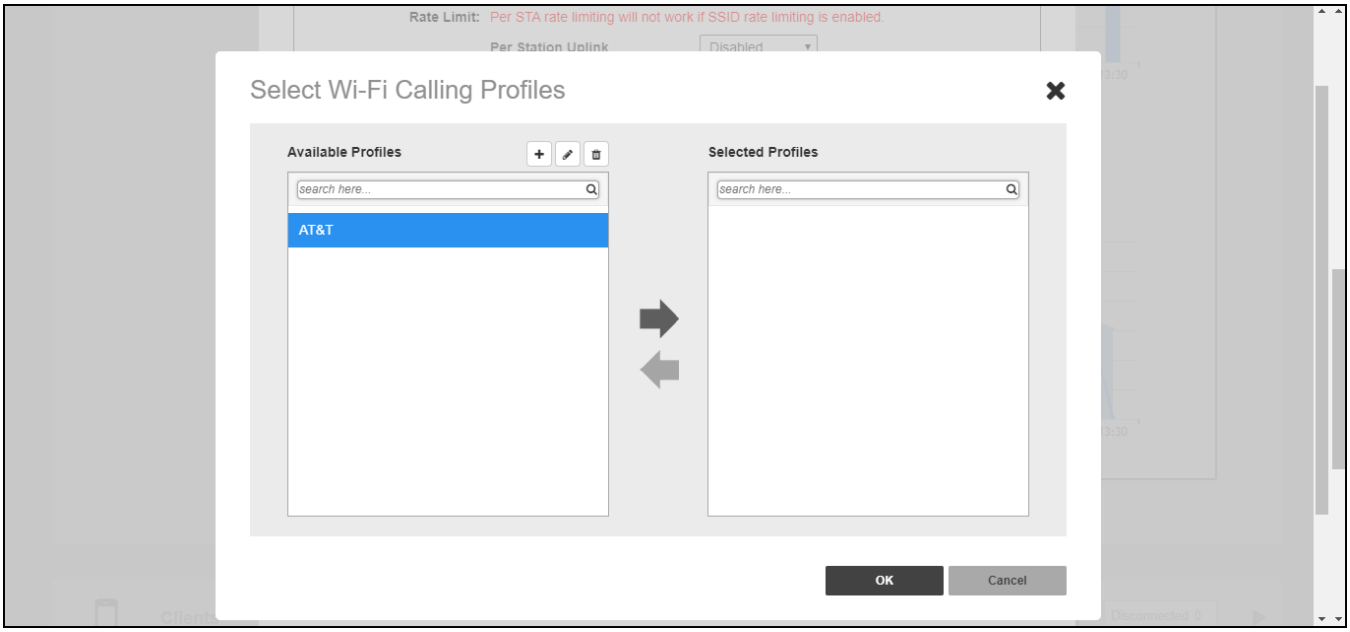
Once a Wi-Fi calling profile has been created, you must configure each WLAN with one or more profiles to enable the feature for the WLAN.

To enable Wi-Fi calling for a WLAN:

1. Select the WLAN that will support Wi-Fi calling, and click **Edit**.
2. Click **Show Advanced Options > Access Control**.
3. In **WiFi Calling**, click **Edit** to select Wi-Fi calling profiles.

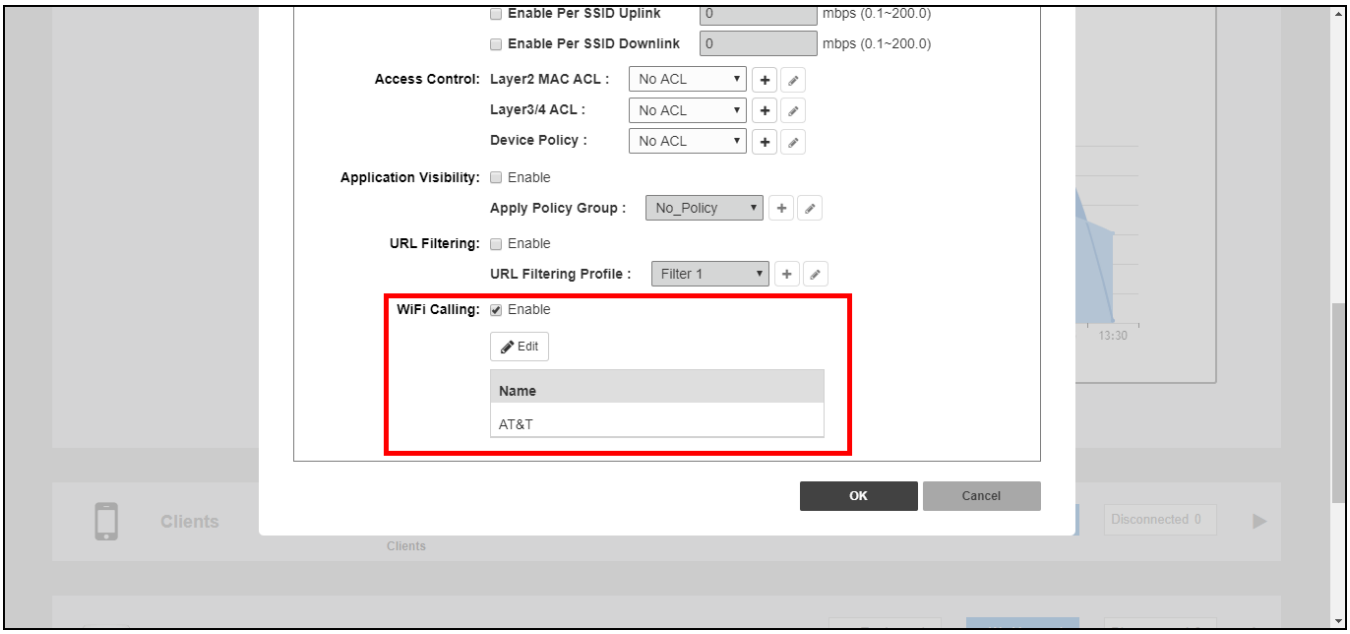
4. Select a profile from the list of *Available Profiles*, click the right arrow to move it to the list of *Selected Profiles*, and click **OK** to save your changes.

FIGURE 375 Add profiles from the available profiles to selected profiles for the WLAN



5. Click **OK** to save the changes to the WLAN advanced options.

FIGURE 376 Enabling Wi-Fi calling for a WLAN



Tunnel Configuration

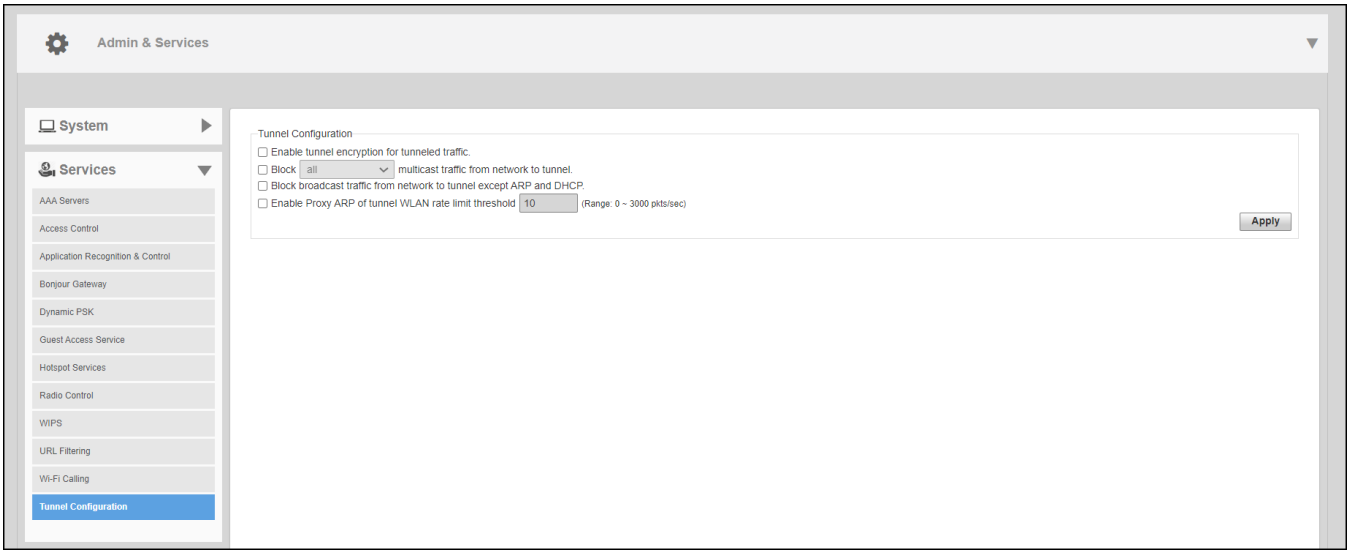
Only WLANs that are enabled with Tunnel mode are affected.

Refer to Configuring Advanced WLAN Options on page 269 in the WLAN configuration section for information on enabling Tunnel mode.

Complete the following steps to configure data encryption and filtering for tunneled WLANs.

1. From the dashboard, select **Admin & Services** > **Services**.
2. Scroll down to the bottom of the page and locate the **Tunnel Configuration** section.
3. Select the check boxes next to the options you want to enable.
   - **Enable tunnel encryption for tunneled traffic**: By default, when WLAN traffic is tunneled to Dedicated Master, only the control traffic is encrypted while data traffic is unencrypted. When this option is enabled, the Access Point will decrypt 802.11 packets and use an AES-encrypted tunnel to send them to Dedicated Master.
   - **Block multicast traffic from network to tunnel**: Prevents [all/non-well-known] multicast traffic from propagating on the tunnel.
   - **Block broadcast traffic from network to tunnel except ARP and DHCP**: Prevents all broadcast traffic other than Address Resolution Protocol and DHCP packets.
   - **Enable Proxy ARP of tunnel WLAN with rate limit threshold**: Reduces tunnels. When Dedicated Master receives a broadcast ARP request for a known host, it acts on behalf of the known host to send out unicast ARP replies at the rate limit it will forward it to the tunnel to all APs according to the rate limit threshold set in the Packet Inspection Filter program (like Wireshark).
4. Click **Apply** in the same section to save your changes.

FIGURE 377 Setting Tunnel Configuration Parameters for all WLANs with Tunnel Mode Enabled



Administration Settings

Administration settings that can be configured from the **Admin & Services > Administer** page include admin name/password, system backup and restore, upgrade, diagnostics and network management options.

Preferences

Use the **Administration > Preferences** page to set the user interface language and to change the Admin login name and password.

Configure the following admin preferences settings and click **Apply** to apply your changes:

- **Language**: Choose the web interface language.
- **Administrator Name/Password**: Change the current admin name and password.
  - **Authenticate using the admin name and password**: This is the default option. Use this option for standard login using an admin username/password.
  - **Authenticate with Auth Server**: Use this option to allow multiple users to perform admin functions based on Active Directory credentials. To enable this option, a valid Microsoft Active Directory AAA server object must be created so that Unleashed can authenticate users to the AD server. If enabled, optionally enable **Fallback to admin name/password if failed** to allow standard login if the AD authentication fails.
- **Setup Password Recovery**: Select this option, and enter a Security email, Security Question and Security Answer that can be used to recover the admin password in the event that the password is lost.

FIGURE 378 Configuring administrator preferences

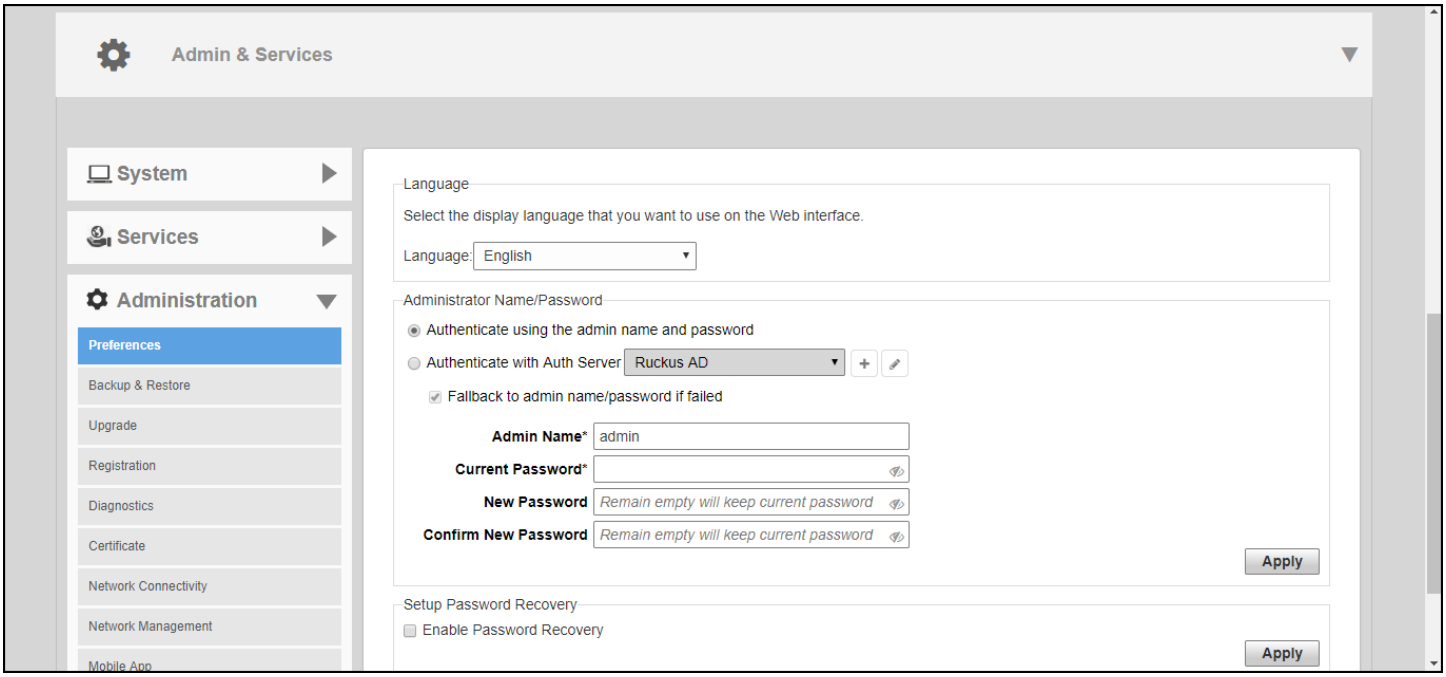
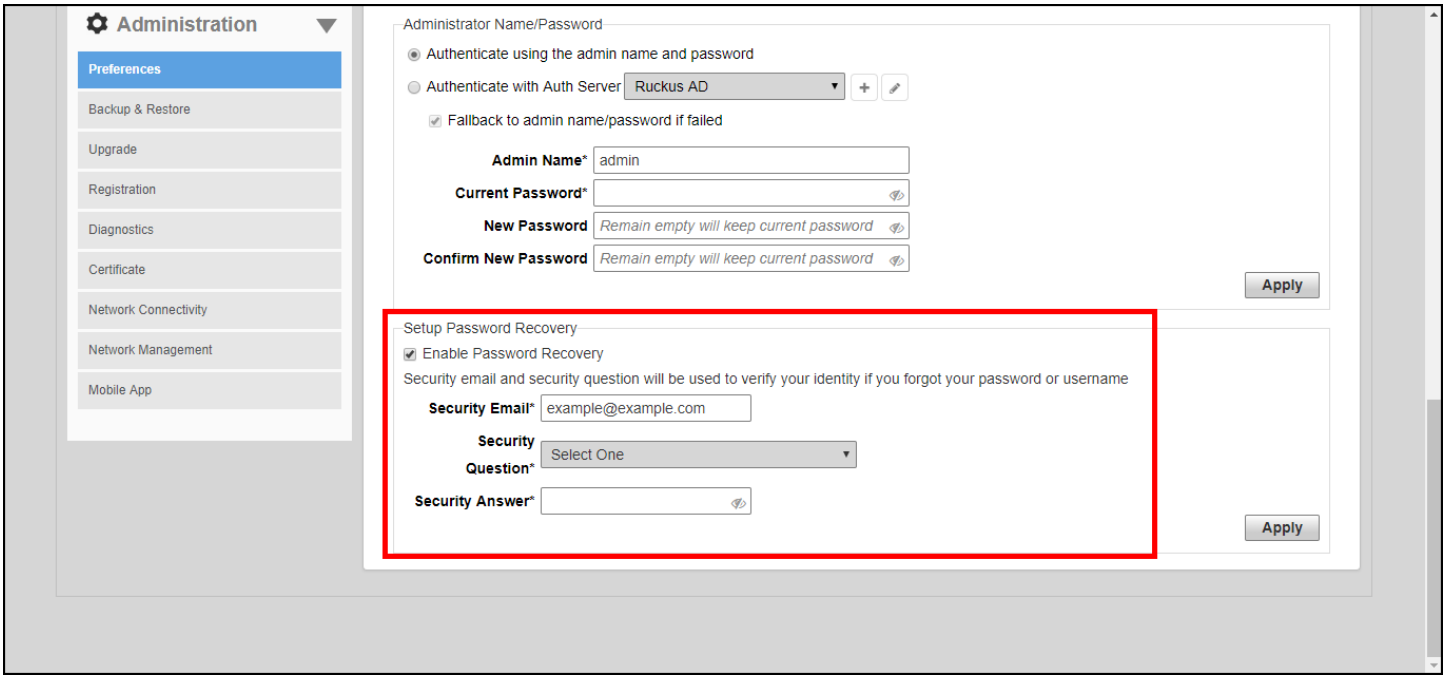


FIGURE 379 Enabling password recovery



Backup and Restore

The **Backup & Restore** page provides options for backing up your current configuration, restoring the configuration from a previous backup file, or restoring the Unleashed Master AP to factory settings.

> **NOTE**
> The backup is a small encrypted file with a .bak extension saved to the location of your choosing.

To restore settings from a backup file, click **Browse**, then select your backup file, and click **Open**. Once the .bak file has been uploaded to Unleashed, select one of three restore options for your Unleashed network.

Options include:

- **Restore Everything**
- **Restore Everything except system name and IP address**
- **Restore only WLAN settings, ACLs, roles, users, country code and system time**

FIGURE 380 Backup and Restore

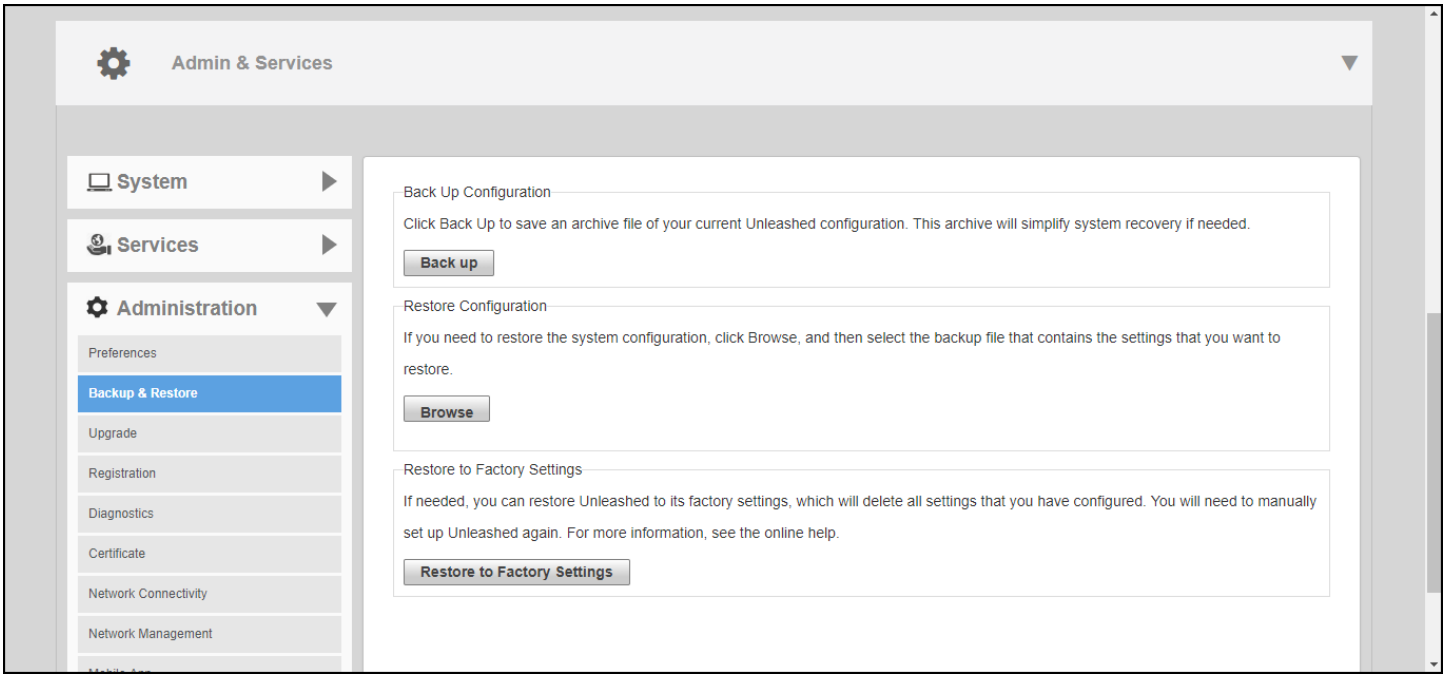
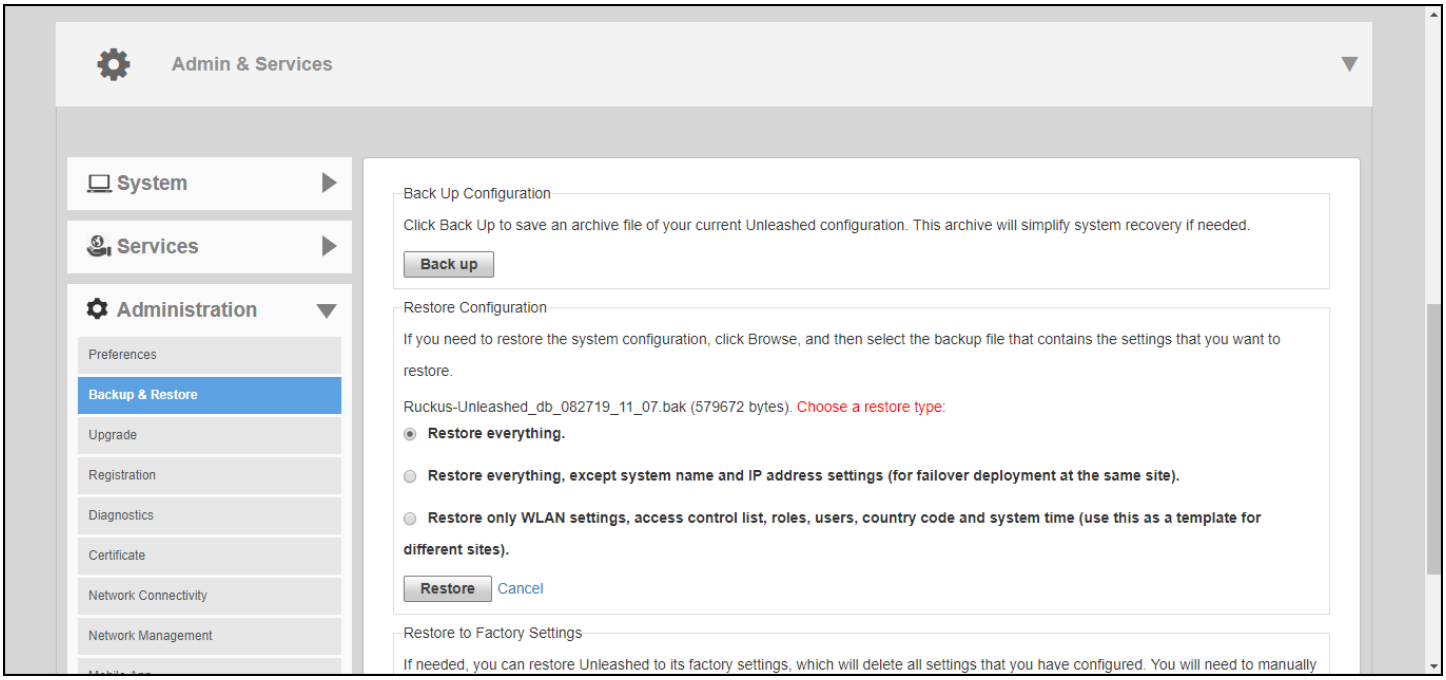


FIGURE 381 Choose a Restore type



Restore to Factory Settings

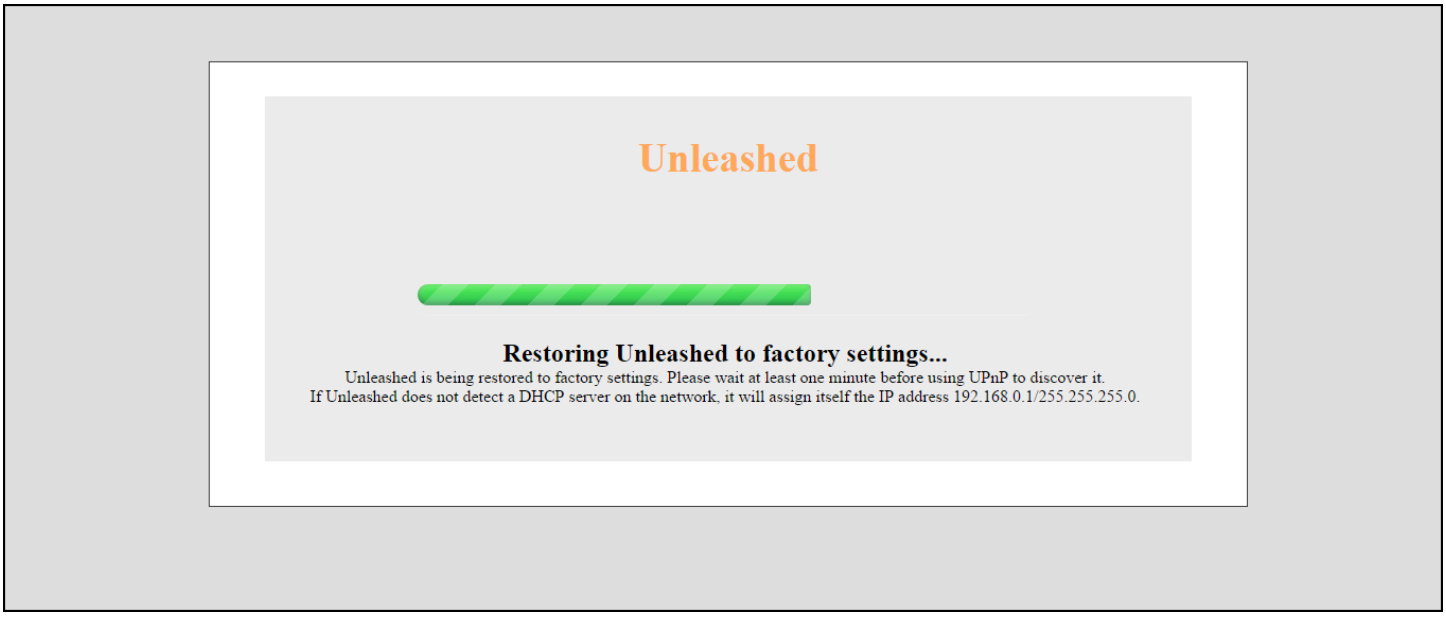
In certain extreme conditions, you may want to re-initialize your Master AP and reset it to the factory default state. Once the Master has been reset to factory default state, all AP logs, client logs, application data and other records, wireless networks, user accounts, and any other configuration settings must be reconfigured.

Complete the following steps to reset your Master AP to factory default settings:

1. Go to **Admin & Services > Administer > Backup & Restore**.
2. Click **Restore to Factory Settings**.
3. Click **OK** to confirm.

   The **Restoring Unleashed to factory settings** progress screen appears. Wait for this progress screen to finish before attempting to login again.
4. Repeat the initial setup and configuration procedures as described in Setting Up an Unleashed Wi-Fi Network on page 131.

FIGURE 382 Restore Factory Settings Progress Screen



Alternate Factory Default Reset Method

If you are unable to complete the software-based resetting of RUCKUS Unleashed to factory default, you can use the following "hard restore" method.

NOTE
Do not disconnect the Master AP from its power source until this procedure is complete.

1. Locate the **Reset** pin hole on the rear panel of the Master AP.
2. Insert a straightened paper clip in the hole and press for at least 6 seconds.

   After the reset is complete, the PWR LED will initially be solid red, indicating bootup is in process. The LED then blinks green, indicating that the system is in the factory default state.

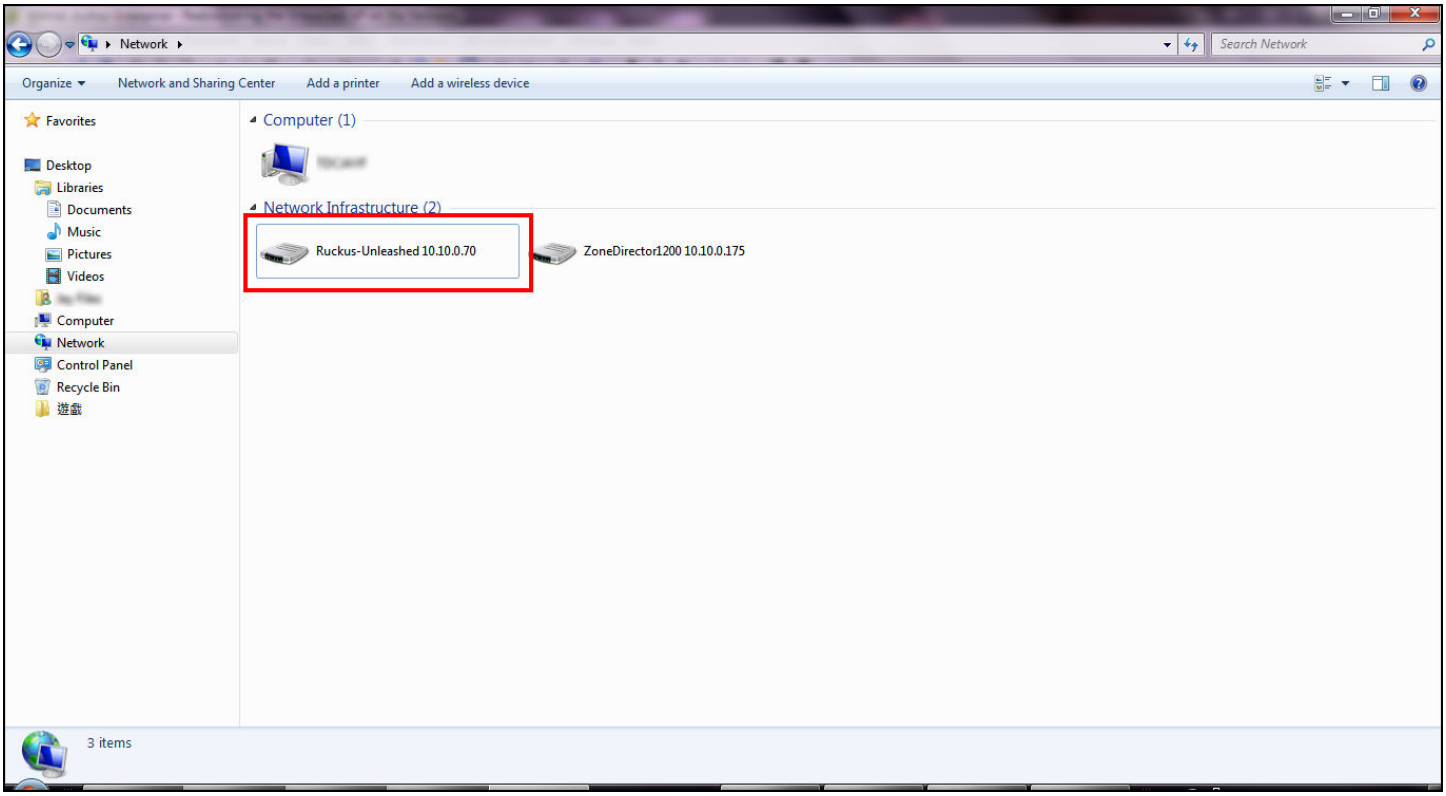
   After you complete the Setup Wizard, the PWR LED will be steady green.

Rediscovering the Unleashed AP on the Network

If you do not know the IP address, you can rediscover an Unleashed AP on the network using UPnP or Bonjour service discovery.

To discover an Unleashed AP using UPnP (Windows clients only), go to the **Network** section of Windows Explorer (**Start > Network** or **Start > Computer > Network**). Locate the Unleashed device in the *Network Infrastructure* section. Double-click the icon to launch the web UI, or right-click and select **View device webpage**, or type the address displayed into your browser's navigation bar.

FIGURE 383 Discovering Unleashed using UPnP in Windows



Additionally, Unleashed also supports Bonjour service discovery. Bonjour discovery allows devices running operating systems other than Windows (such as iOS and Android) to discover the Unleashed Master AP. This allows mobile clients to manage the system using the Unleashed Mobile App in addition to via web browser.

Upgrade

The **Upgrade** page displays the current firmware version and provides an **Upgrade** button which can be used to download the latest firmware and perform an upgrade of the entire Unleashed network.

Unleashed provides two methods of upgrading the firmware:

- Online Upgrade on page 467
- Local Upgrade on page 470

Online Upgrade

Use the online upgrade method to upgrade your RUCKUS Unleashed network with the latest firmware available from the RUCKUS Unleashed firmware server.

Complete the following steps to upgrade the Master AP and all connected member APs using the online upgrade method:

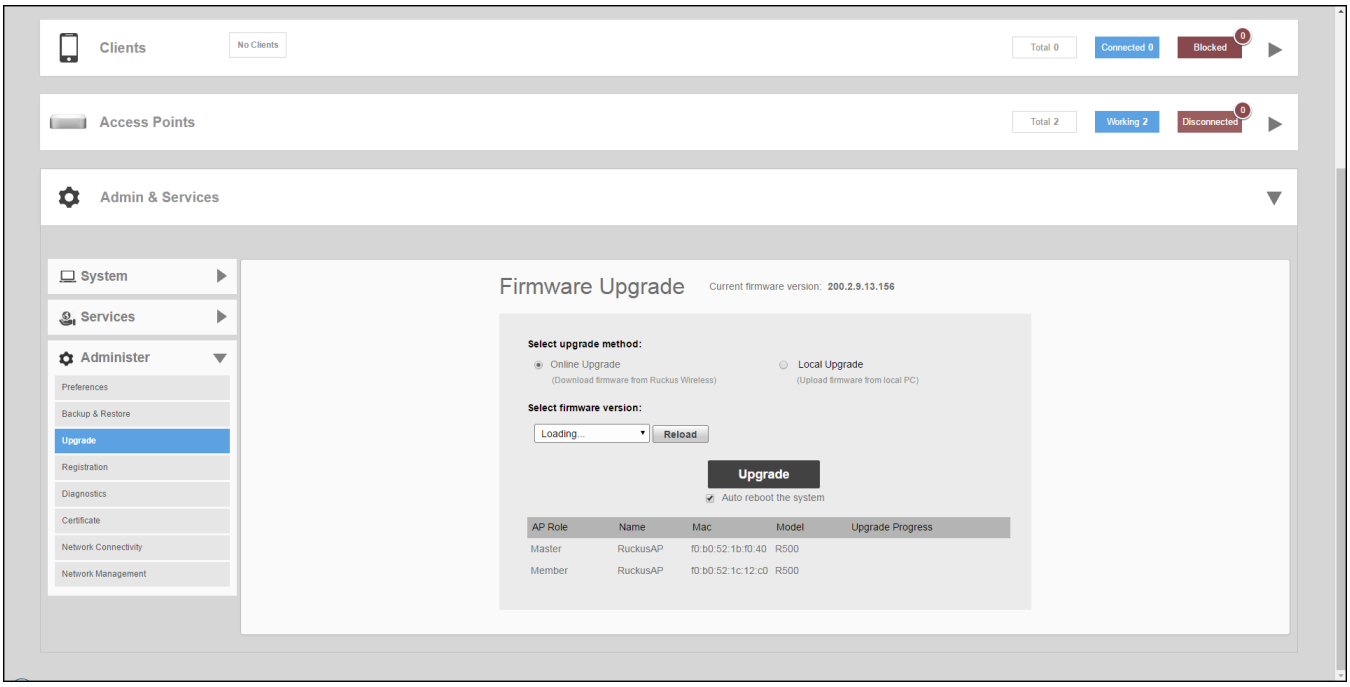
1. Go to **Admin & Services > Administer > Upgrade**.
2. Select **Online Upgrade**.
3. Under **Select Firmware Version**, select one of the available firmware versions.

NOTE
You can rollback to the previous image version and restore the configuration of the previous version. The roll back syncs automatically to all member APs. If the old Master AP reboot fails and a member AP becomes the Master AP, then the new Master AP can still roll back to the previous version with the corresponding configuration.

NOTE
Optionally, select **Auto reboot the system** to automatically reboot each AP after the firmware has been deployed to the AP. By default, this option is enabled. You may want to disable this option if you prefer to wait until all APs have the new firmware before rebooting them all at once. That is, if you have multiple Unleashed AP models that require different firmware image files, you can either select the **Auto reboot the system** option and wait until all the APs have finished downloading the firmware and the entire Unleashed network is automatically rebooted, or you could choose to wait until all the APs have finished downloading the firmware and click **Reboot** to reboot the entire Unleashed network.

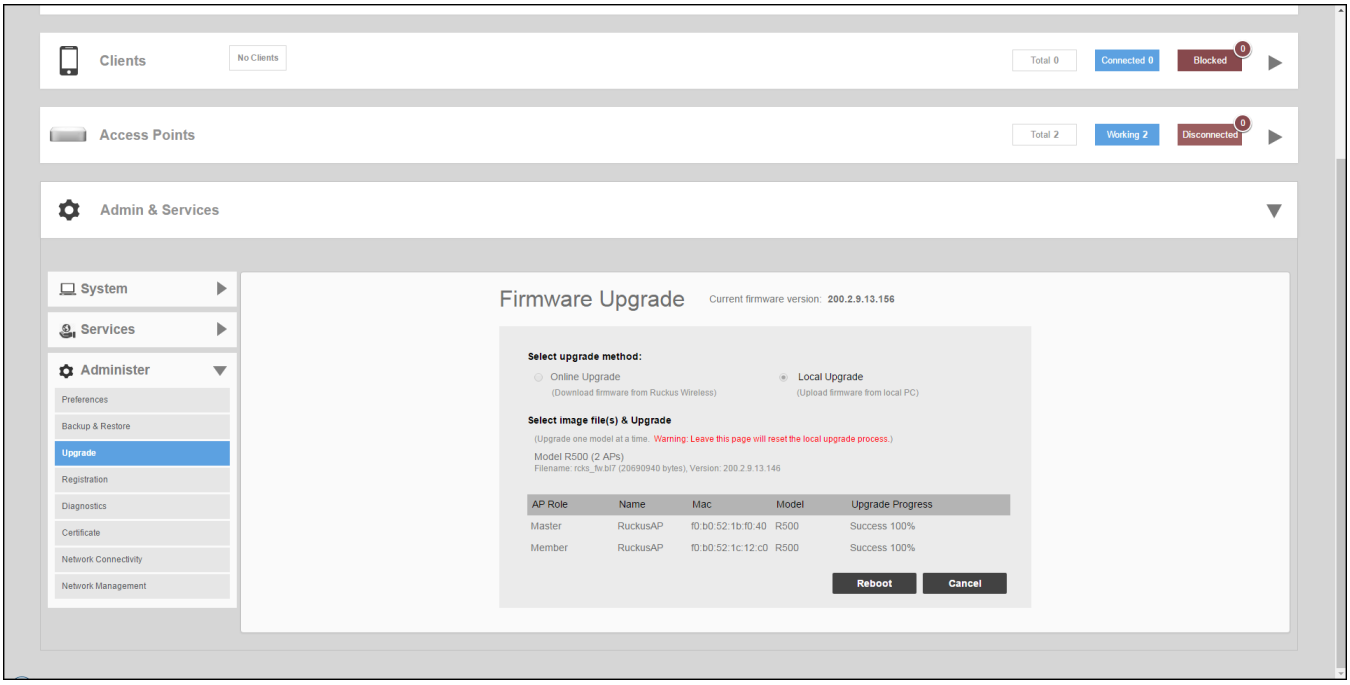
4. Click **Upgrade** to begin upgrading the APs shown in the list.

FIGURE 384 Configuring Online Upgrade



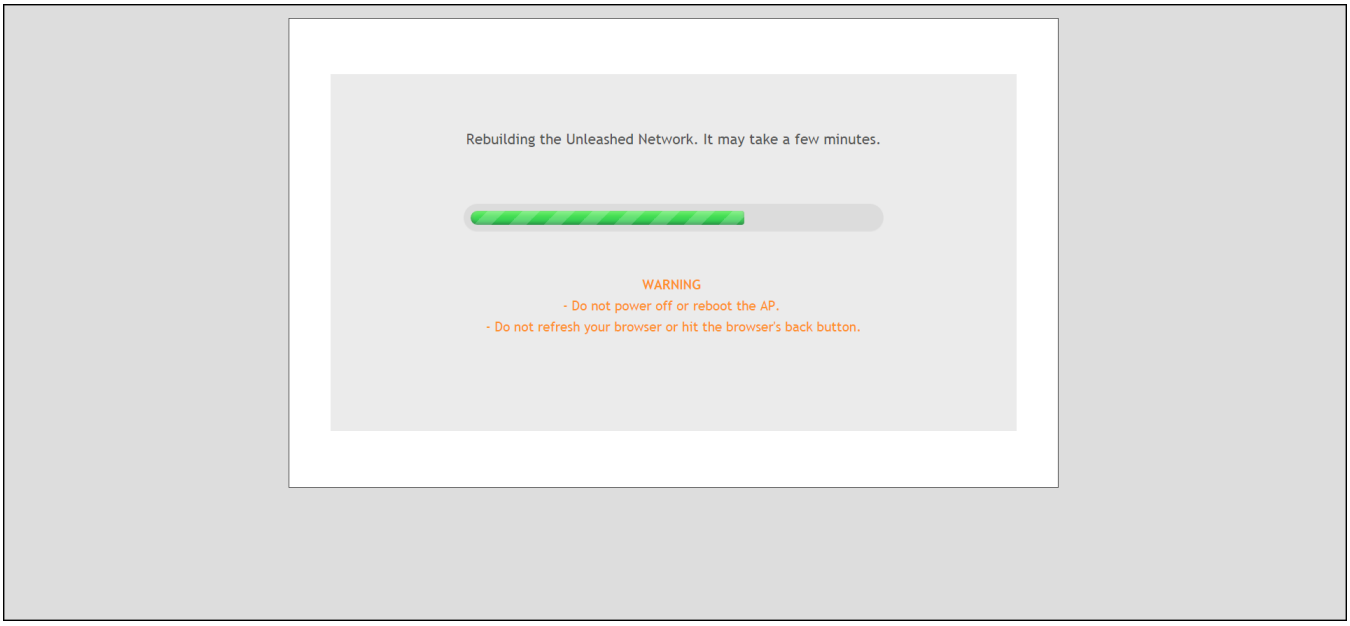
The **Upgrade Progress** column displays the progress for each AP. Once completed, the column will display "Success 100%" next to each AP for which the upgrade was successful.

FIGURE 385 Successful Online Upgrade



5. When all of the APs in the list display "Success 100%" in the **Upgrade Progress** column, click **Reboot**. The **Rebuilding the Unleashed Network** progress screen appears.

FIGURE 386 Rebuilding the Unleashed Network Progress Screen



After the process is completed, you are redirected to the login page.

6. Log in and go to **Admin & Services > System > System Info** to confirm the new software build number.

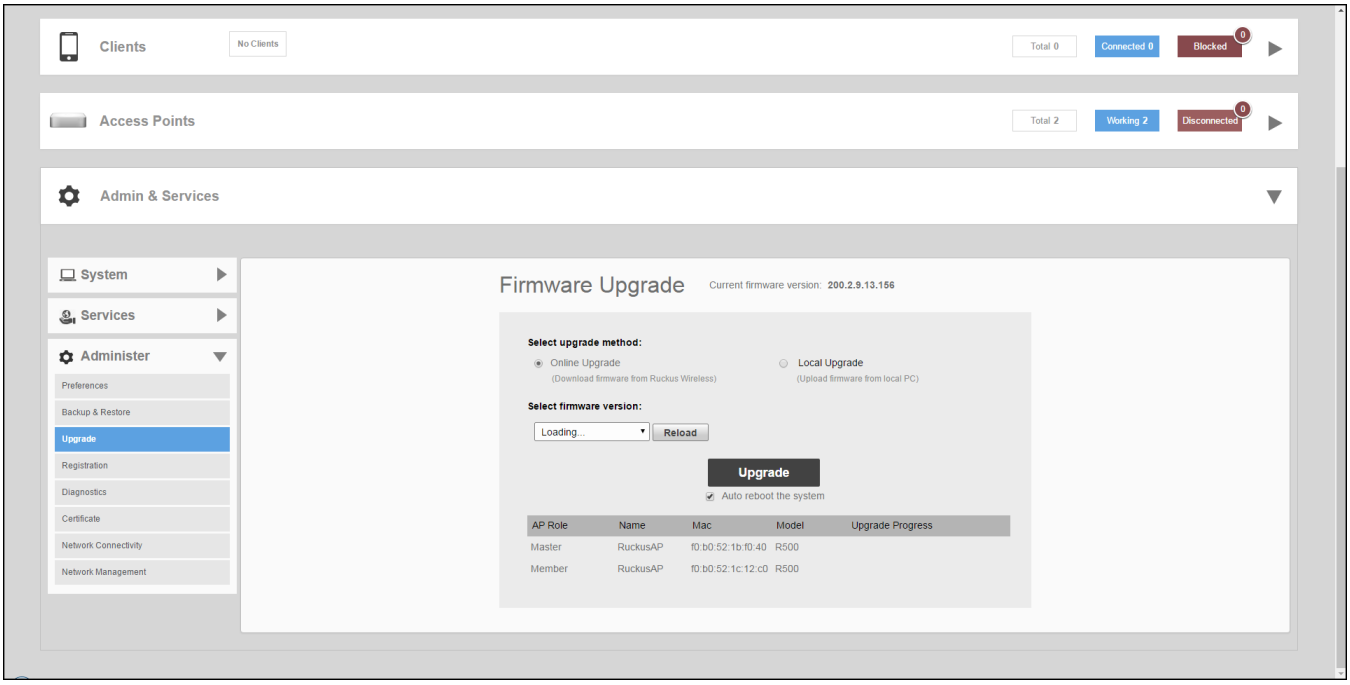
Local Upgrade

Use the Local Upgrade method to upgrade the network using firmware files that you have downloaded from the RUCKUS Support site.

To upgrade the Master AP and all connected member APs using the Local Upgrade method, use the following procedure:

1. Go to **Admin & Services > Administer > Upgrade**.

   FIGURE 387 The Upgrade Page



2. Select **Local Upgrade** as the upgrade method.

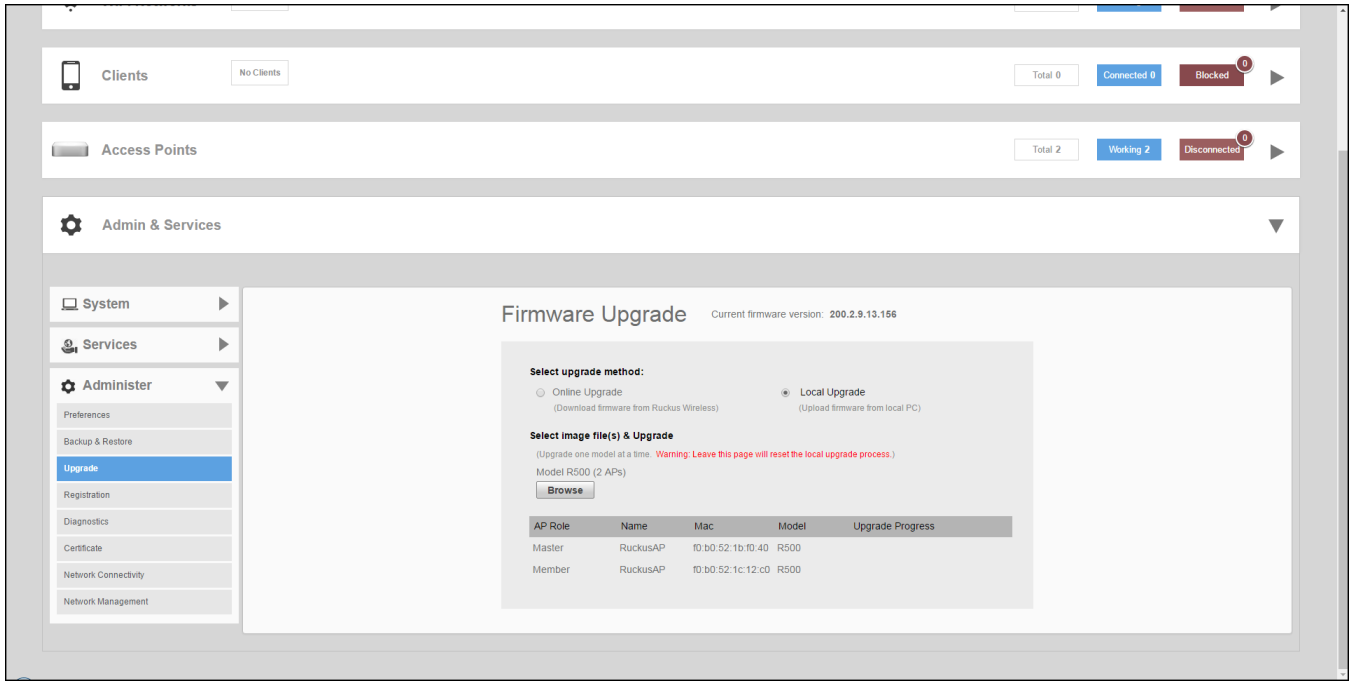
3. Click **Browse** to locate the firmware image file on your local computer.

   RUCKUS Unleashed will perform a check to make sure it is the proper image for the AP model before proceeding.

   NOTE
   Each AP model has a different firmware image file that must be loaded onto the Master and then distributed to all member APs of that model. So, for example, if you have a mix of RUCKUS Unleashed R510 and R610 APs, you could upgrade all of the R510s first and then the R610s, or the other way around, but you cannot upgrade both models at once.

   NOTE
   While the upgrade process will check to make sure you do not try to upgrade an RUCKUS Unleashed AP with the incorrect model firmware, there is no check to ensure that you do not upgrade/downgrade an RUCKUS Unleashed AP to a RUCKUS Solo AP (standalone) firmware image. If you do this, the AP will no longer function as an RUCKUS Unleashed AP until RUCKUS Unleashed firmware is re-loaded onto it.

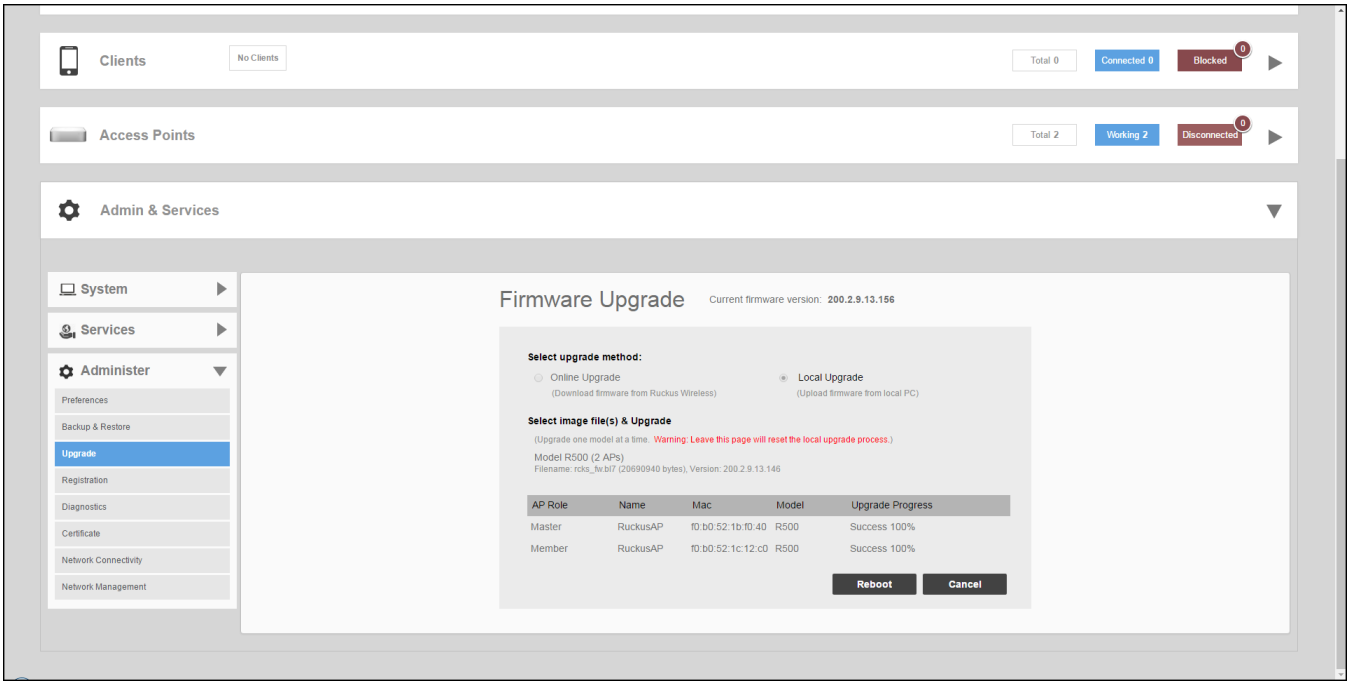
FIGURE 388 Local Upgrade



4. Click **Upgrade** to begin upgrading the APs shown in the list.

5. The **Upgrade Progress** column displays the progress for each AP. Once completed, the column will display "**Success 100%**" next to each AP for which the upgrade was successful.

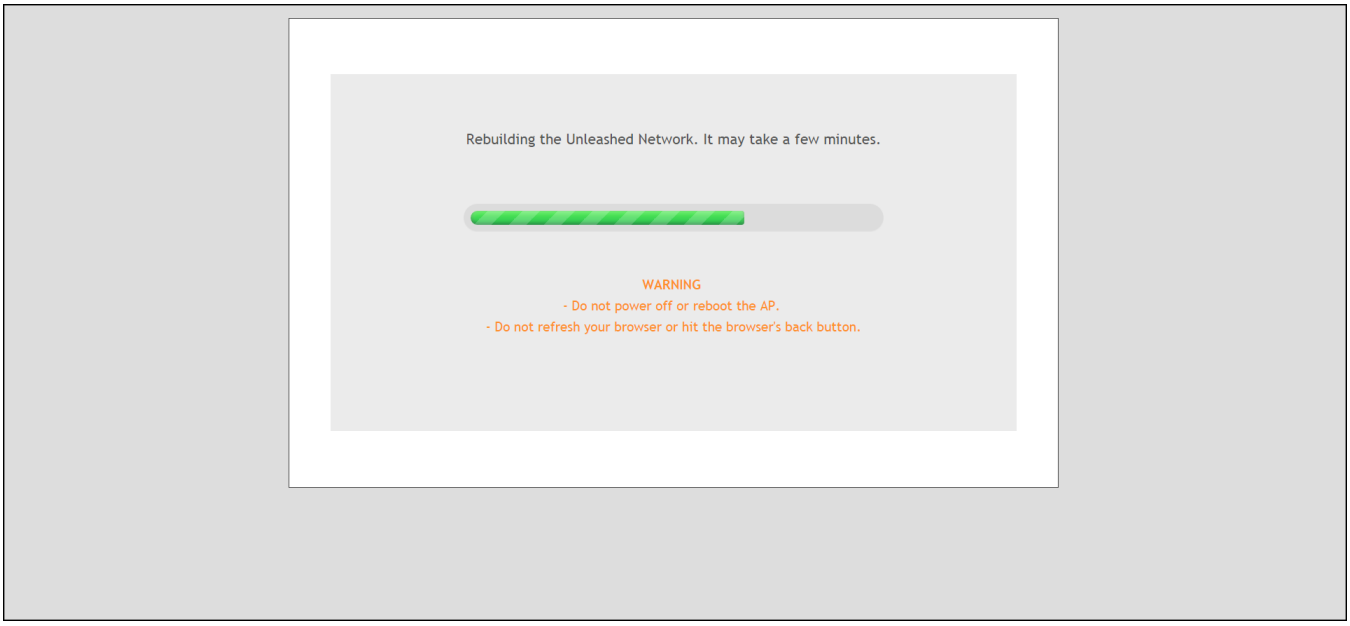
   FIGURE 389 Upgrade successful, click Reboot to reboot the APs and apply the new firmware



6. Repeat steps 3-5 for any additional AP models.

7. When all of the APs in the list are displayed as "**Success 100%**" in the **Upgrade Progress** column, click **Reboot**. A "**Rebuilding the Network**" progress screen appears. Wait until the process completes.

   FIGURE 390 "Rebuilding the Network" Progress Screen

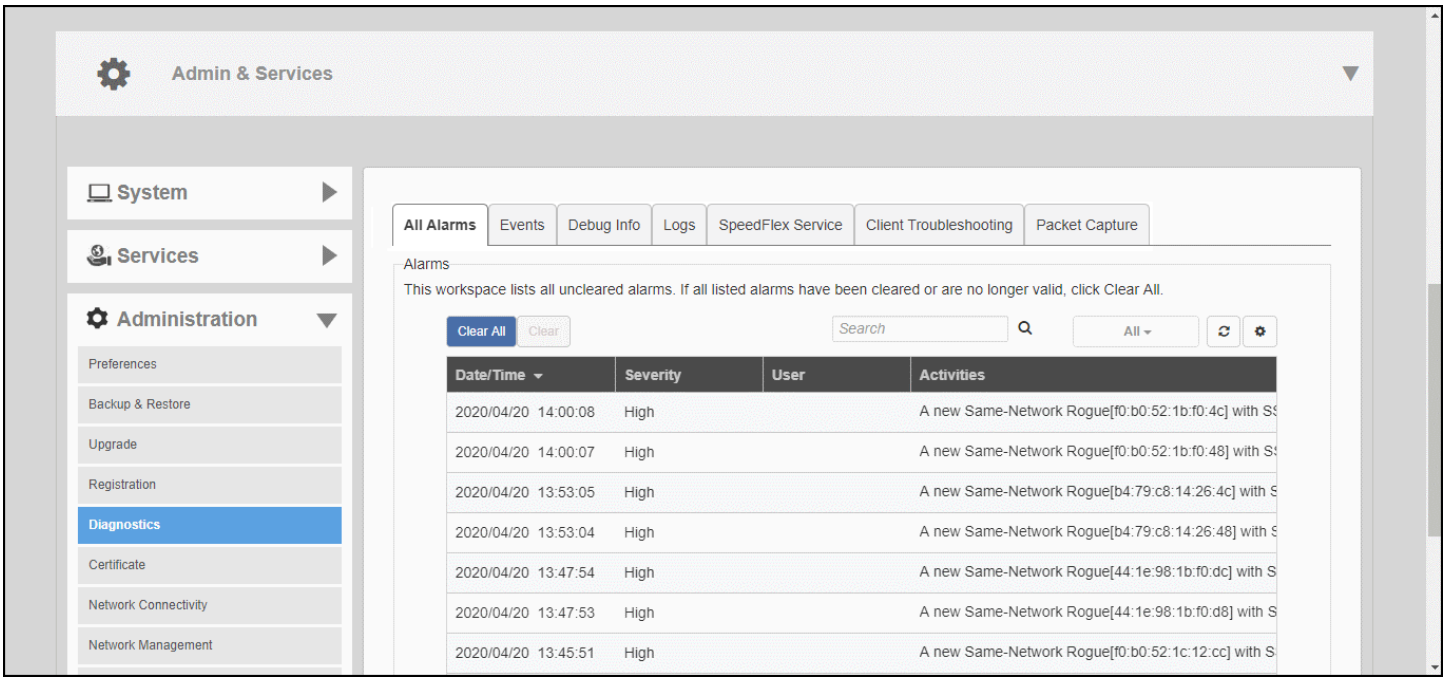


8. Once complete, you will be redirected to the login page.
9. Log in and go to **Admin & Services > System > System Info** to confirm the new software build number.

Diagnostics

The *Diagnostics* pages provide options for troubleshooting and diagnostics, including configuration settings for alarms, viewing system event log messages, configuring which debug information is to be collected in log files, and saving the current logs to your local computer.

FIGURE 391 Configuring Diagnostics Options



Viewing Alarms

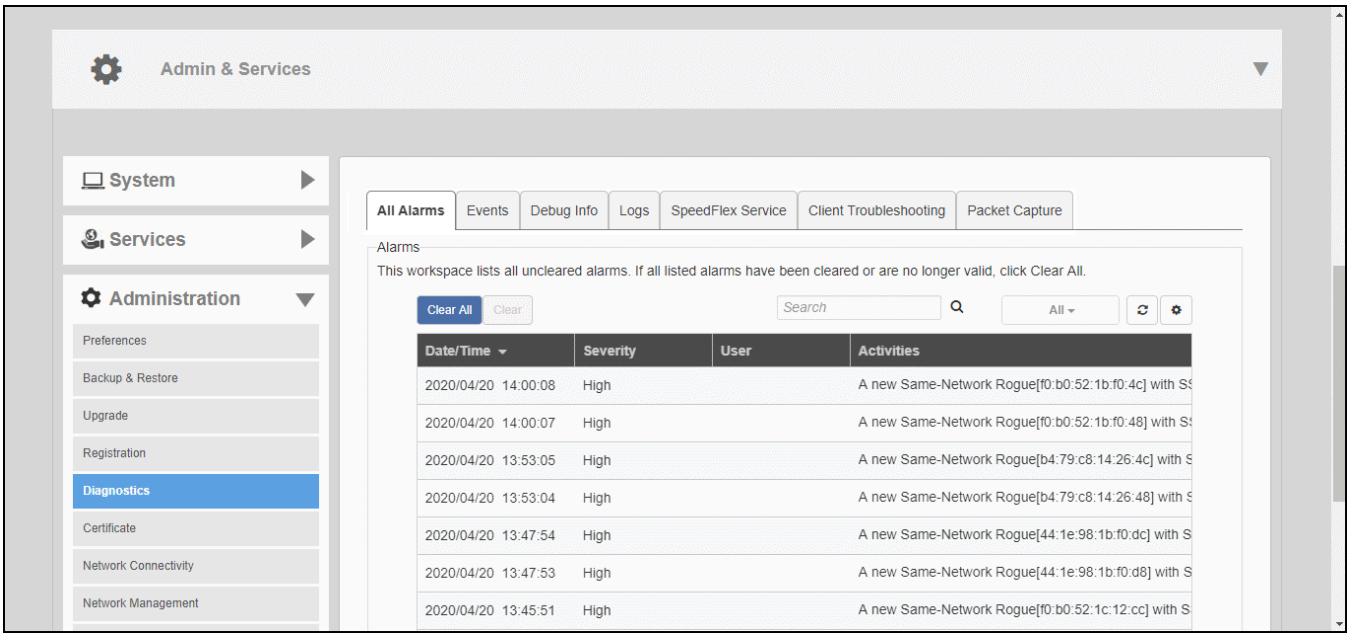
The *All Alarms* page displays a list of all recent alarms. Alarms include important events such as when an AP loses contact with the Master AP, a rogue AP is detected, an authentication server becomes unreachable, or when a Master/Member role change is detected.

To view and clear recent alarm messages:

1. Go to **Admin & Services > Administration > Diagnostics > All Alarms**.
2. To delete an alarm event from the list, select it and click **Clear**.

3. Click **Clear All** to clear all alarm events from the list.

FIGURE 392 Viewing a List of Alarm Event Messages



Viewing System Event Messages

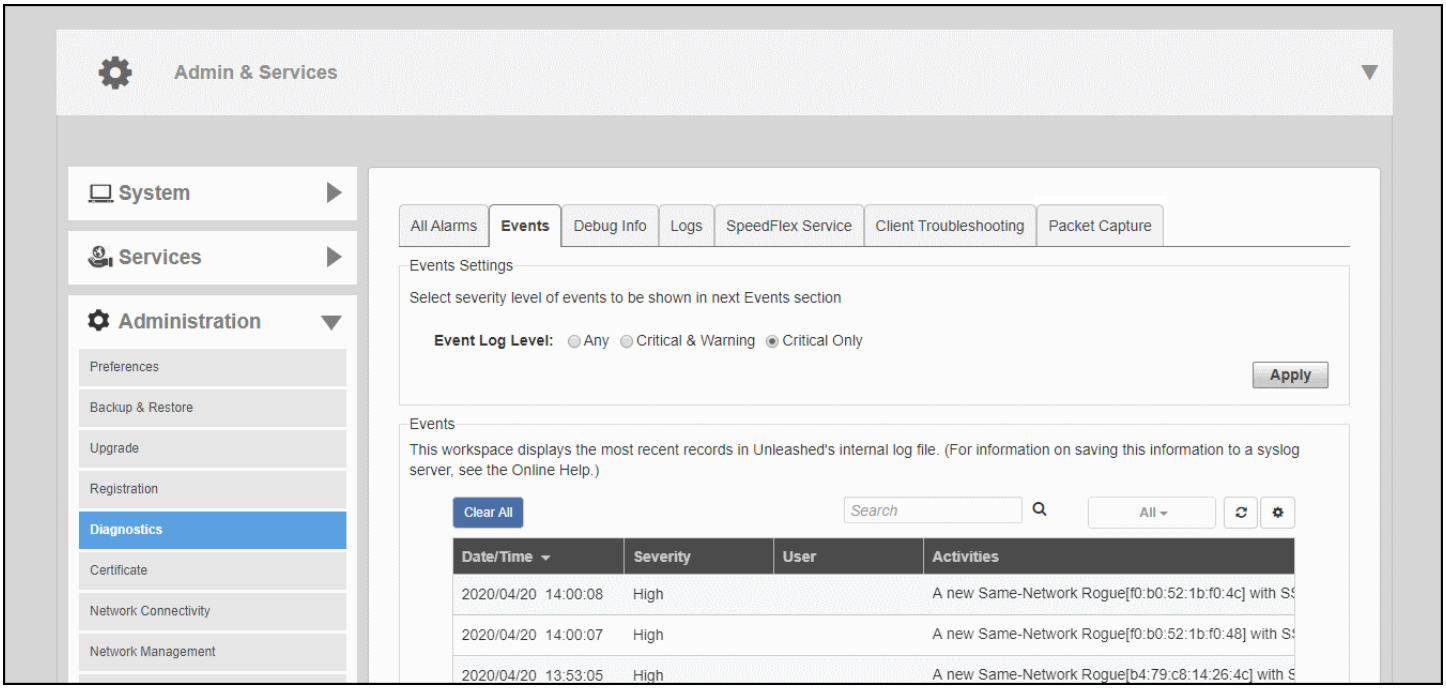
The **Diagnostics > Events** page displays the most recent records in the Master AP's internal log file.

Compared to Alarms, Event messages include less critical messages - such as when an AP changes channel, a configuration sync is performed, a new client joins the network, etc.

You can customize the level of events to display in the Events list using the **Event Log Level** setting, as follows:

- **Any**: All event log levels will be displayed.
- **Critical & Warning**: Only events whose log level is "critical" or "warning" level appear.
- **Critical Only**: Only events whose log level is "critical" will appear.

FIGURE 393 The Events Page



Configuring Debug Logs

You can use the **Diagnostics > Debug Info** page to configure which debug components to include in log files and on the **Events** page.

NOTE
Check the box **Debug log per APs or clients MAC address** and enter AP/Client info to filter debug output for a specific AP or client.

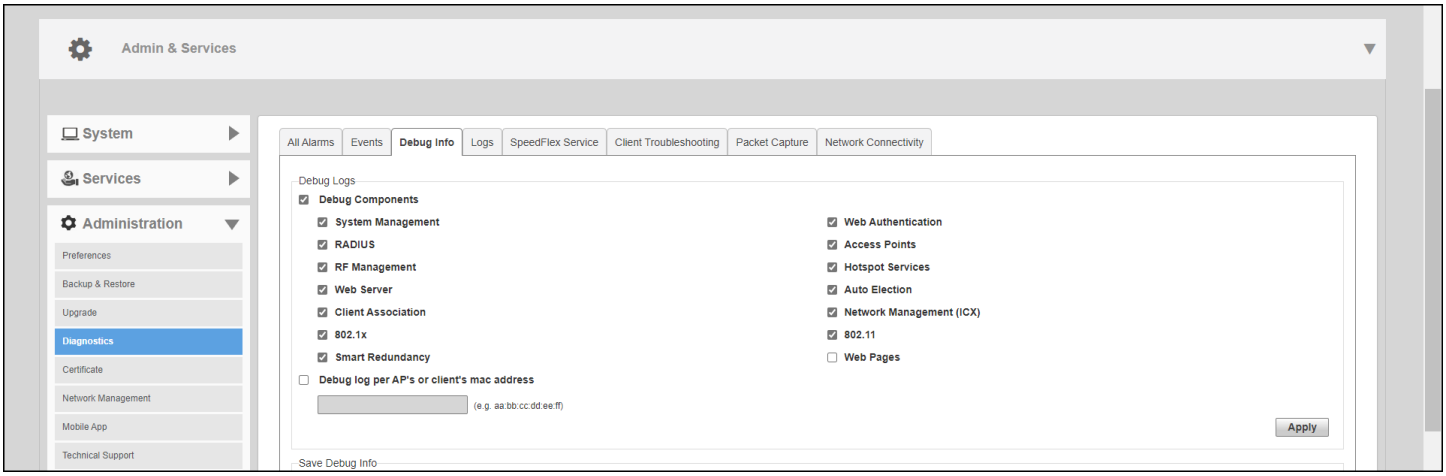
You can also save the log files using the **Save Debug Info** button. If you request assistance from RUCKUS technical support, you may be asked to supply detailed debug information from RUCKUS Unleashed.

Click the **Save Debug Info** button, and then save the file to your computer. You can then email this file to RUCKUS Support to assist with troubleshooting.

NOTE
The Master AP's log files also contain all of the member APs' support info.

You can also allow the Master AP to automatically save log files to a specified FTP or TFTP server in the event of a controller process failure. By default, this feature is disabled. When enabled, the Master will send the core, dump, and debug files to an FTP/TFTP server before restart. This information can be very useful in debugging controller reboot issues. To enable this feature, select the check box next to **Enable upload debug logs to remote server**, select **FTP** or **TFTP**, and enter the server address only (for TFTP) or **Host**, **Port**, **Username** and **Password** (for FTP).

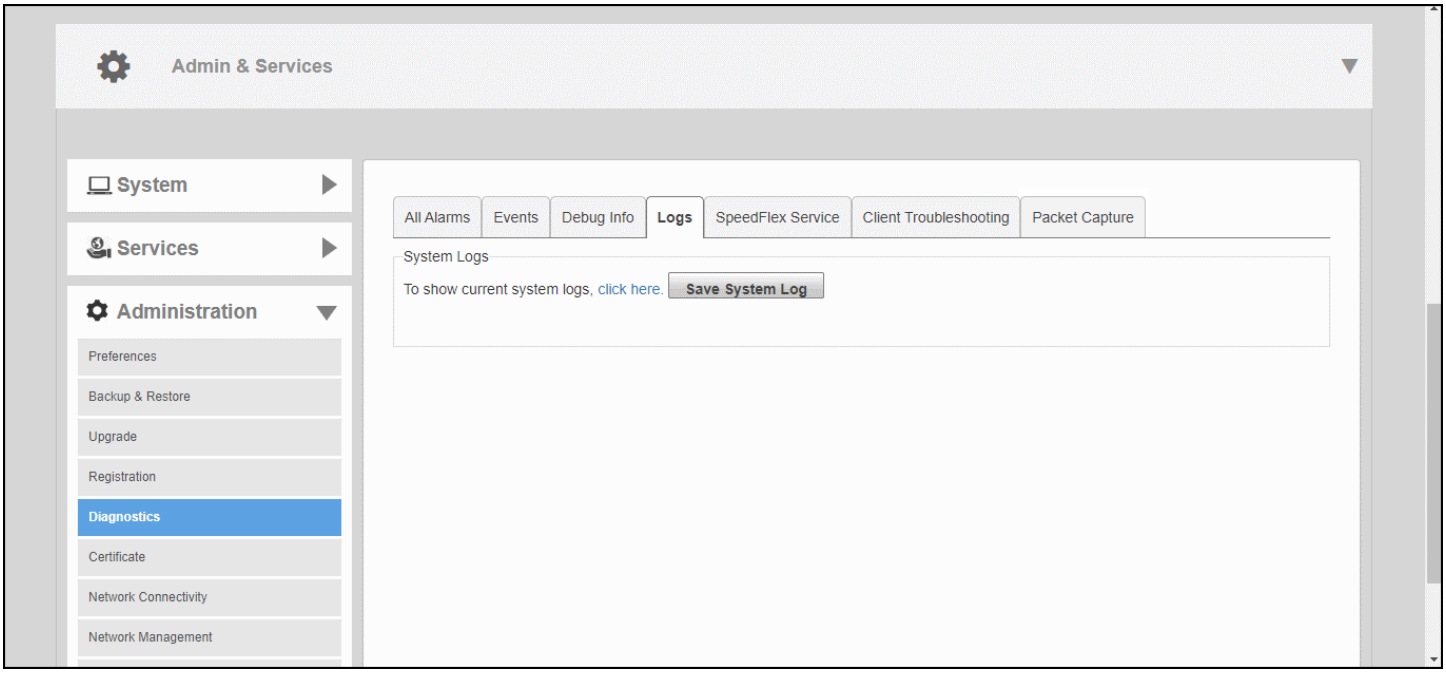
FIGURE 394 The Debug Info Page



Saving System Logs to Your Computer

The **Logs** tab provides an option to view the current system logs of the AP. Click **Save System Log** to save the current log file as a .tar file to a local computer.

FIGURE 395 Logs Tab



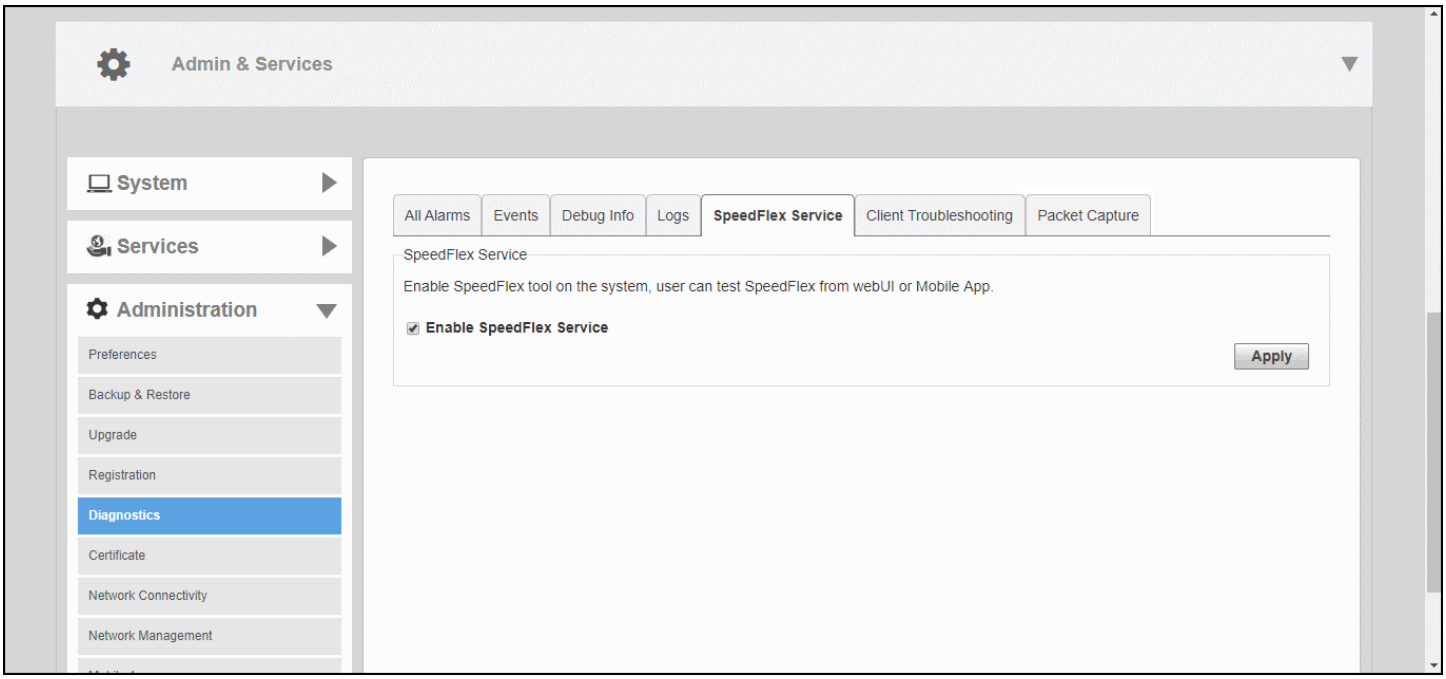
SpeedFlex Service

SpeedFlex service (enabled by default) can be disabled to prevent mobile or web clients from performing a SpeedFlex performance test.

For more information on the SpeedFlex performance testing tool, see Running a SpeedFlex Performance Test on a Wireless Client on page 357.

To disable SpeedFlex, clear the **Enable SpeedFlex Service** option and click **Apply**.

FIGURE 396 Enabling or Disabling SpeedFlex Service



Client Connection Troubleshooting

The client connectivity trace feature is designed to help customers diagnose wireless client connection issues to determine why a client fails to connect to the wireless network.

To perform a client connectivity trace:

1. Open the **Clients** section, and select the problematic client from the list.

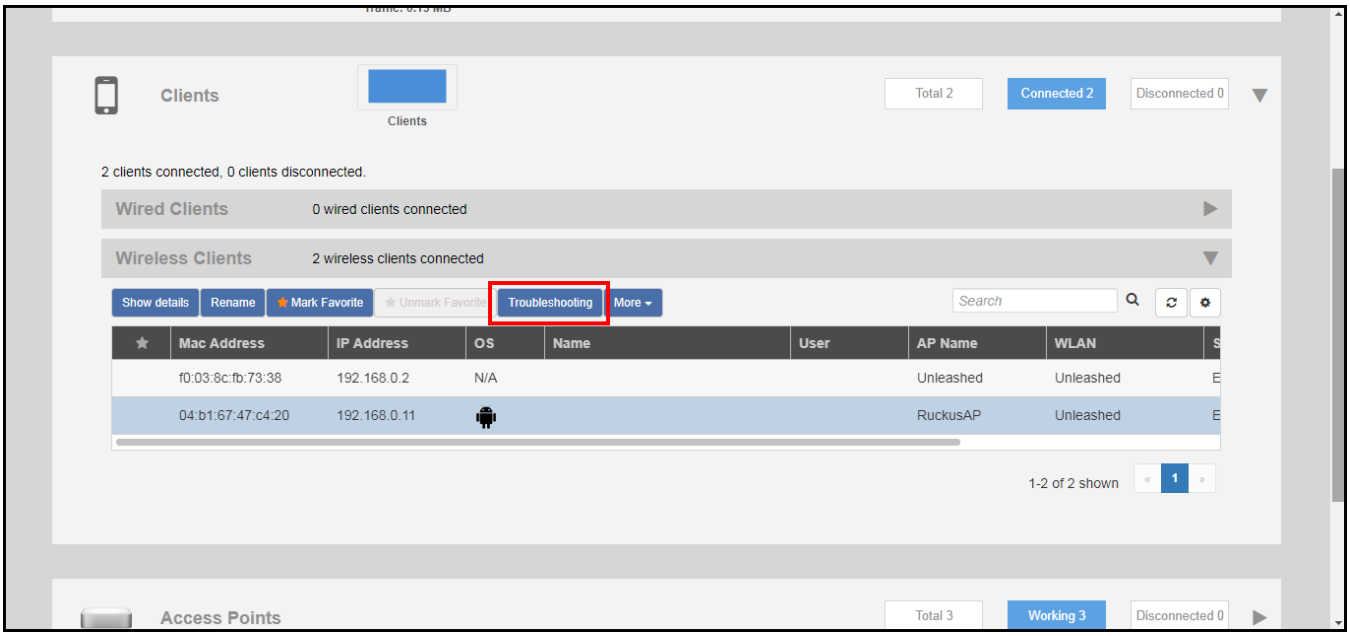
   NOTE
   Alternatively, go to **Admin & Services > Administration > Diagnostics > Client Troubleshooting**, and locate the **Client Connection Logs** section.

   NOTE
   As of release 200.8, client connection traces can be performed on clients connected to the following WLAN types:

   - WPA2
   - Web Auth
   - Hotspot
   - Guest Access

2. Click **Troubleshooting**.

FIGURE 397 Click Troubleshooting to perform client connectivity trace



The *Troubleshooting* screen appears.

3. In *Connectivity Trace*, click the **Start** button to begin. The association trace begins. The page refreshes to display detailed results.

FIGURE 398 Click Start to begin connectivity trace

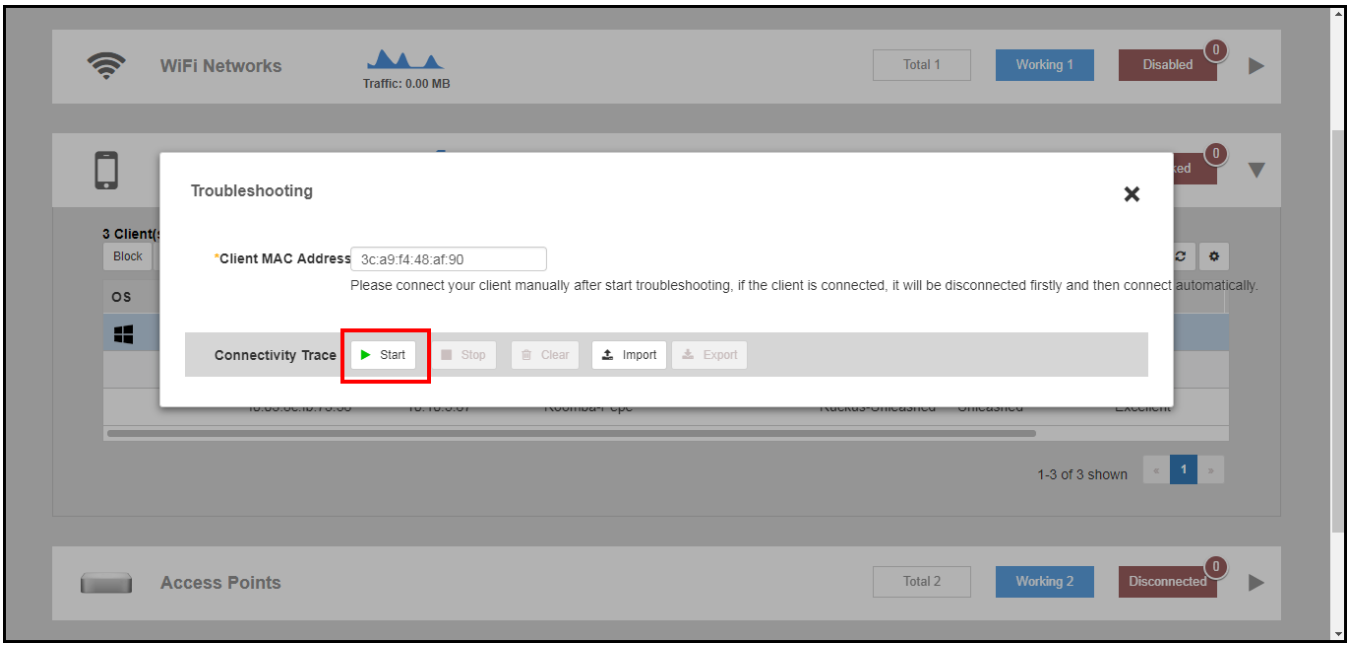
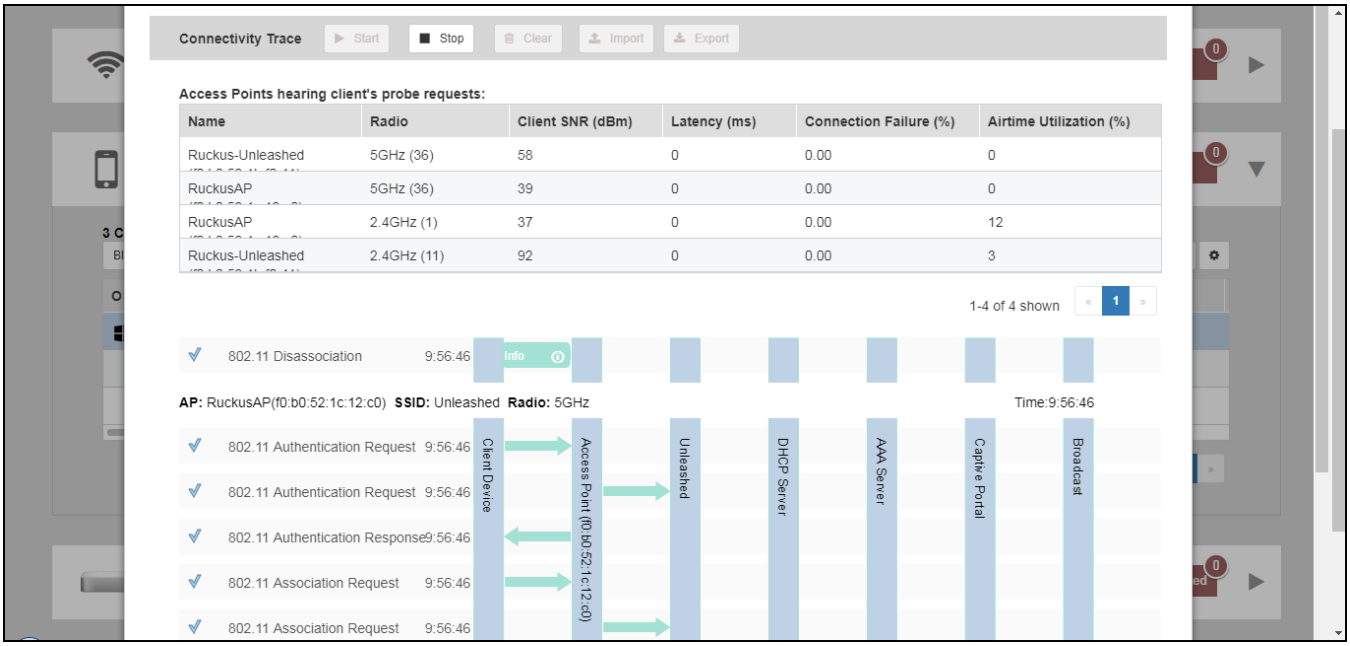


FIGURE 399 Connectivity trace in progress



4. Examine the results to isolate the problematic step in the process.
5. If needed, you can download the client connectivity data to a file, which can later be imported for analysis. Click **Export** to download the data file and save it to your local computer. Click **Import** to import a previously exported file back into Unleashed.

Saving Client Connection Logs

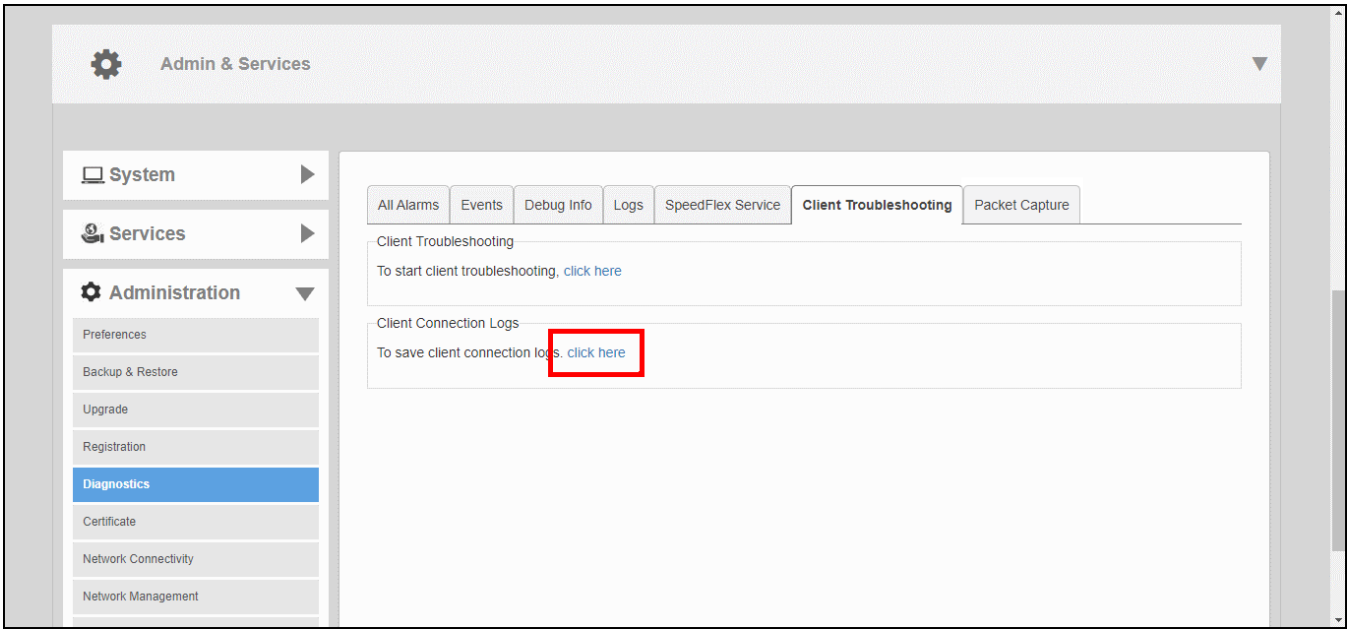
Saving client connection logs may be helpful in troubleshooting client connectivity issues.

RUCKUS Unleashed provides two options for saving client connection logs - download the current log file immediately from the web interface, or configure RUCKUS Unleashed to send the logs to a syslog server automatically. For information on delivering logs to syslog, see *Customizing the Current Log Settings*.

To download and save current client connection logs:

1. Go to **Admin & Services** > **Administration** > **Diagnostics** > **Client Troubleshooting**, and locate the *Client Connection Logs* section.
2. In "*To save client connection logs. click here*," click the **click here** link.
3. Save the file to your local computer.

FIGURE 400 Saving Client Connection Logs to a Local Computer



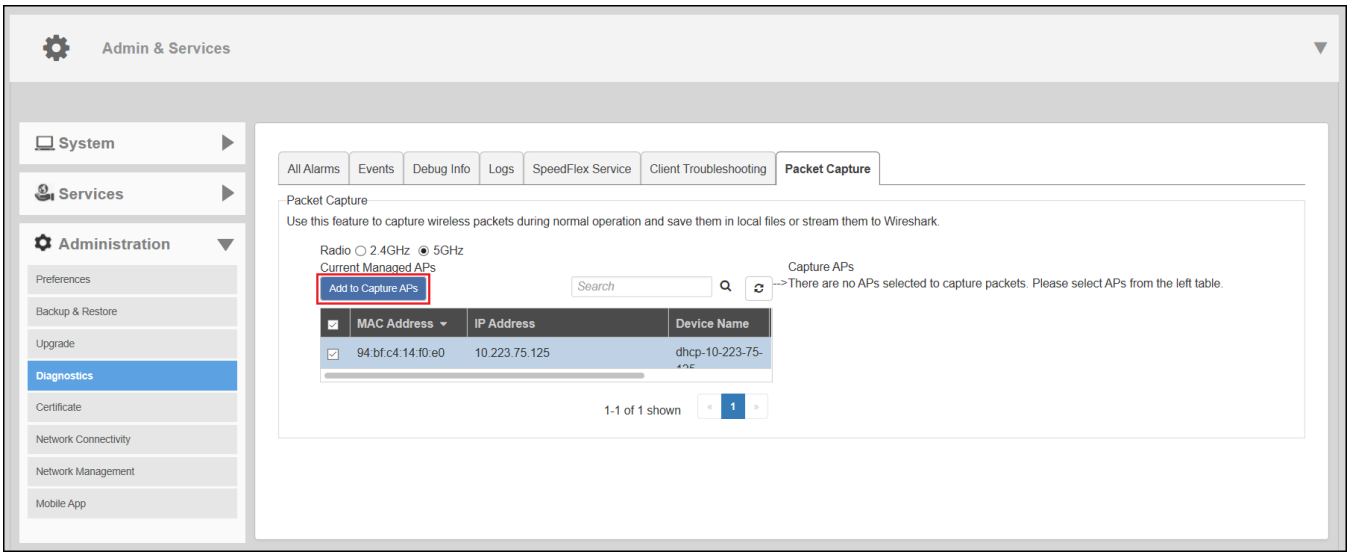
Capturing Remote Packets

Remote packet capture puts one or more APs into packet sniffer mode, allowing them to capture the wireless packets. The packets are either saved to local files or streamed to packet inspection program such as Wireshark for later analysis.

1. Go to **Admin & Services** > **Administration** > **Diagnostics** > **Packet Capture**.
2. For **Radio**, select **2.4 GHz** or **5 GHz**.

3. Under **Currently Managed APs**, select APs from the list and click **Add to Capture APs**.

FIGURE 401 Adding Currently Managed APs to Capture APs

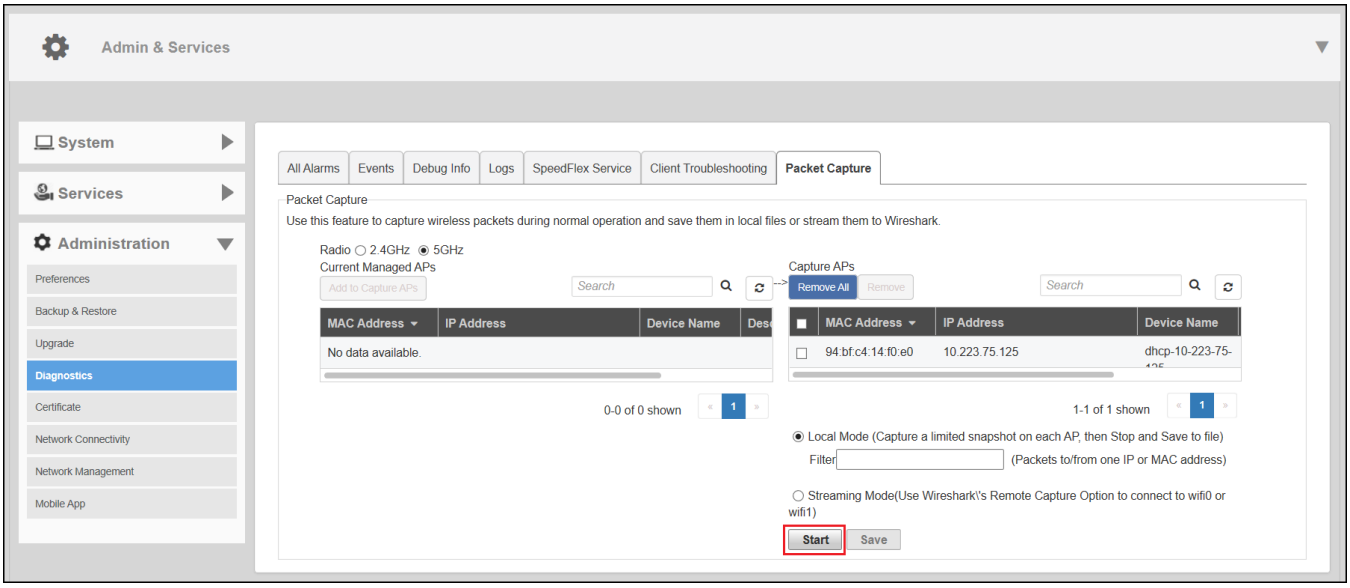


The selected currently managed APs are moved to the **Capture APs** table.

4. Select **Local Mode** or **Streaming Mode** as the capture mode.
   - To capture a limited snapshot on each AP, select **Local Mode**.
     a. Click **Start** to begin capturing packets.
     b. Click **Stop** to end the capture.
     c. Click **Save** to save the packet capture to a local file.
   - To stream the captured packets to Wireshark, select **Streaming Mode**.
     a. Click **Start** to launch Wireshark.
     b. Select **Capture Options**. Under **Capture: Interface**, select **Remote**. A **Remote Interface** dialog box is displayed.
     c. Under **Host**, enter the IP address of the AP you want to view. Leave the **Port** field empty and click **OK**.

        The remote host interface list on the right side is updated.
     d. Select **wifi0** or **wifi1** from the list, depending on whether you are streaming on the 2.4-GHz or 5-GHz radio.

FIGURE 402 Selecting the Capture Mode



Working with SSL Certificates

SSL certificates enable device or user identification, as well as secure communications.

Unleashed captive portal services and the web UI use an SSL certificate when establishing HTTPS connections.

The default SSL certificate that is installed on the Unleashed AP is self-signed and therefore not trusted by any web browser. This is the reason why the SSL security warnings appear when establishing an HTTPS connection to the Unleashed web interface.

To eliminate the security warnings, administrators may purchase a trusted SSL certificate from a public Certificate Authority (CA) and install it on the Unleashed Master AP.

The basic certificate installation process is as follows:

1. Generate a Certificate Signing Request (CSR) with the required requester information.
2. Submit the CSR to a public CA for signing.

3. Receive a signed certificate from the CA.
4. Import the signed certificate into Unleashed.

Generating a Certificate Signing Request

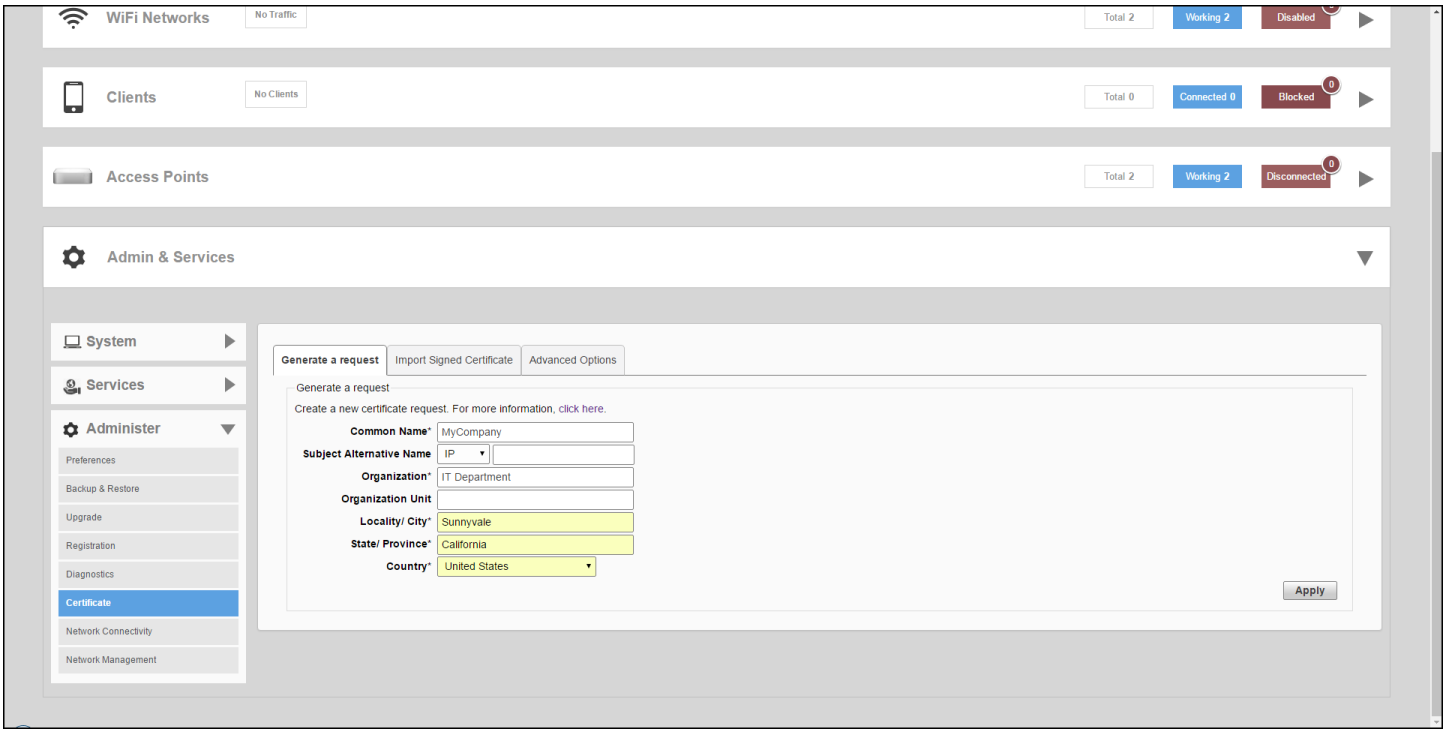
If you do not have an existing SSL certificate, you will need to create a certificate signing request (CSR) file and send it to a certificate authority (CA) to purchase an SSL certificate.

The Unleashed web interface provides a form that you can use to create the CSR file. Fields with an asterisk (*) are required entries. Those without an asterisk are optional.

The **Admin & Services > Administer > Certificate** pages allow you to perform the following actions:

- Generate a certificate signing request.
- Import a signed certificate.
- View the currently installed certificate.
- Advanced Options link displays additional options
- Restore the default private key and certificate.
- Backup private key and certificate.
- Generate a new private key.

FIGURE 403 SSL certificate screens



Creating a Certificate Request File

To create a certificate request file (CSR):

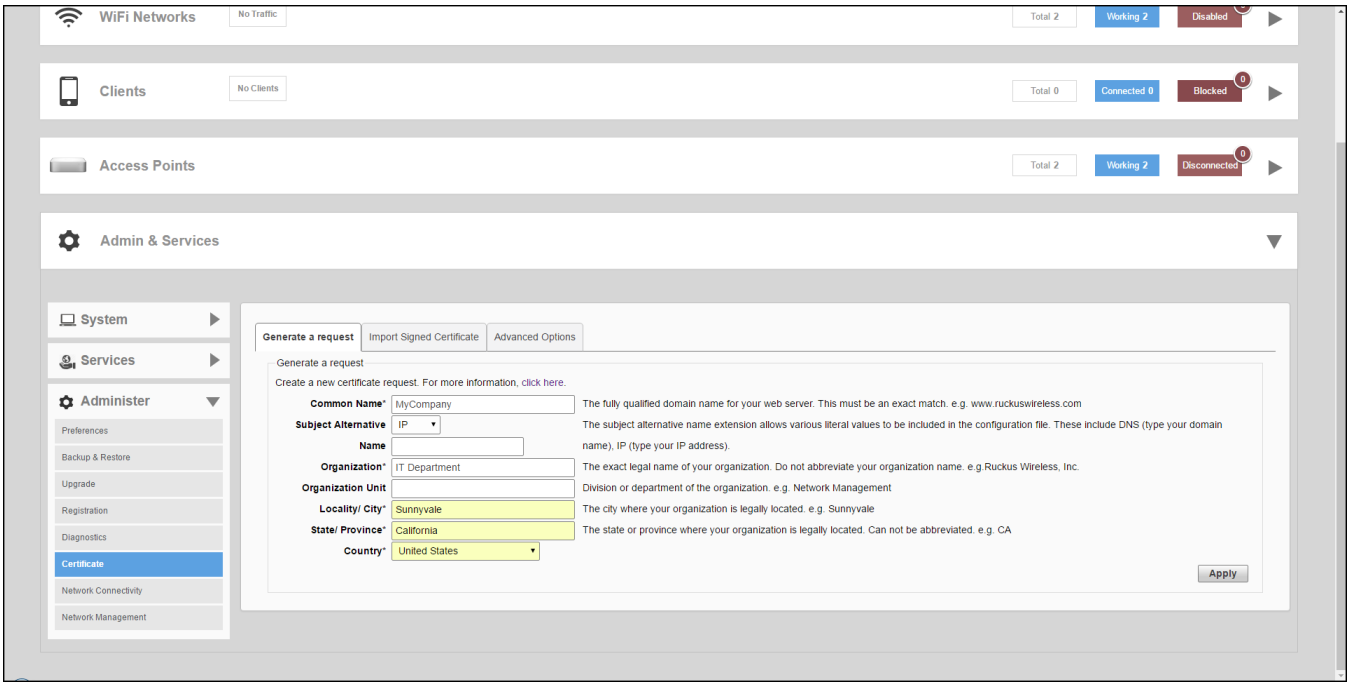
1. Go to **Admin & Services > Administer > Certificate**.
2. In the **Generate a Request** form, complete the following options:
   - **Common Name***: Enter your company's Fully Qualified Domain Name (FQDN). Typically, this will be "unleashed.[your company].com". You can also enter the Master AP's IP address (e.g., "192.168.0.2"), or a familiar name by which the web UI will be accessed in your browser (e.g., by device name such as "unleashed").

     NOTE
     RUCKUS recommends using the FQDN as the Common Name if possible. If your network does not have a DNS server, you may use the Master AP's IP address instead. However, note that some CA's may not allow this.

     - If you wish to access the web UI from a public network via the internet you must use a Fully Qualified Domain Name (FQDN).
     - In all cases when using a familiar name there must be an appropriate private or public DNS entry to resolve the familiar name to the AP's IP address.
     - If you use a familiar name, this name will be shown in the browser's URL whenever accessing the web interfaces (i.e., administrator interface, standard captive portal and guest access captive portal).
   - **Subject Alternative Name**: (Optional) Select either IP or DNS from the menu and enter either alternative IP addresses or alternate DNS names.
   - **Organization***: Type the complete legal name of your organization. Do not abbreviate your organization name.
   - **Organization Unit**: Division or department of the organization (for example, Network Management).
   - **Locality/City***: Type the city where your organization is legally located (for example, Sunnyvale).
   - **State/Province***: Type the state or province where your organization is legally located (for example, California). Do not abbreviate the state or province name.
   - **Country***: Select your country or region from the pull-down menu.
3. Click **Apply**. A dialog box appears and prompts you to save the CSR file (myreq.csr) that you have just created.

4. Save the file to your computer.

FIGURE 404 Generating a CSR File



5. Go to a certificate authority's web site and follow the instructions for purchasing an SSL certificate.
6. When you are prompted for the certificate signing request, copy and paste the content of the text file that you saved to your local computer, and then complete the certificate purchase.

   After the certificate authority approves your CSR, you will receive the SSL certificate via email. The following is an example of a signed certificate that you will receive from a certificate authority:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0B
AQUFADCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJ
bmMuMR8wHQYDVQQLBgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6
Ly9vY3NwLnZlcmlzaWduLmNvbTBDBggrBgEFBQcwAoY3aHR0cDovL1NW
UlNlY3VyZS1haWEudmVyaXNpZ24uY29tL1NWUlNlY3VyZTIwMDUtYWlh
LmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9naWYw
ITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodHRw
Oi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcN
AQEFBQADggEBAI/S2dmm/kgPeVAlsIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMnoc3DMyDjx0SrI9lkPsn223CV
3UVBZo385g1T4iKwXgcQ7WF6QcUYOE6HK+4ZGcHermFf3fv3C1-
FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//
0pykSldW/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
YC4gwH3BuB9wqpRjUahTiK1V1-
ju9bHB+bFkMWIIMIXc1Js62JClWzwFgaGUS2DLE8xICQ3wU1ez8RUPGn
wSxAYtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----END CERTIFICATE-----
```

7. Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You may now import the signed certificate into RUCKUS Unleashed. Refer to Importing an SSL Certificate on page 487 for instructions.

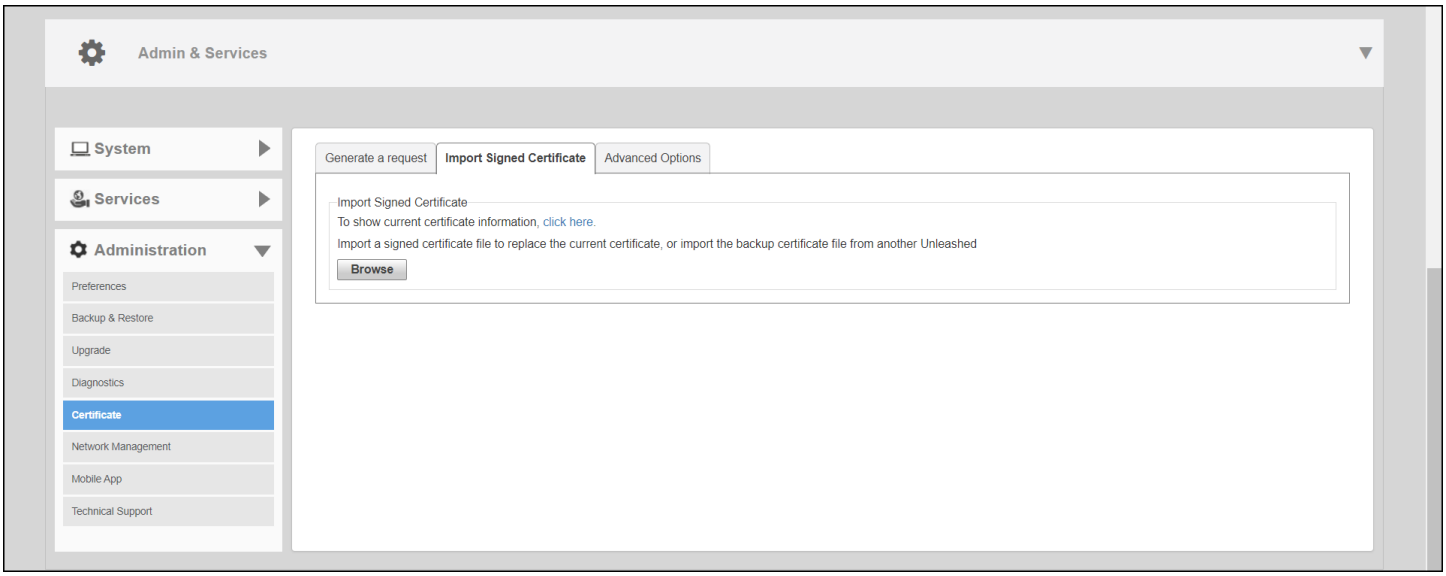
Importing an SSL Certificate

After you receive the signed certificate from the certificate authority, you must import it into RUCKUS Unleashed.

Complete the following steps to import a signed certificate.

1. Click the **Browse** button and select the file that contains the certificate (in PEM, CRT, or CER format) to upload it.

FIGURE 405 Import Signed Certificate Tab



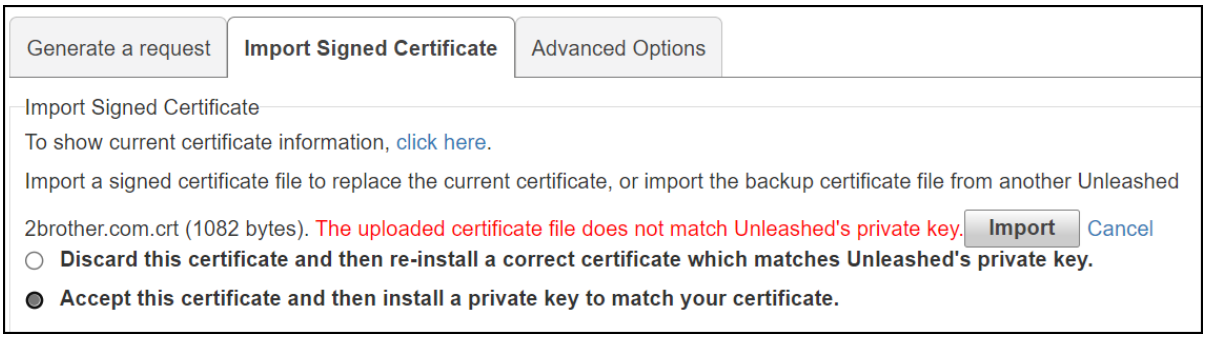
2. If there are no intermediate CA certificates, click the **Import** button to install the uploaded certificate.

NOTE
If the certificate does not match the currently installed private key, you are prompted to upload the correct private key.

NOTE
Beginning with Unleashed 200.13, the Elliptic Curve Cryptography (ECC) certificate is supported. The recommended encryption algorithm is Prime256v1.

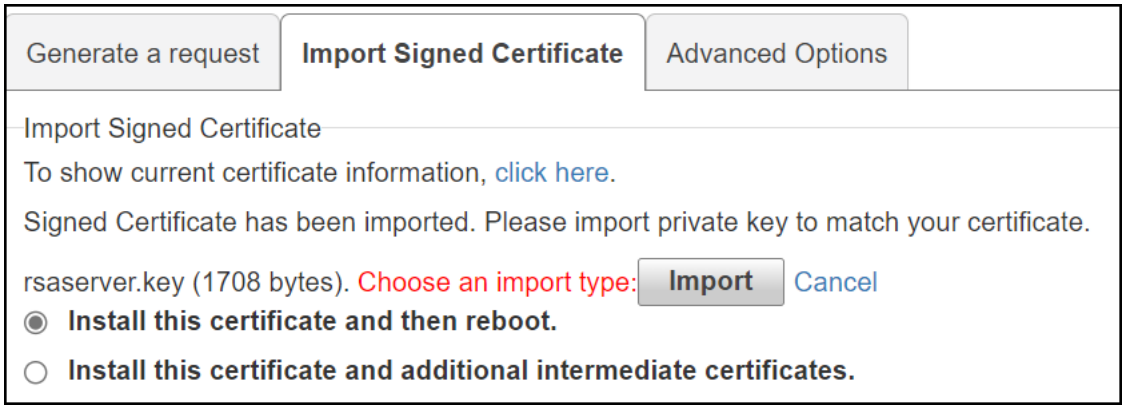
NOTE
Currently, the dual-certificate mode is not supported on an Unleashed AP. If an Elliptic Curve Cryptography certificate is used, the browser of the earlier version may fail to log in to the Unleashed web interface.

FIGURE 406 Installing a Private Key



3. If the certificate was issued by an intermediate CA, you must also import the intermediate CA certificate (as well as all other intermediate CA certificates in the path to the root CA). In this event, you would receive intermediate CA certificate download instructions from the certificate vendor. Complete the following steps to import an intermediate CA certificate.
   a) After selecting the end certificate, click the intermediate certificate import option.
   b) Click the **Import** button to display the **Import Intermediate Certificates** form.
   c) Click the **Browse** button and select the file containing the intermediate certificate (PEM, CRT, or CER format) to upload it.
   d) If there are no additional intermediate certificates, click the **Import** button to install the uploaded certificate.

FIGURE 407 Installing the Certificate



Alternatively, you can simplify this process by appending the intermediate CA certificates to the RUCKUS Unleashed certificate file. Then, you only need to import a single file. The intermediate certificates will be imported automatically. In this case, you will see multiple ---BEGIN CERTIFICATE--- and ---END CERTIFICATE--- pairs in the file.

SSL Certificate Advanced Options

The **Advanced Options** section allows you to perform additional certificate management functions.

These include the following:

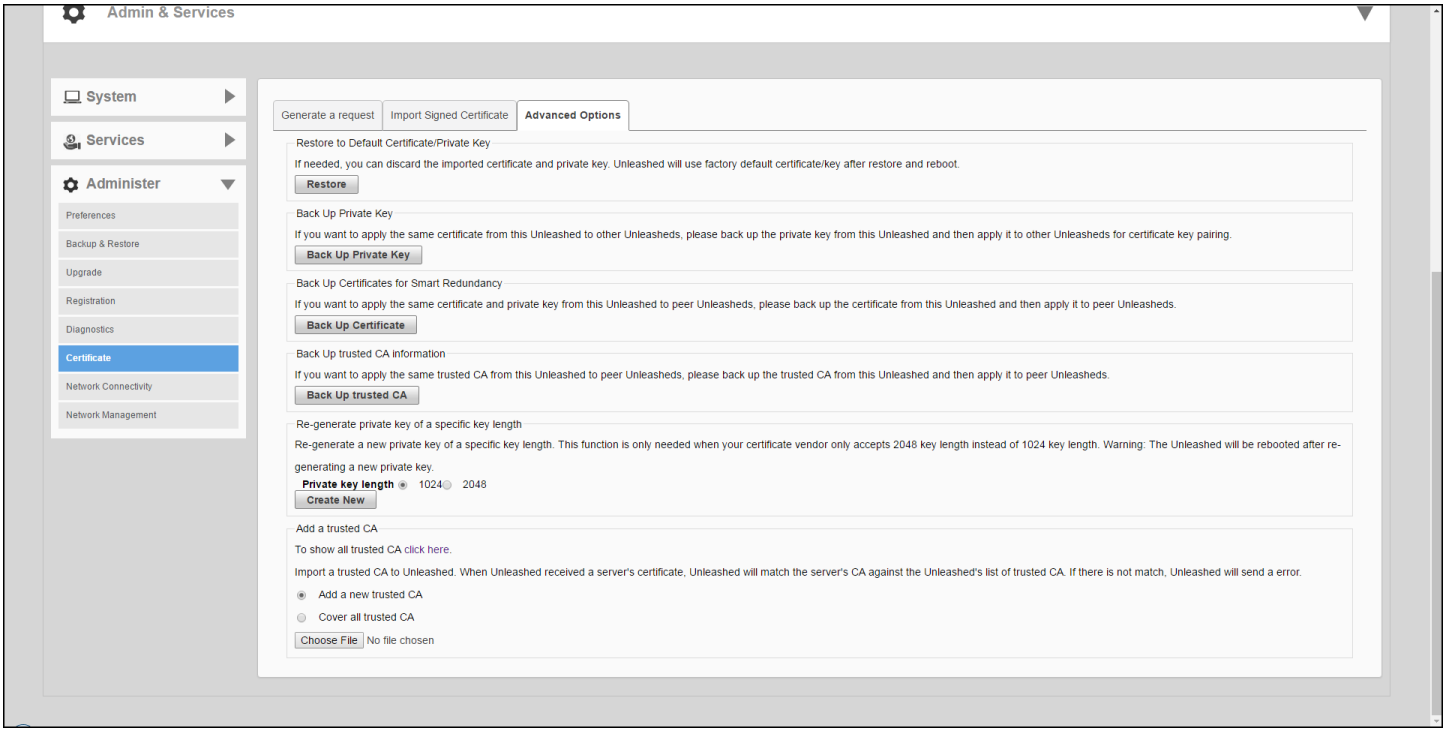
- **Restore to Default Certificate/Private Key**: This deletes any certificate and private key that has been imported, and restores the factory default certificate/private key after restore and reboot.

  NOTE
  Restoring Unleashed to factory default state does not remove imported SSL certificates. Use this option to remove any imported certificates and revert to the factory default state.

- **Back Up Private Key**: Back up the current private key by downloading it for disaster recovery or for use on another Unleashed AP. If your Unleashed AP is replaced due to an RMA, you will need to restore the private key if you have installed a public certificate. Ensure that the private key is kept secure because the security of your SSL communications depends on it.
- **Back up certificates for Smart Redundancy**: If you have more than one Unleashed AP , you can install the same SSL certificate/private key pair on both devices. In this way, you can access the shared virtual management interface advertised in DNS for the same FQDN without seeing the security warning.
- **Back Up Trusted CA Information**: Use this option to apply the same trusted CA from this Unleashed AP to peer Unleashed APs. The file is output as a .tar.gz file containing all trusted Certificate Authoritiy information currently installed on this Unleashed AP. This compressed file must be decompressed and the files imported into the peer Unleashed AP using the Add a Trusted CA feature described below.

- **Re-Generate Private Key of a Specific Key Length**: Use this option if your previous private key has been compromised or you need to use a stronger key (either 1024 or 2048 bits). Note that a new certificate must be generated and installed afterwards.
- **Add a Trusted CA**: Use this option to import CA information. Click the **Click Here** link to display all of the current trusted CA information, with each trusted CA separated by a string of number symbols ("#######"). Options include:
- **Add a new trusted CA**: Import a single CA file.
- **Cover all trusted CA**: Use the new trusted CA file to cover all existing trusted CA files

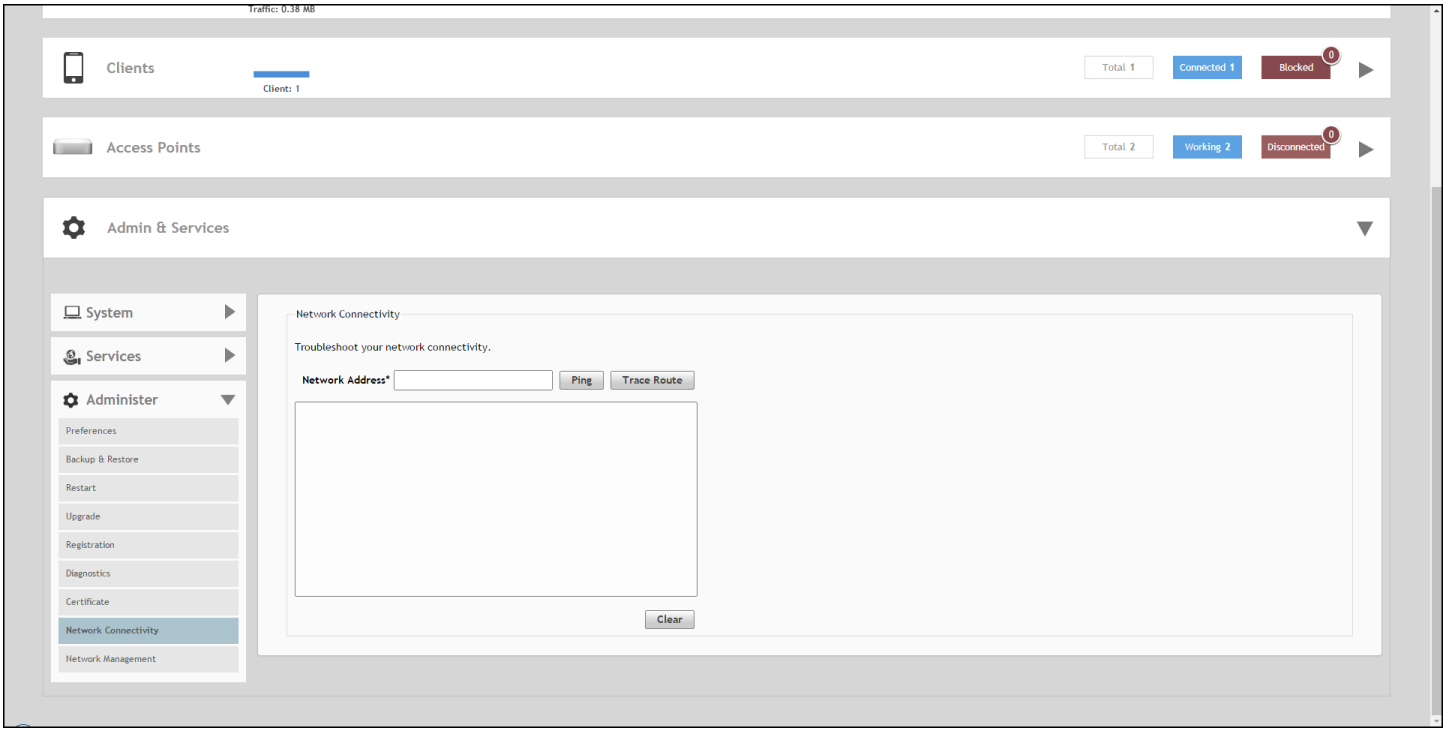
FIGURE 408 SSL Certificate Advanced Options



Testing Network Connectivity

The Unleashed web interface provides two common tools used to diagnose connectivity issues. The Network Connectivity tools - **Ping** and **Traceroute** - can be accessed from the **Admin & Services > Administer > Network Connectivity** page.

FIGURE 409 Using Ping and Traceroute to test network connectivity



Network Management

RUCKUS Unleashed provides support for Simple Network Management Protocol (SNMP v2 and SNMP v3), which allows you to query system information such as system status, AP status, AP Ethernet port status, and so on.

You can also enable SNMP traps to receive immediate notifications for possible AP and client issues.

> **NOTE**
> By default, all traps are disabled, If you need to enable a trap, you can do so using an SNMP SET command under the scalar MIB nodes: ruckusUnleashedEventTrapSwitchCmd.

The procedure for enabling the internal SNMP agent depends on whether your network is using SNMPv2 or SNMPv3. SNMPv3 mainly provides security enhancements over the earlier version, and therefore requires you to enter authorization passwords and encryption settings instead of simple clear text community strings.

Both SNMPv2 and SNMPv3 can be enabled at the same time. The SNMPv3 framework provides backward compatibility for SNMPv1 and SNMPv2c management applications so that existing management applications can still be used to manage Unleashed with SNMPv3 enabled.

> **NOTE**
> For a list of the MIB variables that you can get and set using SNMP, check the related SNMP documentation on the RUCKUS Support website at *http://support.ruckuswireless.com/documents*.

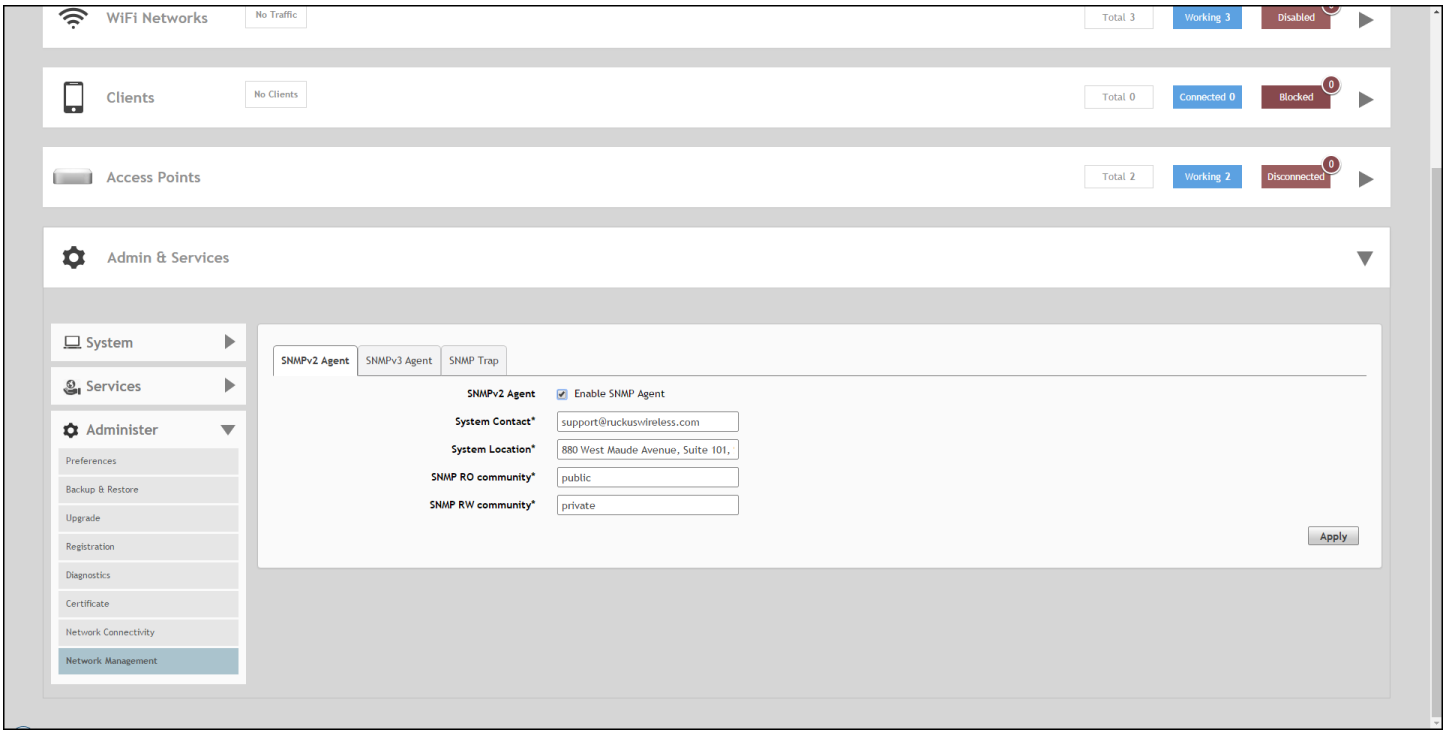
SNMPv2

If your network uses SNMPv2:

1. Go to **Admin & Services > Administer > Network Management**.

2. On the **SNMPv2 Agent** tab, select the **Enable SNMP Agent** check box.
3. Enter the following information:
   - In **System Contact**, type your email address (optional).
   - In **System Location**, type the location of the ZoneDirector device (optional).
   - In **SNMP RO community** (required), set the read-only community string. Applications that send SNMP Get-Requests to Unleashed (to retrieve information) will need to send this string along with the request before they will be allowed access. The default value is public.
   - In **SNMP RW community** (required), set the read-write community string. Applications that send SNMP Set-Requests to Unleashed (to set certain SNMP MIB variables) will need to send this string along with the request before they will be allowed access. The default value is private.
4. Click **Apply** to save your changes.

FIGURE 410 SNMPv2 Agent



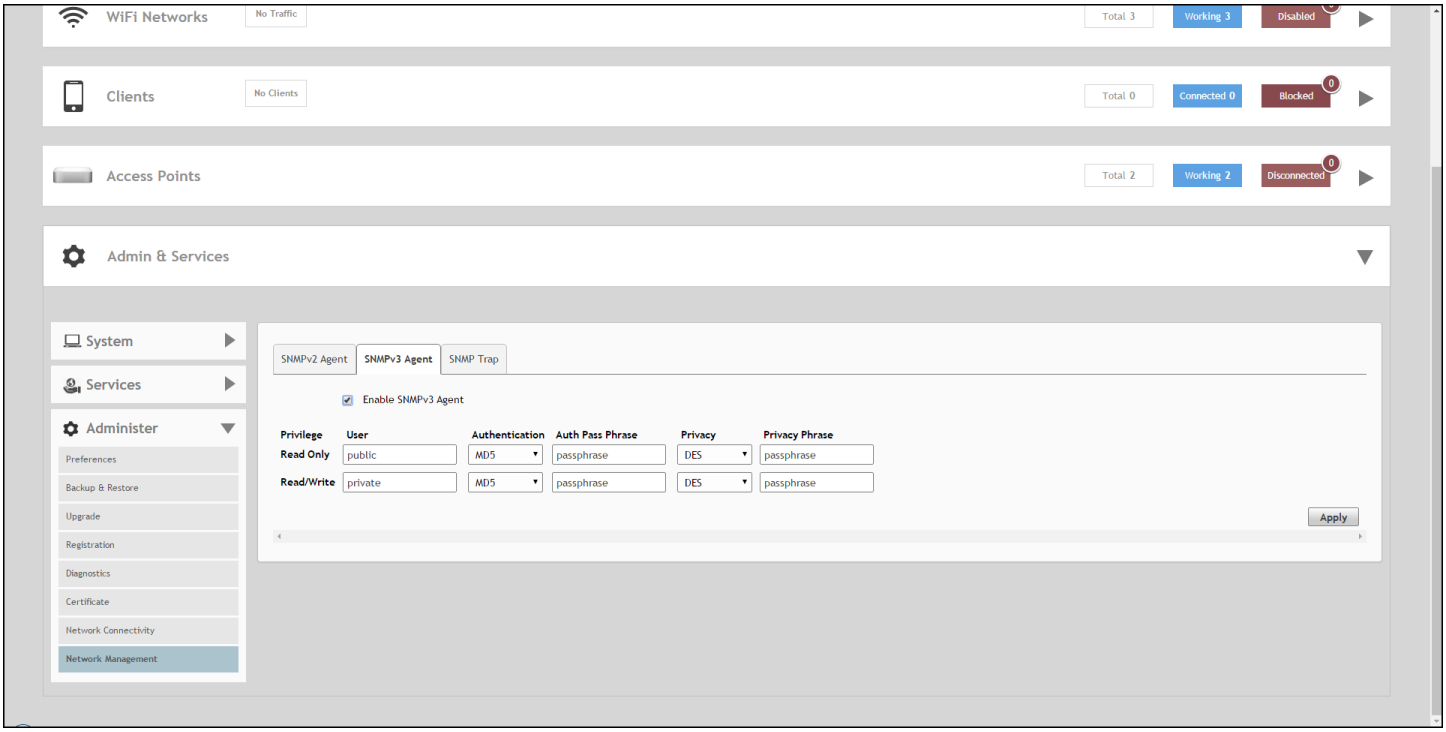
SNMPv3

If your network uses SNMPv3:

1. Go to **Admin & Services > Administer > Network Management**.
2. On the **SNMPv3 Agent** tab, select the **Enable SNMPv3 Agent** check box.

3. Enter the following information for both the **Read Only** and **Read-Write** privileges:
   - **User**: Enter a user name between 1 and 31 characters.
   - **Authentication**: Choose MD5 or SHA authentication method (default is MD5).
   - **MD5**: Message-Digest algorithm 5, message hash function with 128-bit output.
   - **SHA**: Secure Hash Algorithm, message hash function with 160-bit output.
   - **Auth Pass Phrase**: Enter a passphrase between 8 and 32 characters in length.
   - **Privacy**: Choose DES, AES or None.
   - **DES**: Data Encryption Standard, data block cipher.
   - **AES**: Advanced Encryption Standard, data block cipher.
   - **None**: No Privacy passphrase is required.
   - **Privacy Phrase**: If either DES or AES is selected, enter a Privacy phrase between 8 and 32 characters in length.
4. Click **Apply** to save your changes.

FIGURE 411 SNMPv3 Agent



Enabling SNMP Trap Notifications

If you have an SNMP trap receiver on the network, you can configure Unleashed to send SNMP trap notifications to the server.

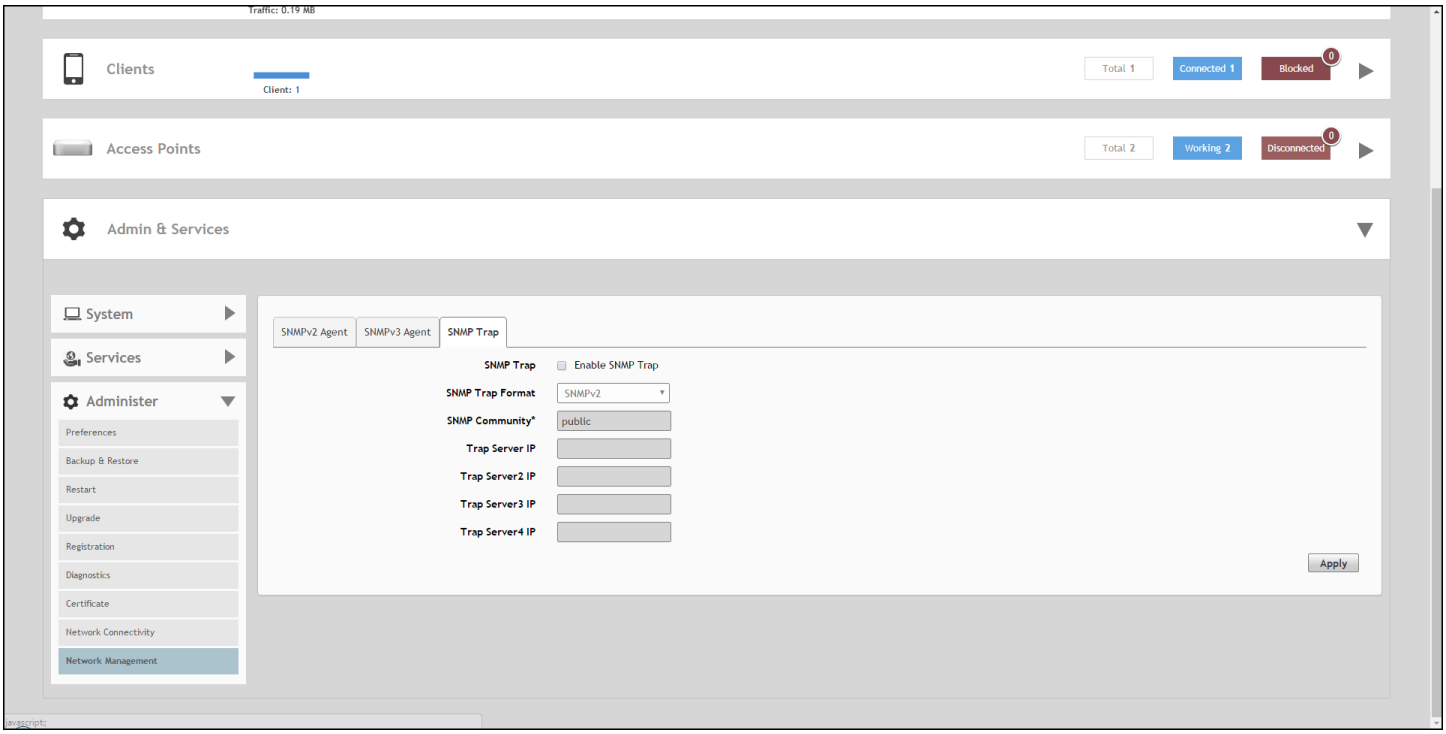
Enable this feature if you want to automatically receive notifications for AP and client events that indicate possible network issues.

To enable SNMP trap notifications:

1. Go to **Admin & Services > Administer > Network Management**.
2. On the **SNMP Trap** tab, select the **Enable SNMP Trap** check box.

3. In **SNMP Trap format**, select either **SNMPv2** or **SNMPv3**. You can select only one type of trap receiver. If you select SNMPv2, you only need to enter the IP addresses of up to four SNMP trap receivers on your network. If you select SNMPv3, enter up to four trap receiver IP addresses along with authentication method passphrase and privacy (encryption) settings.
4. Click **Apply** to save your changes.

FIGURE 412 SNMP Trap



Enabling Management via Unleashed Multi-Site Manager

If you have a RUCKUS Unleashed Multi-Site Manager (UMM) server installed on the network, you can enable Unleashed Multi-Site Manager management to centralize monitoring and administration of your remote Unleashed deployments.

The Unleashed Multi-Site Manager allows customers to manage up to 300 Unleashed networks from a central location, enabling remote administration of multiple Unleashed deployments using a single admin user name and password.

The Unleashed Multi-Site Manager provides the following critical centralized network management functions:

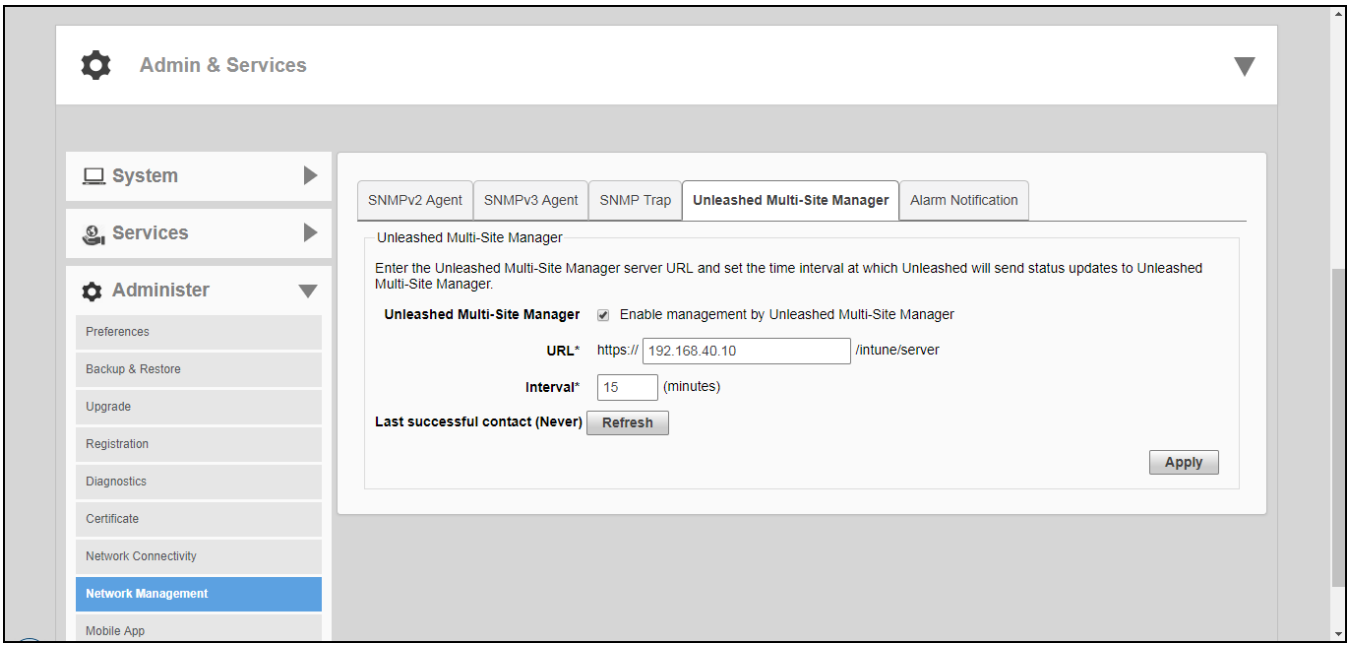
- Monitoring: Provides the ability to view the overall health status of all Unleashed networks, events and alarms, placement of APs on a world map, and connected client information from the dashboard.
- Reporting: Detailed statistics reports are available including device inventories, client associations, resource monitoring, throughput capacity, etc.
- Management: Enables several management activities from a central location, including scheduled software upgrades, backup and restore tasks, and the ability to create cookie-cutter configuration templates for deployment at multiple sites.

To enable Unleashed Multi-Site Manager administration:

1. Go to **Admin & Services > Administer > Network Management**, and click the **Unleashed Multi-Site Manager Management** tab.
2. Under *Unleashed Multi-Site Manager Management*, select the **Enable management by Unleashed Multi-Site Manager** check box.

3. In **URL**, type the Unleashed Multi-Site Manager DNS host name or IP address of the Unleashed Multi-Site Manager server.
4. In **Interval**, type the time interval (in minutes) at which Unleashed will send status updates to the Unleashed Multi-Site Manager server. The default interval is 15 minutes.
5. Click **Apply**. The message *Setting Applied* appears. You have completed enabling Unleashed Multi-Site Manager management. For more information on how to configure and manage your Unleashed deployment from the Unleashed Multi-Site Manager web interface, refer to the Unleashed Multi-Site Manager documentation.

FIGURE 413 Enabling Unleashed Multi-Site Manager management



Configuring Alarm Event Notification Settings

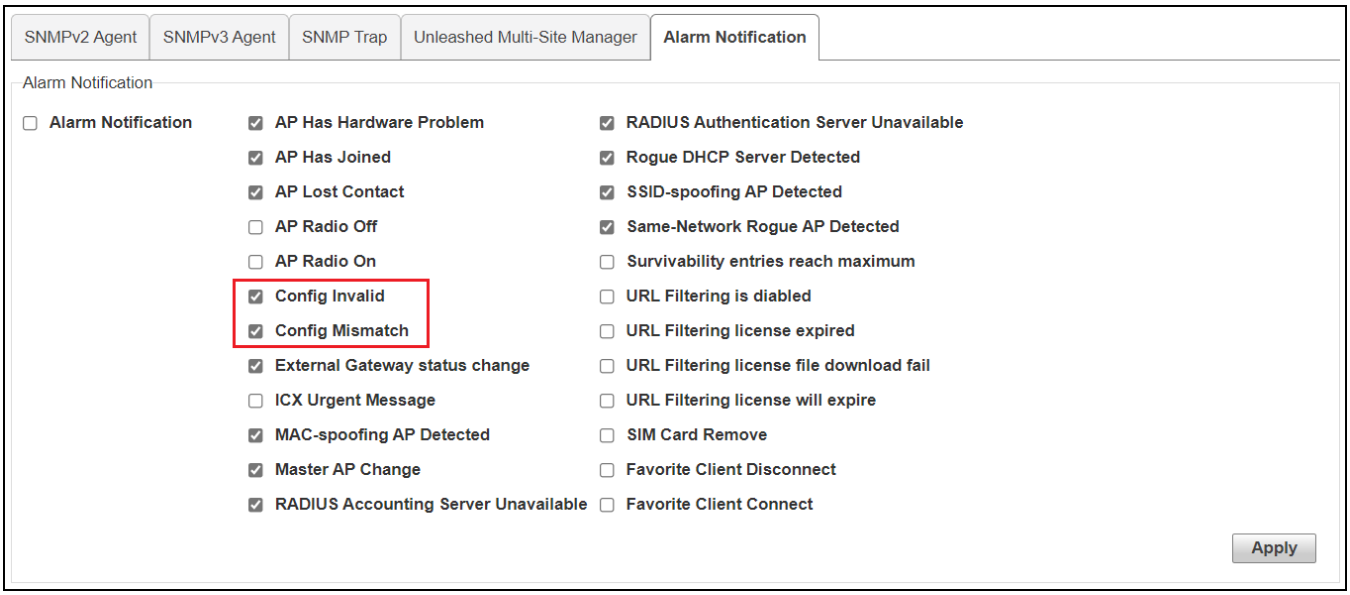
The web interface allows you to customize the content and delivery for a wide range of alarm events. When a matching event occurs, admins can be notified either through email or the mobile app.

To configure alarm event notifications and email/mobile app delivery:

1. Go to **Admin & Services** > **Administer** > **Network Management** > **Alarm Notification**.
2. In *Alarm Event*, select/deselect the event categories for which notifications will be delivered.
3. Click **Apply** to save your changes.
4. In *Email Address*, enable the check box and enter the destination address for alarm notifications. An email server must first have been configured from the *System* > *System Info* screen.

5. Click **Test** to test email delivery. Click **Apply** to save your changes.

FIGURE 414 Alarm Notification Settings



Enabling Mobile App Remote Management

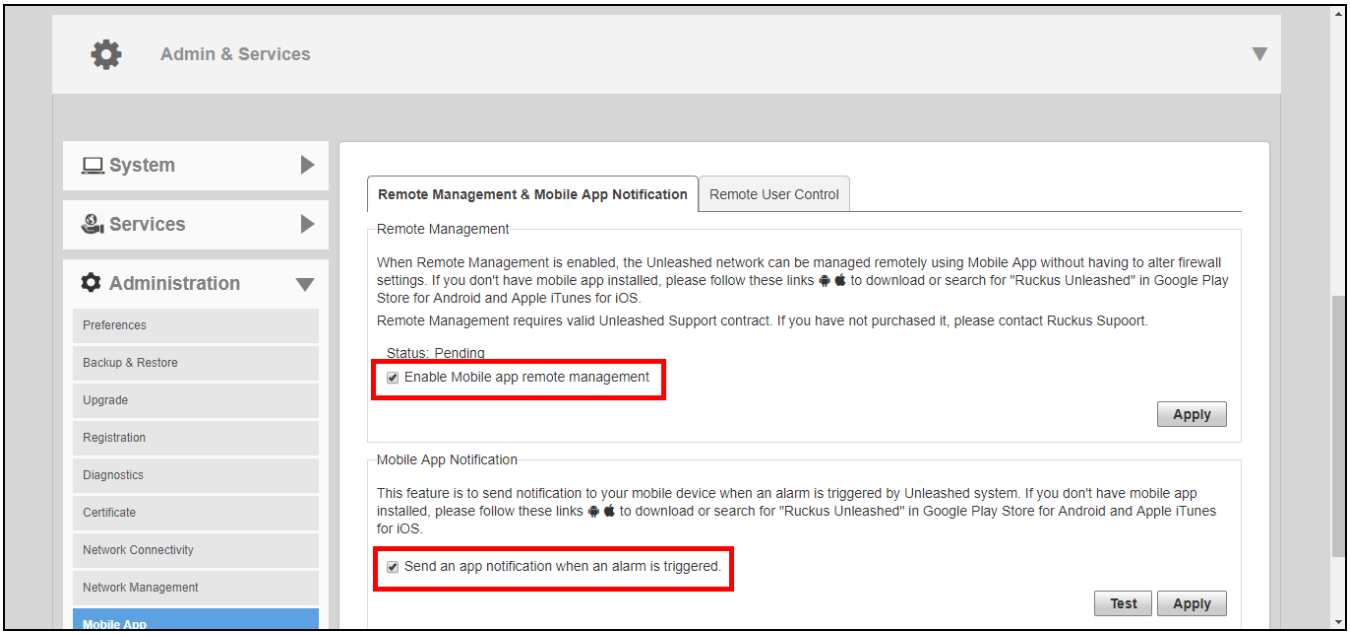
The Unleashed mobile app provides another way to manage your Unleashed network - using an Android or iOS client.

To enable Unleashed mobile app remote management:

1. Go to **Admin & Services > Administration > Mobile App**.

2. On the **Mobile App Notification** tab, select whether to send a notification to the app when an alarm is triggered. Click **Test** to send a test notification, and click **Apply** to save your changes.

FIGURE 415 Enabling mobile app remote management

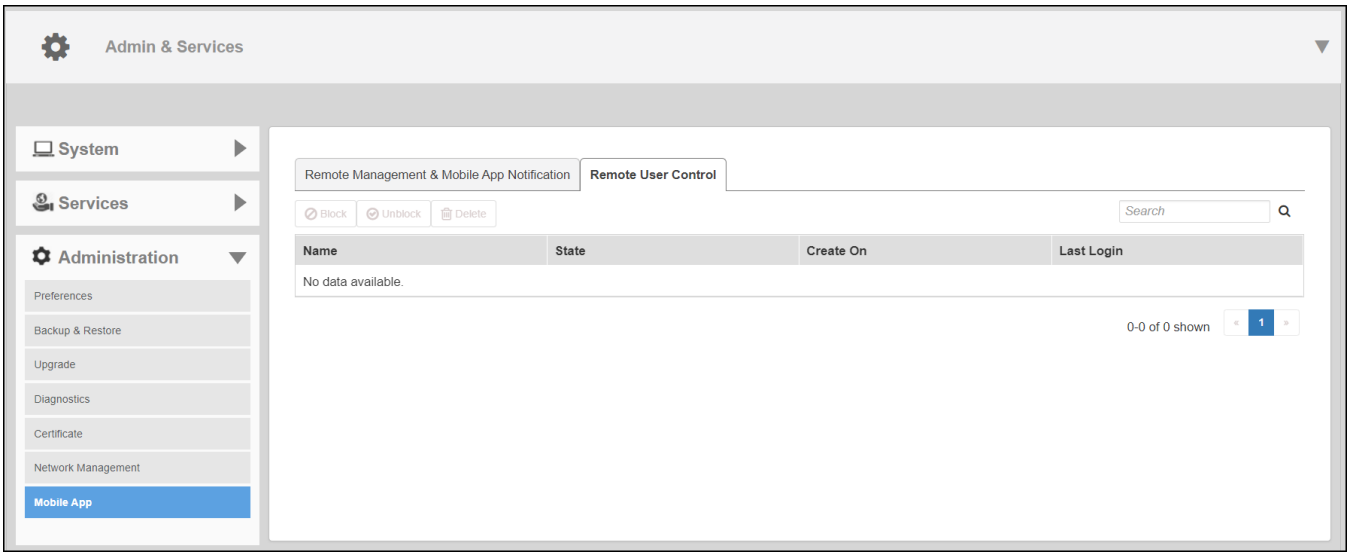


3. Optionally, enable the check box next to **Enable Mobile app remote management**, and click **Apply**.

FIGURE 416 Remote Management

4. On the *Remote User Control* tab, you can view mobile app connections and block or unblock mobile app clients.

FIGURE 417 Remote user control



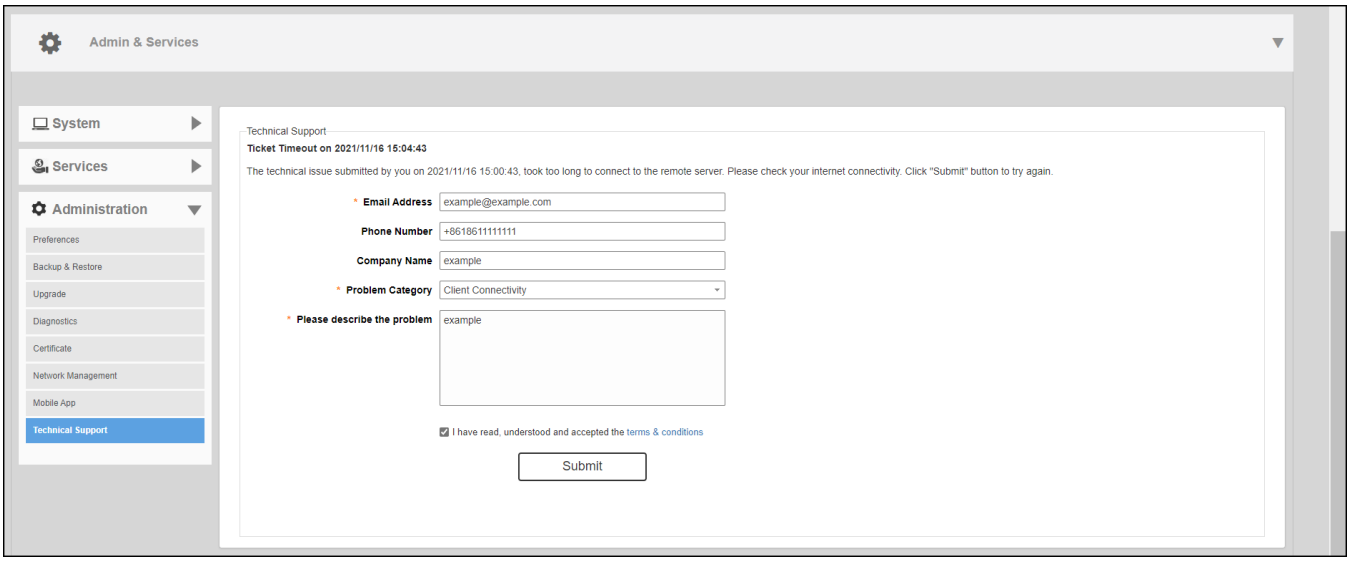
Technical Support

You can request technical support to troubleshoot your Unleashed technical issues.

Complete the following steps to request technical support.

1. Select **Admin & Services** > **Administration** > **Technical Support**.

FIGURE 418 Requesting Technical Support



2. Enter your email address.
3. (Optional) Enter your phone number and company name.
4. From the **Problem Category** list, select a problem type.
5. Enter a description about your technical problem.
6. Select the **I have read, understood and accepted the terms & conditions** check box and click **Submit**.

NOTE
When you enable technical support, Unleashed disconnects from its registered UMM and connects to the RUCKUS remote UMM. After the requested technical support is completed, Unleashed registers back to UMM.

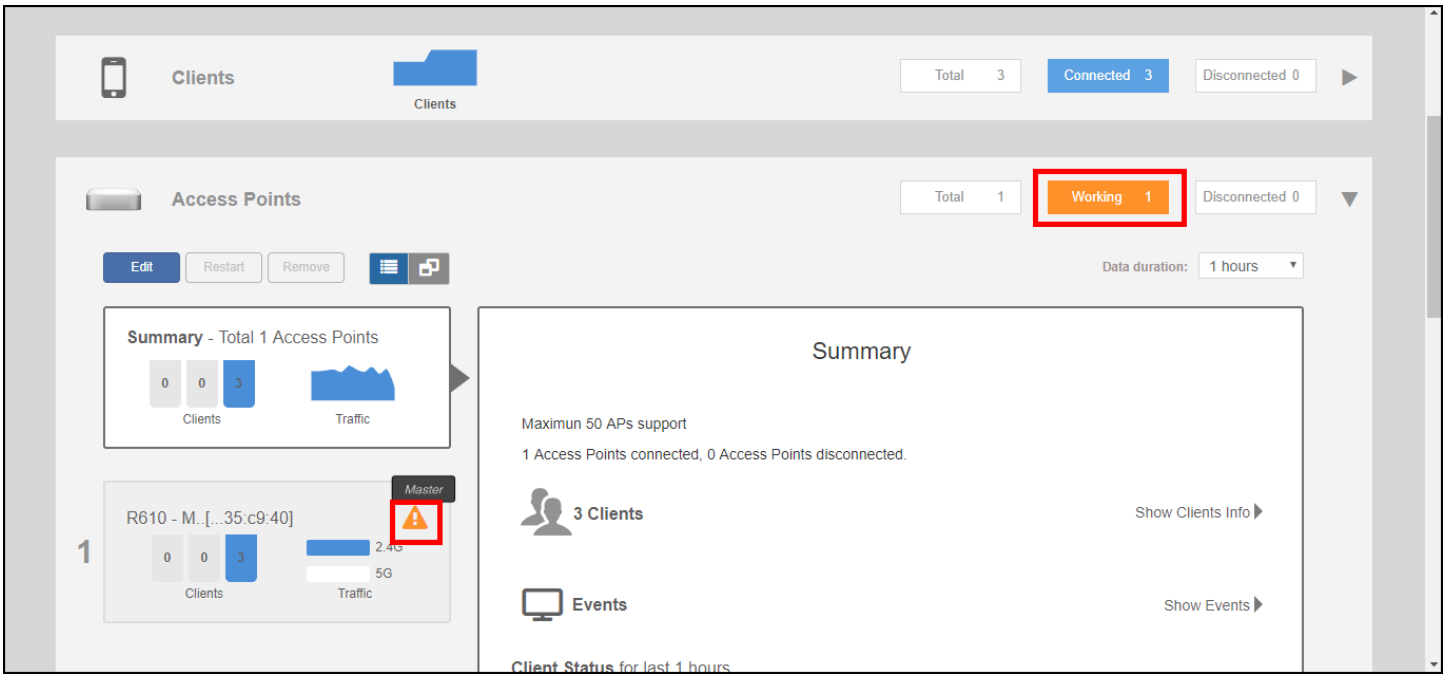
Unleashed Access Point Power Supply Considerations

- AP Power Warnings..... 501
- Power Limitations by PoE Mode and AP Model..... 503

AP Power Warnings

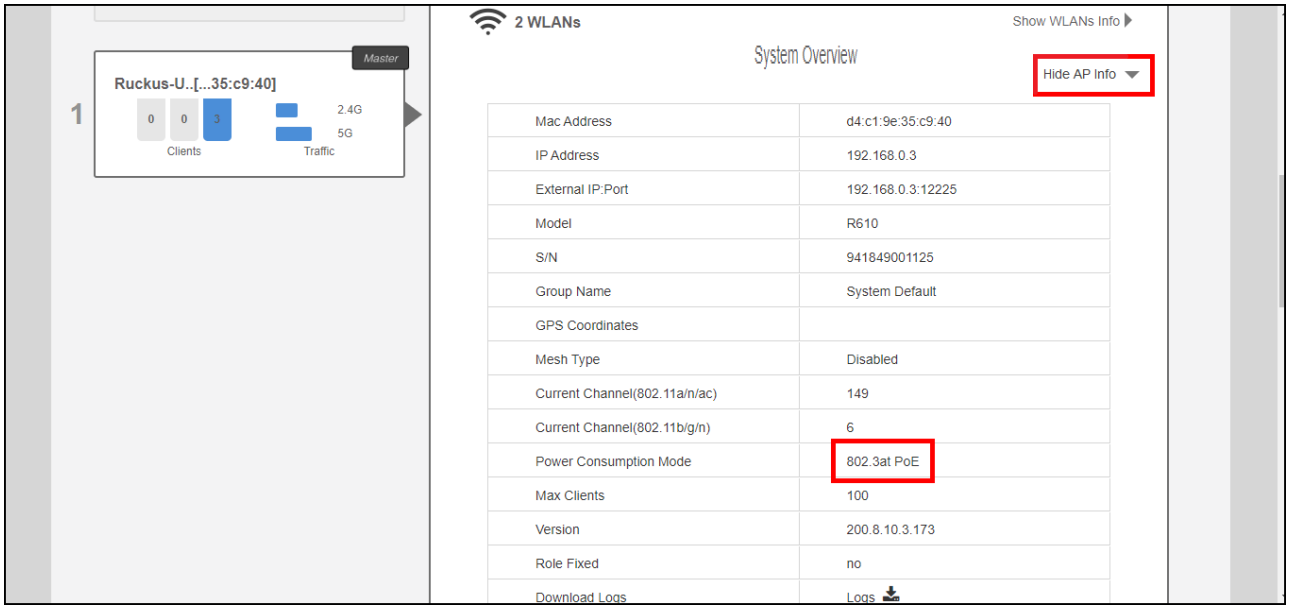
Beginning with release 200.8, the RUCKUS Unleashed dashboard displays warning icons when an AP is operating in reduced power mode.

FIGURE 419 Warning icons indicate an AP is operating in reduced-power mode



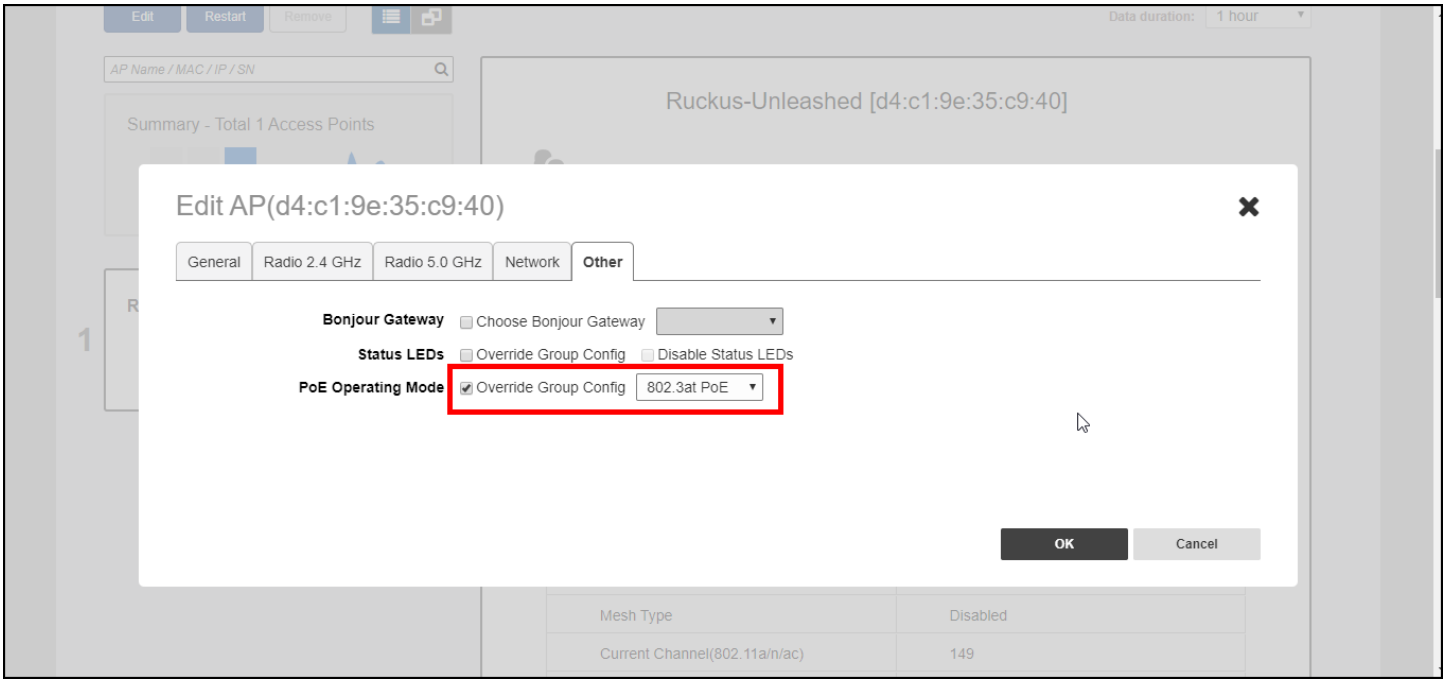
If a warning icon appears, click **Show AP Info** and locate the **Power Consumption Mode** entry. Refer to *Power Limitations by PoE Mode and AP Model* to see what limitations are in effect.

FIGURE 420 Showing AP Power Consumption Mode



If power supply deficiency is caused by incorrect power level negotiation between the AP and the switch/PoE injector, you can enforce the AP Power Level on the AP's configuration page. Go to **Access Points > [AP] > Edit > Other > PoE Operating Mode**. Enable **Override Group Config** and select a power mode from the menu.

FIGURE 421 Override PoE Operating Mode



Power Limitations by PoE Mode and AP Model

The following tables list the Power over Ethernet (PoE) operating modes for each AP model, along with the performance and feature limitations when the AP is in any of the supported reduced power modes.

Indoor AP	Outdoor AP
R850	T610
R750	M510
R720	T750
R710	T750SE
R650	T350c
R610	T350d
R550	T350SE
H550	

R850

TABLE 37 R850 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	5Gbps Eth	1Gbps Eth	USB	Comments
DC		4/4	8/8	Enabled	Enabled	Enabled	
802.3af		1/4	1/8	Enabled	Disabled	Disabled	Not supported in operation mode
802.3at	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	
802.3bt/class5	35W	4/4	8/8	Enabled	Enabled	Enabled	
PoE injector (Model 480125A) 60W		4/4	4/8	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from SZ GUI

R750

TABLE 38 R750 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB
DC		4/4	4/4	Enabled	Enabled	Enabled
802.3af		2/4	2/4	Enabled	Disabled	Disabled
802.3at	25W	4/4	4/4	Enabled	Enabled	Enabled
PoE injector (Model 480125A) 60W		4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled

R720

TABLE 39 R720 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	Comments
DC		4/4 (22dBm)	4/4 (23dBm)	Enabled	Enabled	Enabled	
802.3af		1/4 (20dBm)	1/4 (18dBm)	Enabled	Disabled	Disabled	

TABLE 39 R720 PoE Modes (continued)

802.3at	25W	4/4 (20dBm)	4/4 (18dBm)	Enabled	Disabled	Disabled	
802.3bt/Class 5	35W	4/4 (22dBm)	4/4 (23dBm)	Enabled	Enabled	Enabled	
PoE injector (Model 480125A) 60W		4/4	4/4	Enabled	Enabled	Enabled	Force to 802.3bt/ Class 5 from GUI

R710

TABLE 40 R710 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC		4/4 (22dBm)	4/4 (20dBm)	Enabled	Enabled	Enabled
802.3af		2/4 (20dBm)	4/4 (19dBm)	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	25W	4/4 (22dBm)	4/4 (20dBm)	Enabled	Enabled	Enabled

R650

TABLE 41 R650 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth(PoE)	1Gbps Eth	USB
DC		2/2	4/4	Enabled	Enabled	Enabled
802.3af		2/2	2/4	Enabled	Disabled	Disabled
802.3at	25W	2/2	4/4	Enabled	Enabled	Enabled
PoE Injector (Model 480125A)		2/2	4/4	Enabled (1Gbps speed)	Enabled	Enabled

R610

TABLE 42 R610 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC		4/4	4/4	Enabled	Enabled	Enabled
802.3af		2/4	4/4	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	24W	4/4	4/4	Enabled	Enabled	Enabled

R550

TABLE 43 R550 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1bps Eth(PoE)	1Gbps Eth	USB
DC		2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled
802.3af		2/2 (10 dBm)	2/2 (18 dBm)	Enabled	Disabled	Disabled
802.3at	25W	2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled
PoE Injector (Model 480125A)		2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled

H550

TABLE 44 H550 PoE Modes

	LLDP Power Ask	2.4G Tx/ Rx(16dBm)	5G Tx/ Rx(19dBm)	1Gbps Eth	USB	PSE		
						POE_Out	Power @ PD	Maximum Cable Length
DC		2/2	2/2	Enabled	Enabled	Enabled		
802.3af	12.95W	2/2	2/2	Enabled	Disabled	Disabled	NA	NA
802.3at/ injector	25W	2/2	2/2	Enabled	Enabled	Disabled	NA	NA
					Enabled	Enabled	8.4W	20m
					Disabled	Enabled	12.4W	20m
802.3bt, uPoE, PoH	40W	2/2	2/2	Enabled	Enabled	Enabled	12.95W	100m

T610

TABLE 45 T610 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC		3/3 (22dBm)	3/3 (20dBm)	Enabled	Enabled	Enabled (0.5W)
802.3af		2/3 (18dBm)	3/3 (20dBm)	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	25W	3/3 (22dBm)	3/3 (20dBm)	Enabled	Enabled	Enabled (0.5W)

M510

TABLE 46 M510 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC	Full	2/2 (23dBm)	2/2 (20dBm)	Enabled	Enabled	Enabled
802.3af	12.95W	1/2 (19dBm)	2/2 (19dBm)	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	25W	2/2 (23dBm)	2/2 (20dBm)	Enabled	Enabled	Enabled

T750

TABLE 47 T750 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	PSE	Comment
DC		4/4	4/4	Enabled	Enabled	Enabled	Enabled	
802.3af		1/4	1/4	Enabled	Disabled	Disabled	Disabled	Not supported operation mode
802.3at w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Disabled	
802.3at w/ USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Disabled	Alt AT mode config by AP CLI
802.3bt/Class 5	35W	4/4	4/4	Enabled	Enabled	Enabled	Disabled	

TABLE 47 T750 PoE Modes (continued)

803.3bt/Class 6		4/4	4/4	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/Class 7		4/4	4/4	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
PoE injector (Model 480125A)		4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Disabled	Force to 802.3bt/Class 5
PoE injector		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/Class 7

T750SE

TABLE 48 T750SE PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	PSE	Comment
DC		4/4	4/4	Enabled	Enabled	Enabled	Enabled	
802.3af		1/4	1/4	Enabled	Disabled	Disabled	Disabled	Not supported operation mode
802.3at w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Disabled	
802.3at w/ USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Disabled	Alt AT mode config by AP CLI
802.3bt/Class 5	35W	4/4	4/4	Enabled	Enabled	Enabled	Disabled	
803.3bt/Class 6		4/4	4/4	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/Class 7		4/4	4/4	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
PoE injector (Model 480125A)		4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Disabled	Force to 802.3bt/Class 5
PoE injector		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/Class 7

T350c

TABLE 49 T350c PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth
802.3af		2/2 (19dBm)	2/2 (18dBm)	Enabled
802.3at/PoE injector	25W	2/2	2/2	Enabled

T350d

TABLE 50 T350d PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth	USB
DC		2/2	2/2	Enabled	Enabled

TABLE 50 T350d PoE Modes (continued)

802.3af		2/2 (19dBm)	2/2 (18dBm)	Enabled	Disabled
802.3at/PoE injector	25W	2/2	2/2	Enabled	Enabled

T350SE

TABLE 51 T350SE PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth	USB
DC/PoE injector		2/2	2/2	Enabled	Enabled
802.3at	25W	2/2	2/2	Enabled	Enabled
802.3af		2/2 (16dBm)	2/2 (16dBm)	Enabled	Disabled

© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com